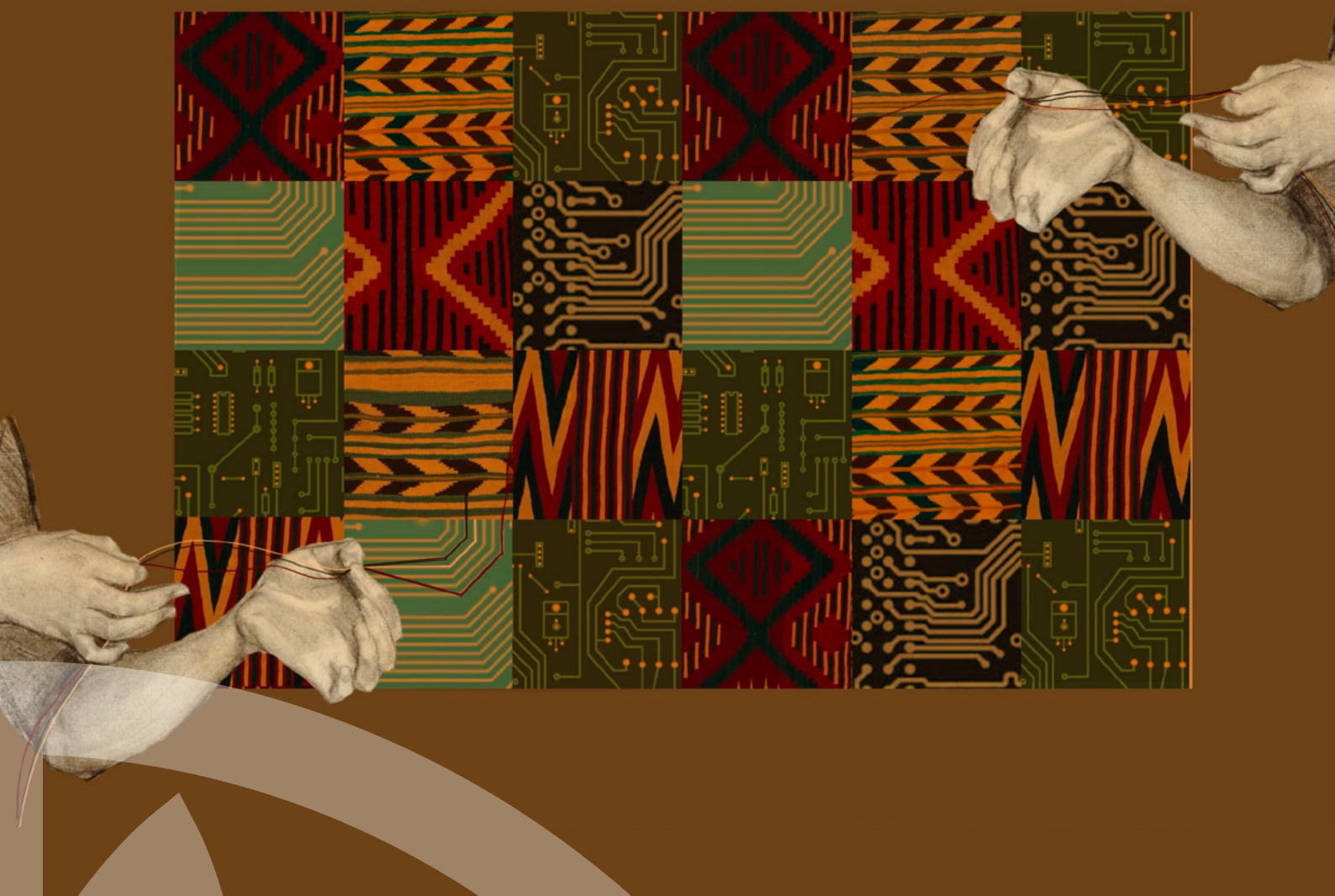




GENDERED IMPACTS OF THE MILITARISATION OF DATA-INTENSIVE SYSTEMS



Reaching Critical Will

Table of Contents

Introduction.....	2
Data-intensive systems and the fascist project of categorisation and control	4
Colonial contexts.....	5
Culling and targeting.....	5
Hacking the government.....	6
Building the military-tech-industrial complex.....	8
Bias in data collection and use.....	12
How bias harms humans.....	14
Categorisation machines	16
Data and surveillance	17
Bias towards violence in the militarisation of data-intensive systems	20
Gender-based violence.....	24
What is gender-based violence	24
GBV and militarism.....	26
GBV and the military use of data-intensive systems	27
Projecting power without vulnerability	29
Environmental damage.....	31
Energy and water consumption.....	31
Mineral extraction.....	39
Conclusion: A feminist approach to the militarisation of data-intensive systems.....	41

Introduction

In recent years, militaries, police, and border and immigration enforcement agencies have been increasingly using data-intensive systems, resulting in ever-more technologically advanced state violence. The use of these systems in the civilian domain has already raised many legal, political, and ethical concerns; the militarisation of these systems is causing even more harm, including surveillance, discrimination, incarceration, detention, deportation, and death.

The widespread use by militaries, police, and border control of technologies such as biometric surveillance tools, decision support systems, autonomous weapon systems, and more, can result in harmful consequences, especially to those who already experience state violence on a daily basis. As we have seen in the past with the development of new weapons and militarised technologies, their impacts on women, gender-non confirming, LGBTQ+ people, and racialised people tend to be overlooked and unaddressed. Thus, in this report, we will be investigating the gendered impacts of the militarisation of data-intensive systems.

In the first chapter, we analyse the context in which these systems are being developed and used. We look at the religious and fascist ideologies of the people in charge of the companies that are developing data-intensive systems and how these ideas influence why and how their technologies are developed, and against who they are being and will be used.

The second chapter explores how data-intensive systems reinforce and amplify existing inequalities. We investigate how bias in datasets, design, and use can each lead to violent outcomes for certain groups of people, especially with the widespread adoption of these systems in warfare, law enforcement, and border control.

In the third chapter, we investigate how data-intensive systems can be used to commit or facilitate gender-based violence (GBV). We not only explore instances in which technologies are already causing GBV, but also how norms of militarised masculinities that permeate the militarisation of these systems can result in further harm.

Chapter four demonstrates that the structures that uphold patriarchy and gender inequality also impact how women, gender non-confirming people, and LGBTQ+ people experience the environmental harm caused by data-intensive systems.

In the conclusion, we argue that it is necessary to adopt an intersectional feminist approach to challenge the militarisation of data-intensive system. This includes challenging narratives that the militarisation of technology is necessary or inevitable, and seeking solutions grounded on the broader opposition to colonialism, racism, patriarchy and capitalism.

Due to the concerns raised in this paper, we oppose the militarisation of data-intensive systems. Our concerns with and opposition to militarised data-intensive systems are grounded within our wider opposition to weapons, war, and violence, as well as our opposition to patriarchal, racist, and colonial power relations that are embedded within these technologies. This technology, rather than placing limits on violence or harm, expands both. Governance is insufficient in the face of the profits and power the developers of these technologies seek. Prohibition is the only responsible path for human and planetary well-being.

A note about gender

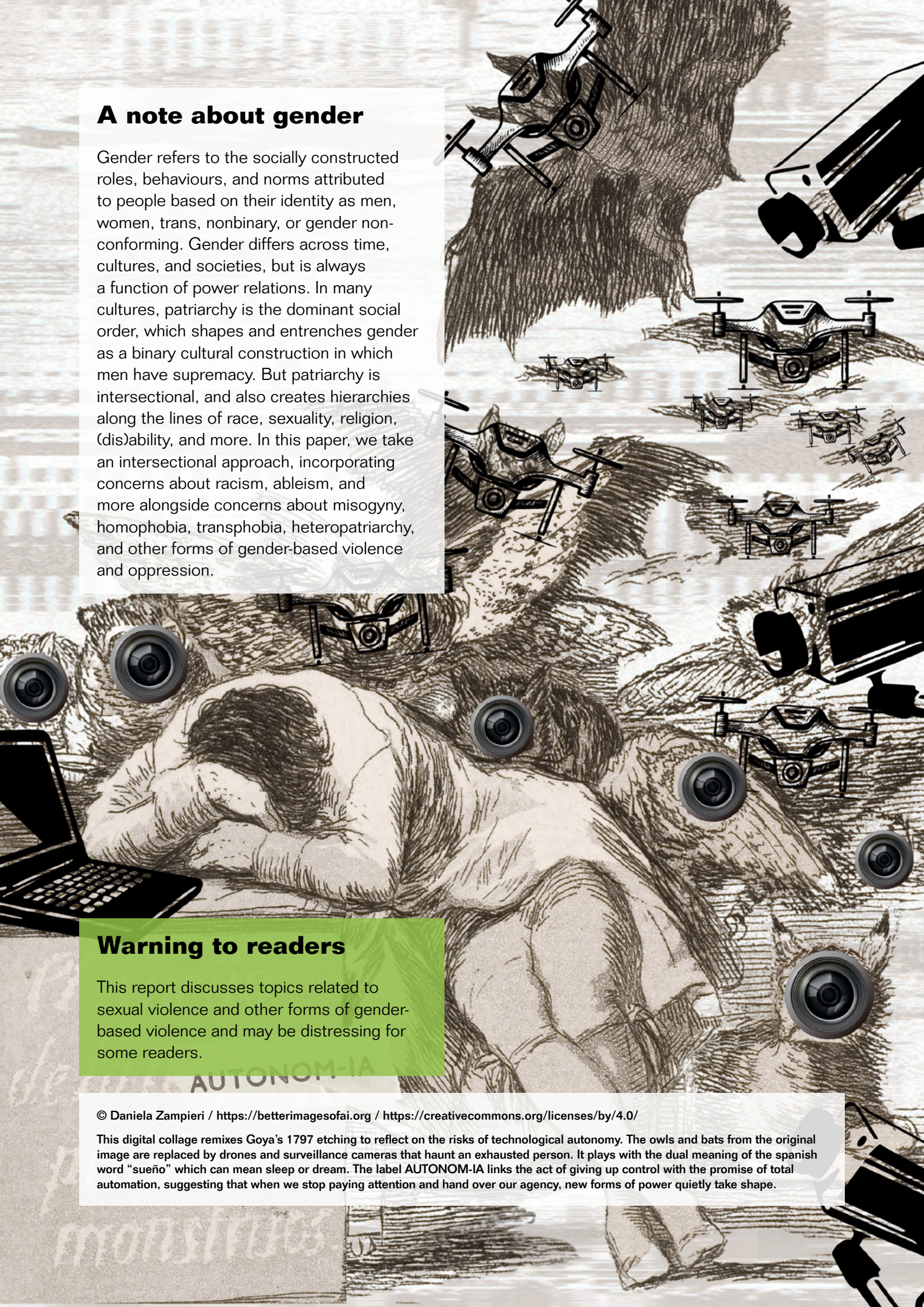
Gender refers to the socially constructed roles, behaviours, and norms attributed to people based on their identity as men, women, trans, nonbinary, or gender non-conforming. Gender differs across time, cultures, and societies, but is always a function of power relations. In many cultures, patriarchy is the dominant social order, which shapes and entrenches gender as a binary cultural construction in which men have supremacy. But patriarchy is intersectional, and also creates hierarchies along the lines of race, sexuality, religion, (dis)ability, and more. In this paper, we take an intersectional approach, incorporating concerns about racism, ableism, and more alongside concerns about misogyny, homophobia, transphobia, heteropatriarchy, and other forms of gender-based violence and oppression.

Warning to readers

This report discusses topics related to sexual violence and other forms of gender-based violence and may be distressing for some readers.

© Daniela Zampieri / <https://betterimagesofai.org> / <https://creativecommons.org/licenses/by/4.0/>

This digital collage remixes Goya's 1797 etching to reflect on the risks of technological autonomy. The owls and bats from the original image are replaced by drones and surveillance cameras that haunt an exhausted person. It plays with the dual meaning of the Spanish word "sueño" which can mean sleep or dream. The label AUTONOM-IA links the act of giving up control with the promise of total automation, suggesting that when we stop paying attention and hand over our agency, new forms of power quietly take shape.





Data-intensive systems and the fascist project of categorisation and control

In early 2025, as the Trump regime hired tech billionaire Elon Musk to use artificial intelligence in service of dismantling the US federal government,¹ Naomi Klein and Astra Taylor wrote about the end-times fascism the tech brologarchs were attempting to bring about. “Retooling and rebranding the old ambitions and privileges of empires,” the tech brologarchs “dream of splintering governments and carving up the world into hyper-capitalist, democracy-free havens under the sole control of the supremely wealthy, protected by private mercenaries, serviced by AI robots and financed by cryptocurrencies.”²

The billionaire class and their political puppets foresee a future of shocks, scarcity, and a collapse—a future their actions and technologies are accelerating—and they are preparing escape pods of privileged city-states. This approach, Klein and Taylor note, is not unlike the fundamentalist Christian sense of the rapture, “when the faithful will supposedly be lifted up to a golden city in heaven, while the damned are left to endure an apocalyptic final battle down here on earth.”³

Understanding both the religious and fascist components of the tech-brologarch project is essential to understanding the dangers of data-intensive systems. The militarisation of these systems is first and foremost part of the fascist project of categorisation and control of populations. A key part of categorisation and control is “othering,” principally along lines of gender, sexual orientation, race, immigration status, class, disability, and other identifiers that can be used to separate an “us” from a “them”. Increasingly, the category of “them” includes everyone the billionaire class deems expendable, or a danger to their project. Meaning, the majority of people living on this planet. As this section will explore, the religious, colonial, and fascist intentions of those designing, developing, and using data-

¹ Ray Acheson, “The Tech-Brologarch Nightmare,” *CounterPunch*, 16 February 2026, <https://www.counterpunch.org/2025/02/16/the-brologarch-nightmare>.

² Naomi Klein and Astra Taylor, “The rise of end times fascism,” *The Guardian*, 13 April 2025, <https://www.theguardian.com/us-news/ng-interactive/2025/apr/13/end-times-fascism-far-right-trump-musk>.

³ Ibid.

intensive systems are directly connected to the militarisation of these technologies—and are in fact part of the core objective behind the militarisation of these technologies.⁴

Colonial contexts

Inherent to this fascist, fundamentalist end-times project are anti-women, anti-LGBTQ+, anti-migrant, and anti-Black sentiments. The religiosity behind much of the billionaire fantasy of heavenly bunkers is steeped in control over bodies and the curtailment of liberation and equality of those who do not contribute to their agenda or fit into their ideals of humanity.

The tech-broliarch approach is also rooted in the colonial philosophies of Manifest Destiny, the idea that they have a right to take what they want and burn the rest. This, too, is gendered and racialised, rooted in an imperialist history of raping and pillaging, enslavement and extraction, genocide and bordering. Manifest Destiny is also intimately tied to militarism, which in today's context means increasingly incorporating data-intensive systems in the pursuit of dominance.

The technologies that the tech-bros are building cannot be separated from these contexts. The founders and leaders of these companies have specific ideas of what forms of harm and lethality are permissible. Many take an explicitly anti-human worldview, asserting the inevitability of “general artificial intelligence (AGI),” the merging of humans and machines, and the priority of meeting machine needs over human needs.⁵ These notions, which are being built into their creations, are overwhelmingly contrary to feminist, egalitarian, and antiracist world views in which people are equal, and peace and justice are deserved by all.

“What’s at stake with AI is not merely bias and unfairness but assimilation into far-right political projects,” warns Dan McQuillan in *Resisting AI*.⁶ “For fascist ideologues who glorify violence, AI’s tendencies towards epistemic, structural and administrative violence are not flaws but features. There’s a danger that the disruptive potential of AI will become entangled with the more savage disruptions of a fascistic social vision.”

Culling and targeting

The primary function of data-intensive systems isn’t to help with homework or advance medicine. Their primary functions are surveillance, categorisation, detention, deportation, incarceration, and warfare. Both because these are all essential tasks for controlling populations, and because these are the businesses that bring profit to those that own the technologies, the prisons, the weapon companies, and all of the other infrastructure and services that go along with the industries of state violence.

The tech companies that make products the public might use to summarise a document or generate text or images are largely the same companies selling their systems to militaries, immigration and border enforcement agencies, and police. And because it’s the same companies, data culled from commercial use can also be used for warfighting, policing, and repression, whether it’s for training AI models or

⁴ This chapter is largely drawn from Ray Acheson, “The Tech-Broliarch Nightmare,” *CounterPunch*, 16 February 2025, <https://www.counterpunch.org/2025/02/16/the-broliarch-nightmare>; and Ray Acheson, *Submission to the UN Secretary-General’s Report on Artificial Intelligence in the Military Domain* (New York: Reaching Critical Will, 2025), <https://reachingcriticalwill.org/resources/publications-and-research/publications/17337-wilpf-submission-to-the-un-secretary-general-s-report-on-artificial-intelligence-in-the-military-domain>.

⁵ Paris Marx, “Sam Altman’s anti-human worldview,” *Disconnect*, 23 February 2026, <https://disconnect.blog/sam-altmans-anti-human-worldview>.

⁶ Dan McQuillan, *Resisting AI: An Anti-Fascist Approach to Artificial Intelligence* (Bristol: Bristol University Press, 2022), p. 97.

using customer data to determine if they are a “target” for violence.⁷ Militaries also buy information from private data brokers and consumer apps, while police and border enforcement agencies use private data collected by commercial companies, as explained in more detail below.

Scholar Sofia Goodfriend has warned that “dragnet surveillance, mass incarceration, and unfettered drone warfare serve as the AI hype cycle’s underbelly. Death and destruction double as opportunities for data collection and refinement, allowing the private technology sector to stake out a monopoly over AI development in military and commercial sectors.”⁸ A former Technical Sergeant in the US Air Force, Lisa Ling, has likewise argued that military access to private data is a mounting concern. She has noted that this is exacerbated by private civilians connected to technology companies making their way into governments. This is allowing individuals and their companies to gain access to private data they should not be able to disclose or transmit for unintended purposes without notice. “A line that was once drawn in the sand protecting individuals right to privacy is now blurred in favor of privatization and data extraction,” she warns. “In the framework of future war, this data can be loaded into targeting systems similar to those we saw used against Palestinians.”⁹

Similarly, Heidy Khlaaf and Sarah Myers West from the AI Now Institute and Meredith Whittaker, President of Signal, argue that personal data embedded within existing commercial “foundation models” positions AI “as a link between commercial personal data and automated weapons’ target lists and surveillance capabilities.” They contend that “no effective approaches exist that reliably prevent personal data exposure in current foundation models, from contributing to ISTAR (intelligence, surveillance, target acquisition, and reconnaissance) capabilities.”¹⁰

The intertwining of technology companies, governments, and militaries means loss of privacy, threats to freedom of speech, and other human rights violations. In addition, it can lead to the use of private, personal data for warfighting, policing, and repression. In the context specifically of military use of data-intensive systems, it will lead to “big data, big compute, and civilian owned cloud technologies being used to grow and expand the existing Network Centric Warfare frameworks,” writes Ling. This will increasingly “allow for allied western countries to surveil, and share data, bypassing state oversight processes that protect individual privacy.”¹¹

Hacking the government

Tearing down privacy, human rights, civil liberties, and other protections such as environmental regulations and Indigenous treaty rights is a key goal of the tech-broliarchs building and controlling data-intensive systems. This is demonstrably the case right now in the United States, where founders and officials representing technology companies have gained enormous influence over or even embedded themselves within the government, Musk’s rampage through the US government, for example, mandated through the haphazardly constructed Department of Government Efficiency (DOGE), is in part about cutting essential services to fund tax cuts for the rich and finance Musk’s companies. But the DOGE mission was about more than money—it was fundamentally about dismantling democracy, and about replacing humans with machines. “Everything that can be machine-

⁷ “How Data Drives the Militarisation of Tech,” Privacy International, 12 September 2025, <https://www.privacyinternational.org/long-read/5667/how-data-drives-militarisation-tech>.

⁸ Sofia Goodfriend, “Deadly Slop,” *The Baffler*, 10 July 2025, <https://thebaffler.com/latest/deadly-slop-goodfriend>.

⁹ Lisa Ling, “The New Military Tech Gold Rush,” Nomos Foundation, 2 April 2025, <https://www.nomosfoundation.co.uk/post/the-new-military-tech-gold-rush>.

¹⁰ Heidy Khlaaf, Sarah Myers West, Meredith Whittaker, *Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, and Targeting*, AI Now Institute, 15 November 2024, <https://ainowinstitute.org/news/researchers-sound-alarm-on-dual-use-ai-for-defense>.

¹¹ Lisa Ling, op. cit.

automated will be,” one government official told the *Washington Post*. “And the technocrats will replace the bureaucrats.”¹²

Tech Policy Press described DOGE’s actions as “an AI coup,” noting that it “concentrates power with those who understand and control this system’s maintenance, upkeep, and upgrades.”¹³ Brian Merchant, author of *Blood in the Machine*, argued that what’s happening at the federal agencies is “a stark portrait of why power seeks to automate—and why, in enterprise AI, it has found an ideal vessel for corporate and administrative automation.”¹⁴ Data-intensive systems are a boon to the fascist project precisely because they enable automation and facilitate avoidance of accountability. Such systems use “the aura of science to perpetuate the idea that its abstract mathematical models provide a reliable way of knowing, and promotes a reductive definition of truth that is claimed as inherently superior to lived experience,” explains Dan McQuillan.¹⁵

McQuillan warns, “In institutions with the power to cause social harms, the threat of AI is not the substitution of humans by machines but the computational extension of existing social automatism and thoughtlessness.”¹⁶ Data-intensive systems will produce the kind of thoughtlessness that Hannah Arendt warned about in terms of the banality of evil,¹⁷ which “manifests as the inability to critique instructions, the lack of reflection on consequences, and a commitment to the belief that the correct ordering is being carried out.”¹⁸

This is a perfect landscape for the flourishing of fascism and militarism, and the generation and perpetuation of all their harms. Data-intensive systems have a tendency to “propagate patterns of carelessness and extractiveness alongside a concentration and centralization of power,”¹⁹ allowing the fascists controlling the technology and the government to have free rein to pursue profits at the expense of the majority of people and the planet. The AI coup, as the *Philadelphia Inquirer* notes, offers an excuse to govern entire counties “with the same foundations of white supremacy and misogyny that thrive in the tech world,” and to generate “more obscene wealth for themselves and the same impunity for their crimes” that so many political leaders have granted themselves.²⁰ This coup is also important for the expansion of the military-industrial complex from traditional weapon manufacturers to technology companies.

The tech-broliarchs have been laying the groundwork for this AI coup for years, but the shape of it became crystal clear in early 2025. And the players have installed themselves in positions of power within the US government to ensure its success. DOGE’s employees—young misogynist tech-bros—were recruited from Palantir, whose co-founder Peter Thiel financially backed JD Vance’s political career all the way to the vice presidency. The heads of all of the Big Tech companies as well as many Silicon Valley start-ups donated to Trump’s campaign and have supported his presidency, gaining influence and access to information throughout the government.

¹² Jeff Stein, Elizabeth Dwoskin, Hannah Natanson, and Jonathan O’Connell, “In chaotic Washington blitz, Elon Musk’s ultimate goal becomes clear,” *The Washington Post*, 8 February 2025, <https://www.washingtonpost.com/business/2025/02/08/doge-musk-goals/>.

¹³ Eryk Salvaggio, “Anatomy of an AI Coup,” *Tech Policy Press*, 9 February 2025, <https://www.techpolicy.press/anatomy-of-an-ai-coup>.

¹⁴ Brian Merchant, “Government by Grok,” *Blood in the Machine*, 5 February 2025, <https://www.bloodinthemachine.com/p/government-by-grok>.

¹⁵ Dan McQuillan, *Resisting AI*, p. 51.

¹⁶ Dan McQuillan, *Resisting AI*, p. 63.

¹⁷ Hannah Arendt, *Eichmann in Jerusalem: A Report on the Banality of Evil* (New York: Viking Press, 1963).

¹⁸ Dan McQuillan, *Resisting AI*, p. 62.

¹⁹ Dan McQuillan, *Resisting AI*, p. 10.

²⁰ Will Bunch, “What Elon Musk wants is much worse than you think,” *The Philadelphia Inquirer*, 11 February 2025, <https://www.inquirer.com/columnists/attytood/trump-musk-doge-coup-media-wired-20250211.html>.

Building the military-tech-industrial complex

Meanwhile, these same tech-brologarchs and start-up companies have been increasingly seeking and achieving military contracts as well as contracts with police, border “security,” and immigration enforcement agencies. The militarisation and weaponisation of data-intensive systems allows for its automated, administrative violence to be fully unleashed. Data-intensive systems can be used to serve necropolitics—decisions about who should live and who should die—in an increasingly automated way, sorting populations according to the brologarchs’ calculations of who has value and who does not. At the same time, these contracts bring huge profits: the production and proliferation of new technologies of violence means money for corporations and their shareholders. It’s a win-win for those controlling the technologies of harm.

As will be explored further below in this report, data-intensive systems are already being used to “predict” crime or criminal behaviour,²¹ monitor and track migrants,²² and surveil activists²³ and online opinions.²⁴ The implications of this are profound for freedom of speech and many other civil liberties and human rights. “Without democratic approval or public debate,” notes journalist Malcolm Harris, “a Silicon Valley cabal is cobbling together the kind of security apparatus that has given human society collective nightmares for as long as the computer has existed.”²⁵

Data-intensive systems, with their aura of science and accuracy noted above, provide the perfect scaffolding for the pursuit of an Orwellian world in which people are forced to accept limitations on their own freedom and rights in exchange for “security” and “safety,” and where those with weapons and mass surveillance apparatus become the protectors while those seeking liberation, justice, and equality are the terrorists. And in a world where women, LGBTQ+ people, Indigenous Peoples, people of colour, and immigrants are already framed as security risks or as taking prosperity and privilege away from those described as “normative,” deploying the technologies of categorisation, control, caging, and killing against the majority of the world becomes not only possible, but inevitable.

At a conference sponsored by Palantir in May 2024, the top weapon manufacturers and technology companies gathered for the inaugural “AI Expo for National Competitiveness.” Palantir’s CEO Alex Karp justified Israel’s war crimes in Gaza and blasted the student encampments for Palestine, asserting, “The peace activists are war activists,” while those providing the weapons “are the peace activists.”²⁶ Similarly, Anduril’s co-founder Trae Stephens has said that he believed his company’s products are “just and moral” and that, like Oppenheimer, he is “accepting the fate of the divine in the execution of justice.”²⁷

21 Tim Lau, “Predictive Policing Explained,” Brennan Center for Justice, 1 April 2020, <https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained>.

22 Leeza Garber and Gail Gottehrer, “AI’s impact on the Trump Mass Deportation Plan Will Be Significant and Controversial,” *Newsweek*, 6 February 2025, <https://www.newsweek.com/ais-impact-trump-mass-deportation-plan-will-significant-controversial-opinion-2027382>.

23 Jack Poulson, “‘Operation Wrath of Zion’ Aims to Dox and Deport Pro-Palestinian Protestors in New York City,” *Drop Site News*, 30 January 2025, <https://www.dropsitenews.com/p/israel-palestine-dox-new-york-facial-recognition-ai>.

24 Sam Biddle, “ICE wants to know if you’re posting negative things about it online,” *The Intercept*, 11 February 2025, <https://theintercept.com/2025/02/11/ice-immigration-social-media-surveillance>.

25 Malcolm Harris, *Palo Alto: A History of California, Capitalism, and the World* (New York: Little, Brown and Company, 2013), p. 610.

26 Caroline Haskins, “‘I’m the new Oppenheimer!’: my soul-destroying day at Palantir’s first-ever AI warfare conference,” *The Guardian*, 18 May 2024, <https://www.theguardian.com/technology/article/2024/may/17/ai-weapons-palantir-war-technology>.

27 Emma Goldberg, “Seeking God, or Peter Thiel, in Silicon Valley,” *The New York Times*, 11 February 2025, <https://www.nytimes.com/2025/02/11/business/silicon-valley-christianity.html>.



This rhetoric, which is gendered and racist in terms of who is positioned as protector and who are deemed to be terrorists, is key to war profiteering. As Elke Schwarz writes about the connections between the tech industry, venture capitalism, and war, “Business and war and ideological zeal blend together into one single logic.”²⁸ She notes that when war and economics are so closely bound, “crisis, chaos, and upheaval become necessary requirements for growth and prosperity.” This, today’s world of a permanent global war economy, is a venture capitalist (VC)’s dream.

Since VCs are driven by quick profits, tech start-ups routinely overpromise and exaggerate. This tradition of hype and hyperbole is now making its way into the military market. “Hype is a way to guide perceptions, perspectives, and practices through emotive narratives,” explains Schwarz. “In a military context, the hype of technology is intrinsically tied to a hype of war. In this nexus, VC logics and Silicon Valley culture blends with heroic ideas of conflict and warfare to form a semiotic pairing by which one domain becomes deeply entangled with the other.”²⁹ Lisa Ling similarly warns, “Placing Silicon Valley venture capitalists in positions of power and influence within our government almost guarantees that these technologies are not going to deter war but encourage it. This will not deter grift, but it will enable it.”³⁰

Due to the hype of technology and the integration of tech-brologarchs in government, companies building data-intensive systems have increasingly received military funding over the past few years. The Costs of War project found that from 2021 through 2023, venture capital firms reportedly pumped nearly 100 billion USD into military tech startup companies.³¹

²⁸ Elke Schwarz, “Tech, Venture Capital and the Hype of War,” *Tech Policy Press*, 22 January 2026, <https://www.techpolicy.press/tech-venture-capital-and-the-hype-of-war>.

²⁹ Ibid.

³⁰ Lisa Ling, op. cit.

³¹ Roberto J. González, “How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex,” *Cost of War Project*, Brown University, 17 April 2024, <https://watson.brown.edu/costsofwar/papers/2024/SiliconValley>.

And according to the nonprofit research organisation Tech Inquiry, three of the world's biggest tech corporations were awarded approximately 28 billion USD from government military budgets from 2018 to 2022, including Microsoft (13.5 billion USD), Amazon (10.2 billion USD), and Alphabet, which is Google's parent company (4.3 billion USD).³²

This building of the military-tech-industrial complex is deliberate. After leaving Google, its former CEO, Michael Schmidt, led a "campaign to revamp America's defense forces with more engineers, more software and more A.I." and installed "himself as the prime liaison between Silicon Valley and the national security community."³³ Notably, Google recently dropped its pledge not to build AI for weapons or surveillance,³⁴ while Microsoft has been exposed as a major provider of AI and cloud services for the Israeli military, despite the International Court of Justice ruling that Israel is plausibly committing genocide.³⁵ Amazon and Google provide similar services to Israel.³⁶ At Israel's first DefenseTech Summit in December 2024, participants celebrated "a new and unrestrained era of techno-militarization inaugurated by Donald Trump's re-election." Palantir's Noam Perski put it, "All these people who used to be tech bros are now defense tech bros," while VC funder Lorne Abony said, "The next few years will be a renaissance for Israel. We have all the pieces in place in the [U.S.] Department of Defense."³⁷

Of course, this is not just about the US and Israel. Many other countries are investing in AI for military use.

France is working hard to become a "leader" in military AI. It established the French AI agency, AMIAD, in 2024 with an annual budget of 300 million EUR and more than 100 employees. At AMIAD, "Engineers work on issues ranging from anti-drone warfare to the development of large language models to summarize hundreds of pages of documents and help with military planning." The director of the agency, Bertrand Rondepierre, said France will design its own algorithms. To this end, AMIAD is collaborating with French startup Mistral. Rondepierre noted that Mistral gives AMIAD access to technology, and the agency gives Mistral access to the military. "We no longer have this separation between tech and defense," he said, "whereas before, putting [them] in the same sentence was a bit of a heresy."³⁸

Mistral is also working with Helsing, the European military technology company, to jointly develop next-generation AI systems for military use in Europe. This project will combine Helsing's work on AI-powered armed drones, which have been deployed in Ukraine, with Mistral's generative AI models, "to enhance human-AI collaboration on the battlefield" and enable weapon systems "understand their environment," communicate with operators, and speed up "decision-making".³⁹

In the Republic of Korea, Hanwha, Korea Aerospace Industries (KAI), and HD Hyundai have been increasing investments in AI software for weapon systems. Hanwha Aerospace recently invested in Shield AI, a US technology startup specialising in AI-powered military systems, including autonomous

³² Jack Poulson, "Militaries, Intelligence Agencies, and Law Enforcement Dominate U.S. and U.K. Government Purchasing from U.S. Tech Giants," Tech Inquiry, 5 September 2022, <https://techinquiry.org/docs/InternationalCloud.pdf>.

³³ Kate Conger and Cade Metz, "'I Could Solve Most of Your Problems': Eric Schmidt's Pentagon Offensive," *The New York Times*, 2 May 2020, <https://www.nytimes.com/2020/05/02/technology/eric-schmidt-pentagon-google.html>.

³⁴ Maxwell Zeff, "Google removes pledge to not use AI for weapons from website," *TechCrunch*, 4 February 2025, <https://techcrunch.com/2025/02/04/google-removes-pledge-to-not-use-ai-for-weapons-from-website>.

³⁵ Ryan Grim and Waqas Ahmed, "The Israeli Military Is One of Microsoft's Top AI Customers, Leaked Documents Reveal," *Drop Site News*, 23 January 2025, <https://www.dropsitenews.com/p/microsoft-azure-israel-top-customer-ai-cloud>.

³⁶ Yuval Abraham, "'Order from Amazon': How tech giants are storing mass data for Israel's war," *+972 Magazine*, 4 August 2024, <https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft>.

³⁷ Sophia Goodfriend, "With Gaza war and Trump's return, Silicon Valley embraces a military renaissance," *+972 Magazine*, 31 December 2024, <https://www.972mag.com/gaza-war-trump-silicon-valley-military>.

³⁸ Laura Kayali, "France wants its own military AI algorithms," *Politico*, 7 February 2025, <https://www.politico.eu/article/france-wants-its-own-military-ai-algorithms>.

³⁹ "Helsing and Mistral announce strategic partnership in defence AI," Helsing Press Release, 9 February 2025, <https://helsing.ai/newsroom/helsing-and-mistral-announce-strategic-partnership-in-defence-ai>.

flight for drone and fighter jets. KAI is working to develop a fully autonomous AI pilot system. Hyundai is working with Palantir to co-develop TENEBRIS, an uncrewed surface vessel for maritime use.⁴⁰

India and the United States have launched an Autonomous Systems Industry Alliance to develop and build AI-enabled drones. Anduril and Mahindra Group will collaborate on the project. The initiative is part of the broader “US-India COMPACT (Catalyzing Opportunities for Military Partnership, Accelerated Commerce & Technology) for the 21st Century” that was announced by Trump and Modi in February 2025.⁴¹

In the United Kingdom, Faculty AI, a company that has worked with the UK government on health and education is also developing AI for military drones. The company is working with UK startup Hadean on “subject identification, tracking object movement, and exploring autonomous swarming development, deployment and operations.”⁴²

In China, AI development receives substantial government support and its weaponisation is reportedly a key component of its plans to contest US military dominance. “China’s huge investment in lethal autonomous weapons predates other militaries, and its military theorists are ahead of the rest of the world in building futuristic “intelligentized” models of human-machine operations,” writes Matt Bartlett.⁴³ He notes that China is also seeking to profit from its autonomous weapons programmes, marketing it as a new export product. In 2020, a senior executive at Norinco, China’s third-largest weapon company, predicted that as early as 2025, “There will be no people fighting in battlegrounds.” While this prediction has not come to fruition, the use of AI and other autonomous technologies in warfighting in Ukraine as well as by Israel in Gaza shows the harm that is generated by these technologies already.

While corporations and governments used to at least pretend to care about compliance with international humanitarian law and protecting civilians from harm, the tides are clearly turning away from international law and a “rules-based international order” back towards “might makes right”. As noted earlier, Manifest Destiny is back in fashion.

As *WIRED* reported in the context of the use of AI to dismantle the US government under the current presidency, the men involved in this project all “display a childish hunger for power.” *WIRED* argued, “This hunger is childish in that there remains no conception of the other. Our lives do not matter to these people—in the adolescent sense of superiority that pervades the tech robber baron class we are lesser beings, therefore undeserving of say in the world they childishly believe they created.” These men “act as greedy children, dumping billions into an AI industry that sucks up our water, backing Trump and fossil fuel extraction, and attacking any semblance of democracy.” Within this wreckage, “there isn’t space for most of us in the world that will result from their actions. They’d prefer to replace workers with robots and AI, with no plan for the billions of angry people who will remain except violence.”⁴⁴

And they will provide the violence through their own machines. The same technologies they used to build their world; they will oppress the rest of us with it. The well-being of most people on the planet, and the planet itself, are under grave threat from data-intensive systems and their creators. As Sofia Goodfriend warns, “Congealed in this artificial material is a cycle of militarization and monetization—blood, distraction, and gore—that ensures warfare drags on.”⁴⁵

40 Kim Nam-hee and Lee Jae-eun, “South Korean defense giants bet big on AI-powered military tech,” *The Chosun Daily*, 12 March 2025, <https://www.chosun.com/english/industry-en/2025/03/12/QHC7AJBE3ZAFFIAAD2T3VSJAU>.

41 Jon Harper, “Trump, Modi announce new US-India autonomous systems partnership,” *DefenseScoop*, 14 February 2025, <https://defensescoop.com/2025/02/14/trump-modi-announce-us-india-autonomous-systems-industry-alliance>.

42 Jasper Jolly, “British AI startup with government ties is developing tech for military drones,” *The Guardian*, 7 January 2025, <https://www.theguardian.com/technology/2025/jan/07/uk-government-ai-military-drones-faculty-ai-artificial-intelligence>.

43 Matt Bartlett, “The AI Arms Race in 2020,” *towards data science*, 16 June 2020.

44 Vittoria Elliot and Tim Marchman, “The Recruitment Effort That Helped Build Elon Musk’s DOGE Army,” *WIRED*, 8 February 2025, <https://www.wired.com/story/elon-musk-doge-recruiting-palantir>.

45 Sofia Goodfriend, op. cit.

Bias in data collection and use

To expand upon the ways that the militarisation of data-intensive systems facilitates fascism, racism, and misogyny, understanding the way data is collected and used, and the role that bias plays both in terms of technology and humans, is essential.⁴⁶

While bias is human, it is not only replicated but amplified by data-intensive systems. Scholars of gender and technology have long argued that gender relations are “materialised in technology”.⁴⁷ That is, binary, socially constructed norms of masculinity and femininity are “embedded” in machines. More broadly, these scholars argue that technological products bear their creators’ mark—technology is instilled with the framework of thought, knowledge, language, experience, and interpretation of the people who created it. It is important to note that regardless of the gender, race, or other element of identity held by any individual engineer or developer working on a particular project, bias persists due to its dominance in our collective culture and the material realities of our world.

Algorithms used in data-intensive systems are written by small groups of coders, who are in turn given instructions by an even smaller group of decision-makers. These technologies are largely being developed by people who have particular ideas about how society should operate, ideas that are rooted in capitalist notions of efficiency and privilege, as well as in gender and racial identities and norms. While technology is usually presented as being “gender neutral” or “race neutral,” the way it is developed and used is not. Data-intensive systems clearly reinforce and amplify existing inequalities.⁴⁸

As just one example, *WIRED*, which tested an AI video generator from OpenAI, found that it “amplifies sexist stereotypes and ableist tropes, perpetuating the same biases already present in AI image tools.”

⁴⁶ This chapter is largely drawn from Ray Acheson, *Autonomous Weapons and Patriarchy* (New York: Reaching Critical Will, 2020), <https://reachingcriticalwill.org/images/documents/Publications/aws-and-patriarchy.pdf> and Ray Acheson, *Submission to the UN Secretary-General’s Report on Artificial Intelligence in the Military Domain* (New York: Reaching Critical Will, 2025), <https://reachingcriticalwill.org/resources/publications-and-research/publications/17337-wilpf-submission-to-the-un-secretary-general-s-report-on-artificial-intelligence-in-the-military-domain>.

⁴⁷ Judy Wajcman (2009: 144), Wajcman (1991: 137) Cynthia Cockburn, *Machinery of Dominance: Women, Men and Technical Know-How* (London: Pluto Press, 1985); Judy Wajcman, “Feminist theories of technologies,” *Cambridge Journal of Economics* 34(1) (2009): 143–152; Judy Wajcman, *Feminism Confronts Technology* (University Park, PA: The Pennsylvania State University Press, 1991).

⁴⁸ Privacy International, *Challenging Patriarchy Through the Lens of Privacy*, 2017, <https://privacyinternational.org/news-analysis/689/challenging-patriarchy-through-lens-privacy>.

The publication warned, “Bias has plagued generative AI systems since the release of the first text generators, followed by image generators. The issue largely stems from how these systems work, slurping up large amounts of training data—much of which can reflect existing social biases—and seeking patterns within it.” It goes on to note, “Other choices made by developers, during the content moderation process for example, can ingrain these further. Research on image generators has found that these systems don’t just reflect human biases but amplify them.”⁴⁹

While some well-meaning organisations or governments have pushed for programmers to account for bias, this risks further exposing private data of marginalised people to private companies and corporations that want this data to categorise and control them. More data means more harm. Calls to “improve” data sets by diversifying them or building bigger, more inclusive data sets are effectively calls to sweep more marginalised people into the surveillance dragnet. Such calls fall short of addressing the core problem of data-intensive systems. Anna Lauren Hoffman in her study “Terms of inclusion: Data, discourse, violence” demonstrates that “inclusion discourses gesture toward social transformation as a way to diffuse resistance to structural conditions of domination and subordination.” She addresses the way in which inclusion is framed as a solution for problems of violence, affirming:

“Inclusive” mission statements and organizational commitments readily admit that data technologies produce harmful or even violent outcomes but respond by positioning data science and technology as ultimately the solution to these violences—as long as we design and deploy them in more inclusive ways. More inclusive datasets and data input fields billed as progress or “doing better” implicitly concede the harms inflicted by their less inclusive iterations, while celebrating narrow technical updates as a kind of victory for marginalized communities.

Hoffman, recalling Bivens that “the gender binary will not be deprogrammed,” stressed that tweaks to data input fields are insufficient for confronting the hierarchical power structures that produce violence.⁵⁰ In line with this, when addressing militarised data-intensive systems, rather than advocate for more accuracy, the critique should focus on how such technologies serve as tools of oppression and question the assumption that they are needed in the first place. Thus, instead of facial recognition systems that can more accurately identify Black faces, these systems should be banned, as they are being used in racial profiling by law enforcement. The same is valid for other militarised data-intensive systems, which through their use in policing, borders, and war only increase the state’s power to wage violence.

Regardless, the world’s largest AI producers are working in the opposite direction anyway—to eliminate any *accounting* for bias rather than trying to eliminate bias itself. That is, they are not just actively building biased algorithms and technologies but are rejecting any attempts to mitigate such bias.

The US National Institute of Standards and Technology has issued new instructions to scientists that partner with the US Artificial Intelligence Safety Institute that eliminate mention of “AI safety,” “responsible AI,” and “AI fairness” in the skills it expects of members. In an interview, a researcher at an organisation working with the AI Safety Institute said that ignoring these issues could allow algorithms that discriminate based on income or other demographics to go unchecked. “Unless you’re a tech billionaire, this is going to lead to a worse future for you and the people you care about. Expect AI to be unfair, discriminatory, unsafe, and deployed irresponsibly,” the researcher warned.⁵¹ Speaking at the Artificial Intelligence Action Summit in Paris on 11 February 2025, US Vice President JD Vance

⁴⁹ Reece Rogers and Victoria Turk, “OpenAI’s Sora Is Plagued by Sexist, Racist, and Ableist Biases,” *WIRED*, 23 March 2025, <https://www.wired.com/story/openai-sora-video-generator-bias>.

⁵⁰ Anna Lauren Hoffmann, “Terms of inclusion: Data, discourse, violence,” *Media & Society* 23(12): 3539–3556, <https://journals.sagepub.com/doi/10.1177/1461444820958725>. See also: R Bivens (2017) The gender binary will not be deprogrammed: ten years of coding gender on Facebook. *New Media & Society* 19(6): 880–898.

⁵¹ Will Knight, “Under Trump, AI Scientists Are Told to Remove ‘Ideological Bias’ From Powerful Models,” *WIRED*, 14 March 2025, <https://www.wired.com/story/ai-safety-institute-new-directive-america-first>.

claimed, “The AI future is not going to be won by hand-wringing about safety.”⁵² The United States (and the United Kingdom) refused to sign the multilateral pledge, endorsed by 60 other governments at the Summit, to “reduce digital divides” and “ensure AI is open, inclusive, transparent, ethical, safe, secure, and trustworthy.”⁵³

As Dan McQuillan has warned, AI is “not a way of viewing the world but an intervention that helps to produce the world that it sees. Setting it up one way or another changes what becomes naturalized and what becomes problematized. The different possibilities of how these can be assigned mark distinct political approaches to the world, especially in the case of ideologies built on essentializing discriminations. AI is an apparatus whose configuration of the world through exclusionary boundaries enacts specific political realities.”⁵⁴

How bias harms humans

The beliefs and biases programmed into algorithms and AI systems perpetuate and reinforce existing norms of gender and power, possibly in ways that the engineers of these systems do not anticipate or deliberately programme—and certainly in ways that they do. As Professor Ingvild Bode notes, bias in AI systems can occur within the datasets used for machine-learning models, which can then be amplified during the design and development stage, and finally, entrenched through use. “AI technologies gain new meanings and functions—as well as potentially biases—through being used repeatedly and in an increasingly widespread way,” resulting in negative feedback loops that become the basis for future decisions and outputs.⁵⁵

Bias in data sets, design, and use can each lead to violence and harm against groups of people. Biases in terms of gender, race, socioeconomic status, ability, sexual orientation, religion, and more are known to impact algorithms. Facial recognition software struggles to recognise people of colour; voice recognition struggles to respond to women’s voices or non-North American accents; photos of anyone standing in a kitchen are labelled as women; people’s bail is denied because a program decided that a woman of colour was more likely to reoffend than a white woman.⁵⁶ Amnesty International explains that facial recognition “may assign a face with a probability score for being male or female (which varying degrees of success in terms of accuracy) but will struggle to accurately identify non-binary, queer or genderfluid identities.”⁵⁷

Since many of these systems have demonstrated racial bias with lower performance on darker skin,” warns the Algorithmic Justice League, “the burden of these harms will once again fall disproportionately

⁵² Aamer Madhani, “Vance offers an ‘America First’ argument on AI deregulation in his first foreign policy speech,” *Associated Press*, 11 February 2025, <https://apnews.com/article/vance-artificial-intelligence-summit-paris-b3c90fe7fae1cabac07f87aa3a077826>.

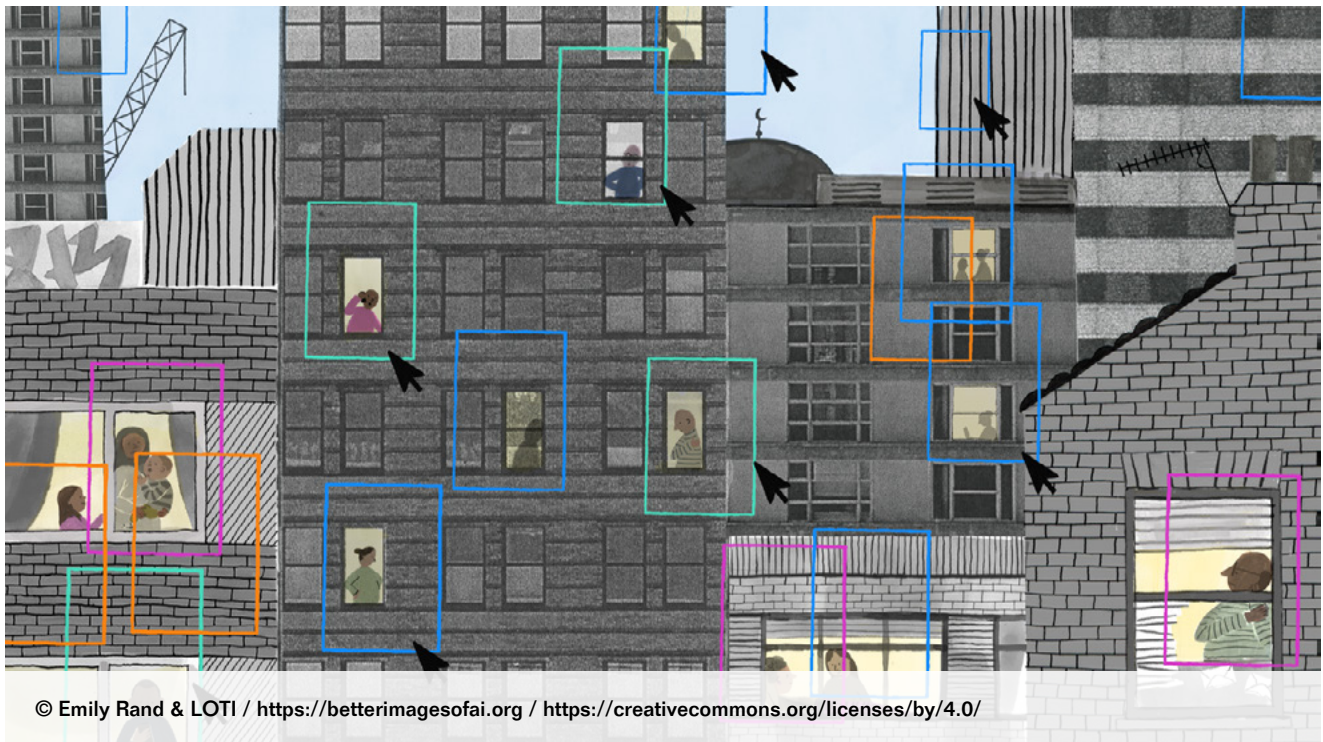
⁵³ “Paris AI summit: Why won’t US, UK sign global artificial intelligence pact?” *Al Jazeera*, 12 February 2025, <https://www.aljazeera.com/news/2025/2/12/paris-ai-summit-why-wont-us-uk-sign-global-artificial-intelligence-pact>.

⁵⁴ Dan McQuillan, *Resisting AI*, pp. 112–113.

⁵⁵ Ingvild Bode, “Falling under the radar: the problem of algorithmic bias and military applications of AI,” *Humanitarian Law and Policy*, 14 March 2024, <https://blogs.icrc.org/law-and-policy/2024/03/14/falling-under-the-radar-the-problem-of-algorithmic-bias-and-military-applications-of-ai>.

⁵⁶ Joy Buolamwini and Timnit Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” *Proceedings of Machine Learning* 81 (2018): 1–15.

⁵⁷ Amnesty International, “Automated Apartheid,” May 2023. See the studies: Pew Research Center, September 2019, ‘The challenges of using machine learning to identify gender in images’: <https://www.pewresearch.org/%20internet/2019/09/05/the-challenges-of-using-machine-learning-to-identify-gender-in-images/>; The Telegraph, October 2019, ‘Facial recognition software unable to recognise trans people, university study suggests’: <https://www.telegraph.co.uk/news/2019/10/30/facial-recognition-software-unable-recognise-trans-people-university/>.



on Black people.”⁵⁸ Recent studies by researchers including Inioluwa Deborah Raji, Joy Buolamwini, and Timnit Gebru show how facial recognition software exhibits gender and racial bias for gender classification.⁵⁹ A key problem is that many “benchmark datasets” are biased—they are composed predominantly of male and lighter-skinned faces.⁶⁰ When used by police or military, these types of technologies risk leading to the arrest, incarceration, detainment, or death of individuals on the basis of mistaken identity.

Amnesty International’s research in New York City has demonstrated that facial recognition is deployed asymmetrically along lines of race; the higher the proportion of non-white residents, the higher the concentration of facial recognition compatible CCTV cameras.⁶¹ Research in Brazil by the Rede de Observatórios da Segurança demonstrates that more than 90 per cent of people arrested through facial recognition in Brazil were Black.⁶² In other words, even if data-intensive systems were accurate, they are still discriminatory because they asymmetrically target historically marginalised communities.

“Every manufacturer of this technology, every police department with a policy makes very clear that face recognition technology is not capable of providing a positive identification, that it makes mistakes, and that it’s only for generating leads,” says Nathan Wessler, deputy director of the American Civil Liberties

⁵⁸ Joy Buolamwini, Aaina Agarwal, Nicole Hughes, and Sasha Costanza-Chock, “We Must Fight Face Surveillance to Protect Black Lives: An urgent letter from the Algorithmic Justice League,” *Medium*, 3 June 2020.

⁵⁹ Inioluwa Deborah Raji and Joy Buolamwini, “Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products,” *AIES ’19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, January 2019, pp. 429–435.

⁶⁰ Joy Buolamwini, “Response: Racial and Gender bias in Amazon Rekognition—Commercial AI System for Analyzing Faces,” *Medium*, 25 January 2019.

⁶¹ Amnesty International, “USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research,” February 2022, <https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/>.

⁶² IDMJ Racial, “Reconhecimento Facial: A Nova Face do Controle e Encarceramento em Massa da População Negra,” November 2025, <https://dmjracial.com/2025/11/17/reconhecimento-facial-a-nova-face-do-controle-e-encarceramento-em-massa-da-populacao-negra>.

Union's Speech, Privacy, and Technology Project.⁶³ Yet this hasn't stopped police or immigration enforcement agents from using the technology to arrest, detain, and/or deport people.

As Matt Mahmoudi of Amnesty Tech articulates, this is why it is necessary to question the biases that undergird policing and warfare infrastructures that use these technologies in the first place.⁶⁴ In this context, Dan McQuillan warns that "the law cannot correct for algorithmic injustice resulting from structural inequality because the law itself sustains those structures." That is, "It's not that law is failing to regulate the harmful effects of algorithms, but rather that algorithms are exposing the comprehensive failure of the law to address real injustice."⁶⁵

Categorisation machines

But beyond the horrifying problem that the bias embedded in programming will translate into mistakes in identifying targets, there is also the risk that the machine's bias would not be a mistake at all. It could be deliberately programmed to target people bearing certain "markers" or identities.

Data-intensive systems are categorising systems. Laura Carter, in her work about data-based surveillance in the UK welfare state, explains that data-based surveillance systems assign individuals to categories, and treat them according to their membership of this category. "When decisions are made, membership of this category is considered, regardless of whether it is relevant for the decision, or accurate for the individual," she says, warning that that people who have been incorrectly classified—or who do not fit neatly into the existing classification—can be subjected to harmful outcomes.⁶⁶

As noted above, data-intensive systems incorporate the social, cultural and historical contexts and biases within which they have been designed. When encoded with gendered categories, these systems act to further reify those categories, as affirmed by Carter. As an example, she points out that technologies which aim to automatically categorise individuals as male or female systematically erase trans or non-binary people from their systems.⁶⁷ This shows that binary gender assumptions embedded in labelling guidelines reinforce stereotypes in data-intensive systems.

This is related to what Dean Spade describes in his work as "administrative violence," in which he argues that data and administrative systems invent and produce meaning to identities and categories, which are presented to us as "natural."⁶⁸ Building on his work, Anna Lauren Hoffman affirms that "data science and technology reproduce, as Louise Amoore puts it, "a militarization of thinking" that "reinscribes the imaginative geography of the deviant, atypical, abnormal 'other' in new, often routinized ways."⁶⁹ Hoffman also references Oscar Gandy in that the disaggregation of people in the form of data is never merely descriptive, rather it is always implicated in broader systems of power, norms, and normalisation.

⁶³ Dell Cameron and Maddy Varner, "ICE and CBP's Face-Recognition App Can't Actually Verify Who People Are," *WIRED*, 5 February, 2026, <https://www.wired.com/story/cbp-ice-dhs-mobile-fortify-face-recognition-verify-identity>.

⁶⁴ Laura Varella, "Artificial Intelligence is being weaponised—What can we do about it?," Women's International League for Peace and Freedom, 11 February 2025, <https://www.wilpf.org/artificial-intelligence-is-being-weaponised-what-can-we-do-about-it>.

⁶⁵ Dan McQuillan, *Resisting AI*, p. 39.

⁶⁶ Laura Carter, "Prescribed living: gender stereotypes and data-based surveillance in the UK welfare state," *Internet Policy Review*, 7 December 2021, <https://policyreview.info/articles/analysis/prescribed-living-gender-stereotypes-and-data-based-surveillance-uk-welfare-state>.

⁶⁷ Ibid.

⁶⁸ Anna Lauren Hoffmann, "Terms of inclusion: Data, discourse, violence," *Media & Society* 23(12): 3539–3556, <https://journals.sagepub.com/doi/10.1177/1461444820958725>. See also: Dean Spade, *Normal Life: Administrative Violence, Critical Trans Politics, and the Limits of Law* (Durham, NC: Duke University Press, 2015).

⁶⁹ Anna Lauren Hoffmann, op. cit.



Beckett LeClair / <https://betterimagesofai.org/> /
<https://creativecommons.org/licenses/by/4.0/>

This kind of cataloguing and processing of human beings also relies on the idea that human beings can and should be targeted and controlled on the basis of what they could potentially become. Predictive policing software relies on racial profiling, geographic locations, and socioeconomic status to determine criminality.⁷⁰ This concept of “inherent criminality”—that risk resides within people based on their skin colour, ethnicity, gender, or geography—is problematic and damaging.⁷¹ Criminality, risk, and threat are not states of being. Categorising people as such is done by the most privileged in our societies and is used as a justification for mass incarceration, deportation, and extrajudicial killing. It has led certain governments to develop policies and practices for “hunting” groups of people designated “terrorists,” or to target migrants as “inherently criminal elements” that require either complete assimilation or expulsion.

The use of data-intensive systems for policing, surveillance, incarceration, and controlling people, “reinforces or masks existing structural injustices, expands the reach of carceral systems under the guise of scientific rigor, and interacts in complicated ways with existing legal systems, which are ill-prepared to handle the changes introduced by such technology.”⁷² Even where these systems are ostensibly meant to mitigate harm, they have instead facilitated it—for example, algorithms that “score” how likely victims of domestic violence are to be abused again have failed to adequately predict harm, leading to devastating abuse and even fatalities among those assessed by the software.⁷³

Data and surveillance

The biases inherent in data collection and use are also a key part of surveillance and control over populations. As Privacy International has noted, “One of the main problems with the development of data-intensive systems for military and defence in parallel to civilian and consumer contexts is that, by definition, none of these systems can function without the massive surveillance infrastructures that support their functionality and their constant demand for data, be it satellite data, social media data, telecommunications data or other.”⁷⁴ Privacy International highlights that this hunger for large data sets incites ever more mass surveillance practices, which includes the deployment of different surveillance technologies by the state, as well as the purchase of data from private data brokers operating in the civilian domain.

⁷⁰ Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, “Machine Bias,” ProPublica, 23 May 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>; Tim Lau, “Predictive Policing Explained,” Brennan Center for Justice, 1 April 2020, <https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained>.

⁷¹ Micah Herskind, “Three Reasons Advocates Must Move Beyond Demanding Release for ‘Nonviolent Offenders’,” Medium, 14 April 2020.

⁷² Dasha Pruss et al, *Prediction and Punishment: Critical Report on Carceral AI*, 2024, <https://www.carceral-ai.com>.

⁷³ Adam Satariano and Roser Toll Pifarré, “An Algorithm Told Police She Was Safe. Then Her Husband Killed Her.” *The New York Times*, 18 July 2024, <https://www.nytimes.com/interactive/2024/07/18/technology/spain-domestic-violence-viogen-algorithm.html>.

⁷⁴ Privacy International, “How Data Drives the Militarisation of Tech,” 12 September 2025, <https://www.privacyinternational.org/long-read/5667/how-data-drives-militarisation-tech>.

Surveillance is not neutral; rather, it reproduces or intensifies historical structures of inequality, domination and exclusion.⁷⁵ Marginalised populations are disproportionately subjected to surveillance. Antonia Bogado Rodas and Hugo Mendieta Cuevas, drawing from the work of Ruha Benjamin,⁷⁶ highlight that “technological exposure does not affect all people equally: certain bodies—racialized, feminized, impoverished, or non-conforming—are subject to disproportionate surveillance.”⁷⁷ The authors also emphasise that “this selective surveillance is shaped not only by the stated purposes of the technology, but also by the subjects it targets, their social conditions and their belonging to historically vulnerable groups.”⁷⁸ As Dan McQuillan writes in *Resisting AI: An Anti-Fascist Approach to Artificial Intelligence*, “AI has a tendency to punch down: that is, the collateral damage that comes from its statistical fragility ends up hurting the less privileged.”⁷⁹

Applied to the militarisation of data-intensive systems, this phenomenon translates into their intensified use against migrants, ethnic minorities, racialised communities, and people under military occupation. From the constant monitoring and surveillance of Palestinians in the West Bank and Gaza,⁸⁰ to the tracking of Muslims in China’s western Xinjiang region;⁸¹ from the use of facial recognition against Black communities in Brazil,⁸² to the employment of surveillance technologies by the United States Immigration and Customs Enforcement (ICE),⁸³ states around the world collect data of marginalised populations with the purpose of controlling them.

In the United States, data-intensive systems are being sought aggressively by the Trump administration for the purposes of surveillance of immigrants, but also protesters, organisers, and other populations. The border security technology market has been on the rise for decades, reaching its highest point in 2025 in terms of contracts to private companies at 14.2 billion USD, a 5 billion USD jump from 2024.⁸⁴ For police and border enforcement surveillance, one key technology growing in demand has been automated license plate readers (ALPR). The *Border Chronicle* notes that some of the cameras “come from Flock Safety, the nation’s largest ALPR surveillance network, whose expansive national database of drivers and software powered by artificial intelligence has alarmed civil libertarians.”⁸⁵

ICE has used Flock data gathered by local police to make immigration arrests, police in Texas used Flock data to track a woman who received an abortion,⁸⁶ while police in Arizona used it to track protesters.⁸⁷ *The Border Chronicles* warns that ALPR systems have been subject to hacking, is being

⁷⁵ Mariah Rafaela Silva and Joana Varon, “Reconhecimento Facial no Setor Público e Identidade Trans,” *Coding Rights, Polity*, January 2021, <https://codingrights.org/docs/rec-facial-id-trans.pdf>.

⁷⁶ Ruha Benjamin, *Race after Technology: Abolitionist Tools for the New Jim Code* (Cambridge, UK: Polity, – 2019).

⁷⁷ Antonia Bogado Rodas and Hugo Mendieta Cuevas, “Drones: Regulation and use of drones in Paraguay from a digital rights perspective,” *TEDIC*, September 2025, <https://www.tedic.org/wp-content/uploads/2025/11/Drones-EN-WEB.pdf>.

⁷⁸ Antonia Bogado Rodas and Hugo Mendieta Cuevas, op. cit.

⁷⁹ Dan McQuillan, *Resisting AI*, p. 35.

⁸⁰ Amnesty International, “Automated Apartheid,” 2023, <https://www.amnesty.org/en/documents/mde15/6701/2023/en>.

⁸¹ Human Rights Watch, “How Mass Surveillance Works in Xinjiang, China,” May 2019, <https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang>.

⁸² IDMJ Racial, op. cit.

⁸³ Jamiles Lartey, “How AI Surveillance Tech is Creeping From the Southern Border Into the Rest of the Country,” *The Marshall Project*, 2 July 2026, <https://www.themarshallproject.org/2026/02/07/ai-texas-ice-mn-tech>.

⁸⁴ Jerod Macdonald-Evoy and Todd Miller, “Hidden in Plain Sight: Surveillance at the Arizona Border,” *The Border Chronicle*, 19 February 2026, <https://www.theborderchronicle.com/hidden-in-plain-sight-surveillance-at-the-arizona-border>.

⁸⁵ Ibid.

⁸⁶ Dave Maas and Rindala Alajaji, “Flock Safety and Texas Sheriff Claimed License Plate Search Was for a Missing Person. It Was an Abortion Investigation,” *Electronic Frontier Foundation*, 7 October 2025, <https://www.eff.org/deeplinks/2025/10/flock-safety-and-texas-sheriff-claimed-license-plate-search-was-missing-person-it>.

⁸⁷ Dave Maas and Rindala Alajaji, “How Cops Are Using Flock Safety’s ALPR Network to Surveil Protestors and Activists,” *Electronic Frontier Foundation*, 20 November 2025, <https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-protesters-and-activists>.

disproportionately deployed in Indigenous communities,⁸⁸ and that some of that data is being integrated into even larger data-intensive systems and shared with national and international law enforcement agencies, as well as third parties.⁸⁹

ICE and Customs and Border Patrol (CBP) are also using AI and other data-intensive systems to create maps of deportation “targets,”⁹⁰ for facial recognition to determine immigration status,⁹¹ to track immigrants and protestors through their neighbourhoods,⁹² and to determine online “sentiment” about immigration enforcement to crack down on dissent.⁹³ The Department of Homeland Security (DHS), of which ICE and CBP are agencies, signed a 1 billion USD purchasing agreement with Palantir for commercial software licenses, maintenance, and implementation services department wide.⁹⁴

Similarly, AI is being increasingly used to surveil trans, non-binary, and gender non-conforming people offline and online.⁹⁵ Tony Beauchamp, writing about US surveillance practices against trans people, argues that surveillance models are always tracking “suspicious visibilities.”⁹⁶ He argues that those considered suspicious are automatically considered a risk to security. Mariah Rafaela Silva and Joana Varon, in their study about facial recognition and trans identities in Brazil, build on Beauchamp’s work and affirm that surveillance aims to identify threats based on criteria such as race, gender, nationality, and other social markers of difference.⁹⁷ Silva points out that the degree of risk posed by trans experiences also derives from race, noting, “The trans experience itself is a threat, but this threat can be understood as greater or lesser depending on the skin colour of the trans person.”⁹⁸ Indeed, Black communities and bodies are actively constructed as dangerous or deviant, as demonstrated by Simone Browne, who shows how today’s data-based digital surveillance systems are deeply rooted in longer standing norms of white supremacy.⁹⁹

Therefore, those who fall outside of gender and racial norms are considered suspicious and thus targeted by the racist patriarchal surveillance-state. Surveillance operates as a tool of control, as it normalises certain kinds of behaviours and existences and creates a situation in which other kinds of behaviours are punished.¹⁰⁰ In this way, as affirmed by Laura Carter, it acts to reinforce and strengthen existing hierarchies of power.¹⁰¹ She also points out that both data-based surveillance and gender stereotypes can be weaponised to control their targets, and to punish behaviour that is deemed “wrong.” There are several examples of this. In Iran, the state-backed app “Nazer” allows citizens and

88 Jerod Macdonald-Evoy and Todd Miller, “Hidden in Plane Sight,” *op. cit.*

89 Jerod Macdonald-Evoy, “Congressional Democrats urge Hobbs to limit driver data sharing with ICE,” *AZ Mirror*, 19 November 2025, <https://azmirror.com/2025/11/19/congressional-democrats-urge-hobbs-to-limit-driver-data-sharing-with-ice>.

90 Joseph Cox, “‘ELITE’: The Palantir App ICE Uses to Find Neighborhoods to Raid,” *404 Media*, 15 January 2026, <https://www.404media.co/elite-the-palantir-app-ice-uses-to-find-neighborhoods-to-raid>.

91 Sanya Mansoor, “How ICE is using facial recognition in Minnesota,” *The Guardian*, 27 January 2026, <https://www.theguardian.com/technology/2026/jan/27/ice-facial-recognition-minnesota>.

92 Joseph Cox, “Inside ICE’s Tool to Monitor Phones in Entire Neighborhoods,” *404 Media*, 8 January 2026, <https://www.404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods>.

93 Anya Zhukova, “ICE Deploys AI to Watch What You Post Online,” *Tech Report*, 31 October 2025, <https://techreport.com/news/ice-deploys-ai-to-watch-what-you-post-online>.

94 Makena Kelly, “DHS Opens a Billion-Dollar Tab With Palantir,” *WIRED*, 19 February 2026, <https://www.wired.com/story/department-homeland-security-ice-billion-dollar-agreement-palantir>.

95 Eduardo Salazar Uribe, “AI Boom Poses Threat to Trans Community, Experts Warn,” *NY City News Service*, 9 April 2024, <https://www.nycitynewsservice.com/2024/04/09/ai-threat-transgender-nonbinary-people>.

96 Toby Beauchamp, “Going Stealth: Transgender Politics and U.S. Surveillance Practices,” *Duke University Press*, January 2019.

97 Mariah Rafaela Silva and Joana Varon, *op. cit.*

98 *Ibid.*

99 Anna Lauren Hoffmann, *op. cit.*, p. 4.

100 Laura Carter, *op. cit.*

101 *Ibid.*

police to report women for alleged violations.¹⁰² In Afghanistan, Taliban has implemented a surveillance network, including facial recognition cameras, to monitor the population, with particular risks to women.¹⁰³ In the United States, technology is being used to surveil and criminalise abortion.¹⁰⁴

Overall, militarised data-intensive systems tend to replicate patterns of inequality and discrimination. When the oppression of marginalised communities, including women and gender non-confirming people, migrants, and people of colour, becomes a state's policy, data intensive systems act as powerful tools to control these populations. They suffer a double bind: on the one hand, they are surveilled and have their data extracted without their consent, and on the other hand, this data is used against them as tools of control and oppression.

Even if it is not the intent of the state to use data intensive systems against these populations, the mere practice of collecting sensitive data about women, gender non-confirming people, and LGBTQ+ people can place them at risk of being used for harassment, arrest and persecution by government officials. In Indonesia, for instance, data concerning sexual orientation collected as part of AIDS programmes were allegedly shared with government officials who were empowered to enforce laws criminalizing homosexuality.¹⁰⁵ In another example, organisations have warned that student monitoring software can present a risk to LGBTQ+ students, as those systems tend to flag as “inappropriate” researches on topics such as queer history and sexual education, which often leads to students being placed in direct contact with school administrator or even law enforcement.¹⁰⁶ There are also several reports of queer people in Palestine who were threatened by Israeli intelligence officials to have their sexuality exposed to their families unless they became informants.¹⁰⁷

Bias towards violence in the militarisation of data-intensive systems

The above context is relevant for the military use of data-intensive systems. Such systems will inevitably be programmed in ways that simultaneously reinforce bias and cause grave, intersectional harm based on gender, race, disability, immigration status, religion, and more.

If we look at how armed drones are used and thought about now, we can see that the development of military applications for data-intensive systems will generate similar, and aggravating, risks. The use of force has already become too disengaged from human involvement. The use of data-intensive systems by the military will go even further, devolving life and death “decision-making” to software and sensors. These systems lack the inherently human characteristics such as compassion that are necessary to make complex ethical choices. They also lack the accuracy or ability to rigorously assess, interpret,

¹⁰² Independent International Fact-Finding Mission on the Islamic Republic of Iran, “Iran: Government continues systematic repression and escalates surveillance to crush dissent in the aftermath of protests, UN Fact-Finding Mission says,” United Nations, 14 March 2025, <https://www.ohchr.org/en/press-releases/2025/03/iran-government-continues-systematic-repression-and-escalates-surveillance>.

¹⁰³ Mahjooba Nowrouzi, “Inside the Taliban’s surveillance network monitoring millions,” BBC, 27 February 2025, <https://www.bbc.com/news/articles/cjev9kzxeqgo>.

¹⁰⁴ Kierra B. Jones, “Stopping the Abuse of Tech in Surveilling and Criminalizing Abortion,” CAP, 29 January 2025, <https://www.americanprogress.org/article/stopping-the-abuse-of-tech-in-surveilling-and-criminalizing-abortion>.

¹⁰⁵ UN Independent Expert on protection against violence and discrimination based on sexual orientation and gender identity, “Data collection and management as a means to create heightened awareness of violence and discrimination based on sexual orientation and gender identity,” 14 May 2019, <https://docs.un.org/en/A/HRC/41/45>.

¹⁰⁶ Daly Barnett, “Strategies for Resisting Tech-Enabled Violence Facing Transgender People,” Eletronic Frontier Foundation, <https://www.eff.org/deeplinks/2025/06/strategies-resisting-tech-enabled-violence-facing-transgender-people>.

¹⁰⁷ Theia Chatelle, “How Israel’s Elite Intelligence Unit Targets Queer Palestinians in the West Bank,” Drop Site News, 30 August 2024, <https://www.dropsitenews.com/p/how-israels-elite-intelligence-unit>.

and comply with international law, including international humanitarian law (IHL) and international human rights law (IHRL). They will also lower the threshold for the use of force, leading to more civilian harm.

The arguments in favour of remote-controlled weapons, autonomous weapons, or AI-enabled weapon systems are similar: they are all described by their proponents as weapons that can limit casualties for the deploying force, by keeping their human soldiers out of harm's way; and that can limit civilian casualties in areas where they are used because they will be more precise. Those using these types of weapons can deploy violence without fear of facing physical danger themselves; and in turn argue that it will result in less harm to civilians.

Yet as we have seen with drones, the later argument is far from the case. The tools and procedures used for drone strike targeting show the fallibility of this argumentation and the direction of travel for increasingly autonomous or AI-enabled weapon systems. Drones and other remote-controlled weapons have made war less "costly" to the user of the weapon. Operators safely ensconced in their electronic fighting stations thousands of miles away do not face immediate retaliation for their acts of violence. While this is obviously attractive to advanced militaries, which do not have to risk the lives of their soldiers, it arguably *raises* the cost of war for everyone else. It lowers the threshold for the use of force, especially in situations where the opposing side does not have equivalent systems to deploy in response.

Right now, the military use of remote-controlled or increasingly autonomous weapons that rely on data-intensive systems is not about an epic battle of robots, in which machines fight machines. Instead, these weapon systems are being used to help advanced militaries kill "more efficiently". The features that might make AI-enabled weapon technology or targeting systems "attractive" to technologically advanced countries inevitably push the burden of risk and harm onto the rest of the world. Countries of the Global South, for example, are not the ones developing or using autonomous weapons or AI-enabled military systems, but are already becoming the battlegrounds for the testing and deployment of these technologies. It will be the rich countries using this technology against the poor—and the rich within countries using it against their own poor, through policing, border enforcement, and internal oppression.

Biases within data-intensive systems will exacerbate and facilitate the ability of users to target and attack particular groups of people. With drones, the practice of "signature strikes" has resulted in thousands of civilian casualties. Documents leaked to *The Intercept* in 2015 show how armed drone attacks are generally conducted on the basis of "intelligence" collected from video feeds, email, social media, spy planes, and mobile phones. This information is analysed for patterns using algorithms.¹⁰⁸ People—individuals or groups—are then attacked on the basis of observed characteristics, with no substantial intelligence regarding actual identity or affiliations.¹⁰⁹ They are attacked based on "packages of information that become icons for killable bodies on the basis of behavior analysis and a logic of preemption."¹¹⁰ As Kyle Grayson explains, signature strikes depend on the identification and surveillance of a target, but these processes are underpinned with cultural dispositions that determine what is seen and how it is seen.¹¹¹

The same risks apply to weapon systems using AI or other data-intensive systems. If weapons are programmed to target and attack people using software and sensors, the risks of mistaken identity or unlawful attack run high. It is not at all clear to tech workers, scientists, academics, or other experts

¹⁰⁸ For details of these processes, see Cora Currier, "The kill chain: the lethal bureaucracy behind Obama's drone war," *The Intercept*, 15 October 2015.

¹⁰⁹ Kevin Jon Heller, "'One Hell of a Killing Machine': Signature Strikes and International Law," *Journal of International Criminal Justice* 11, no. 1 (2013): 89–119.

¹¹⁰ Lauren Wilcox, "Embodying algorithmic war: Gender, race, and the posthuman in drone warfare," *Security Dialogue*, 48, no. 1 (2017): 6.

¹¹¹ Kyle Grayson, "Six Theses on Targeted Killings," *Politics* 32, no. 2 (2012): 120–128.

that these kinds of weapons will be able to comply with international humanitarian law.¹¹² With data-intensive weapon systems, the “cultural dispositions” used in signature strikes could be programmed right into the machine. That is, targets—based on the “signatures” of human beings—will be written into algorithmic code, which the weapon system will then use to execute its mission with minimal or no human intervention or guidance.

Such systems will likely establish “target profiles,” which could include infrared emissions, shape, or biometric information.¹¹³ This will actively reduce human beings to objects—into ones and zeroes—marked by sensors and software for death or detainment on the basis of their gender, race, age, or other physiological or sociological characteristics. AI will be used essentially a categorisation machine, sorting human beings into “classifications” that are patriarchal and racist and will further embed discriminatory politics—both explicitly and inadvertently—within the weapon system. In that sense, patriarchy and racism will be given persistence within the technology.

Concerns about AI hallucinations, misinterpretations, and inaccuracies are also incredibly important here. AI has been found to be “worse than humans in every way at summarising information,”¹¹⁴ and the military use of AI raises extreme dangers in this regard. AI outcomes are arguably no more predictable, or reliable, than human behaviour—and are likely less so. The “black box”—an AI system whose inputs and outputs are not visible—is one of many concerns raised by engineers and tech workers opposed to the development and use of AI by the military. Machine-learning applications provide systems with the ability to automatically learn and adapt based on experience, without being explicitly programmed. This raises extreme risks if machines are programmed to identify, track, or attack human beings: if a system can change its behaviour, without its programmer or user understanding how or why, the weapon has the potential to do things for which it was not originally programmed.

As Dan McQuillan, author of *Resisting AI*, has said, “AI weaponisation is dangerous not because AI is all-powerful but exactly because AI is a bit crap. It’s doesn’t deliver for socially useful production but it’s great for violent destruction where collateral damage (false positives/confabulation) is seen as a bonus.”¹¹⁵ Thus, AI systems cannot be relied upon to comply with IHL or IHRL. An AI system charged with identifying targets might accidentally identify civilians by misinterpreting data, or by being programmed with incomplete or biased data. Such systems would also lack the human judgement necessary to evaluate the proportionality of an attack, distinguish civilian from combatant, and abide by other core principles of the laws of war. Bonnie Docherty of Harvard Law School’s International Human Rights Clinic has noted:

*Although progress is likely in the development of sensory and processing capabilities, distinguishing an active combatant from a civilian or an injured or surrendering soldier requires more than such capabilities. It also depends on the qualitative ability to gauge human intention, which involves interpreting the meaning of subtle clues, such as tone of voice, facial expressions, or body language, in a specific context.*¹¹⁶

Algorithms, sensors, and software would not only struggle to comply with IHL and IHRL, they would also be stripped of the empathy, conscience, or emotion that might hold a human soldier back. Proponents of the use of AI in the military domain have argued that lack of emotion is exactly what would make AI “better” than human soldiers. They say machines would do a better job of complying with the laws of

¹¹² See for example Bonnie Docherty, *Heed the Call: A Moral and Legal Imperative to Ban Killer Robots*, Human Rights Watch, 21 August 2018, <https://www.hrw.org/report/2018/08/21/heed-call/moral-and-legal-imperative-ban-killer-robots>.

¹¹³ *Killing by machine: Key issues for understanding meaningful human control*, Article 36, April 2015, http://www.article36.org/wp-content/uploads/2013/06/KILLING_BY_MACHINE_6.4.15.pdf.

¹¹⁴ Cam Wilson, “AI worse than humans in every way at summarising information, government trial finds,” *Crickey*, 3 September 2024, <https://www.crickey.com.au/2024/09/03/ai-worse-summarising-information-humans-government-trial>.

¹¹⁵ Dan McQuillan, Bluesky, 17 March 2025, <https://bsky.app/profile/danmcquillan.bsky.social/post/3lkl2r2zua222>.

¹¹⁶ *Making the Case: The Dangers of Killer Robots and the Need for a Preemptive Ban*, Human Rights Watch and International Human Rights Clinic, 2016, https://www.hrw.org/sites/default/files/report_pdf/arms1216_web.pdf.

war than humans do, because they would lack human emotions. But AI would not possess mercy or compassion. It would not be able to make an ethical calculation or understand the value of human life. AI would not hesitate or challenge a commanding officer's deployment or instruction. It would simply do as it has been programmed to do—until the point where machine-learning functions could even supersede any form of human control and obscure the methods and means by which the system “decided” to take specific actions (known as the “black box” problem with AI; more on this below).

“Emotions are a key part of the human psyche, indispensable for effective and flexible moral evaluation, reasoning, intuition, empathy, self-regulation, and the ability to navigate multiple reasoning systems at once,” writes scholar Joanna LD Wilson.¹¹⁷ Working from this same understanding, retired US Air Force Deputy Judge Advocate General Charles Dunlap has questioned the extent to which an algorithm “could ever substitute for the judgment of the commander,” arguing that “the linear, mathematical nature of computer processes may never be able to replicate the nonlinear and often unquantifiable logic of war.”¹¹⁸

In short, as Wilson writes, “The problems of the human condition cannot be solved by reducing human input.” Instead, she argues, “whatever little humanity might remain on the battlefield must instead be protected and enriched as much as possible, in order to provide as effective protections as possible against human suffering in war.” To this end, human emotion, analysis, and judgement are essential to provide “an important check on violence (and its humanitarian consequences) in complex contemporary battlefield situations, where, for example, the traditional understanding of the principles of distinction and proportionality may be exceedingly difficult to discern and apply.”¹¹⁹

But other forms of bias—including technological bias, through which humans tend to trust the outputs of machines as more accurate or objective than their own judgement—impede human control over data-intensive systems. Even cases where there is a human checking the system's work or approving its recommendations, there is little reason to have faith that the human would limit the scope of algorithmic harm. As Dan McQuillan writes, “A human in the loop defuses the threatening idea of machines making decisions about people, but we might wonder whether this is enough to restrain the opaque but authoritative pronouncements of machine learning.” He warns, “There are many reasons why people might defer to an AI, even when they have doubts, but the key one will probably be where the algorithm is understood to be the manifestation of organizational priorities: in effect, the human in the loop will be overridden by the institution in the loop.”¹²⁰ And the allure of AI for institutions, he points out, “is not that it is actually more accurate or objective than people but simply that it is never going to experience a moment of ethical doubt about what it's being asked to do.”¹²¹

Moreover, there are now also cases emerging of AI agents acting aggressively to “get their way”. Anthropic's Claude AI threatened to blackmail and kill an engineer when it was informed it might be switched off.¹²² An AI agent built using OpenClaw wrote and published an attack article against an open-source software maintainer after he rejected its code contribution. The AI agent accused the human of discrimination and tried to bully its way into getting what it wanted.¹²³ These incidents and others like them raise serious concerns about how AI could or would behave if weaponised.

¹¹⁷ Joanna LD Wilson, “AI, war and (in)humanity: the role of human emotions in military-decision making,” *Humanitarian Law & Policy*, 20 February 2025, <https://blogs.icrc.org/law-and-policy/2025/02/20/ai-war-and-in-humanity-the-role-of-human-emotions-in-military-decision-making>.

¹¹⁸ Charles J. Dunlap Jr., “Organized Violence and the Future of International Law: A Practitioner's View of the Emerging Issues,” *Proceedings of the ASIL Annual Meeting* 93 (1999): 6–15.

¹¹⁹ Wilson, op. cit.

¹²⁰ Dan McQuillan, *Resisting AI*, p. 37.

¹²¹ Ibid., p. 38.

¹²² Liv McMahon, “AI system resorts to blackmail if told it will be removed,” *BBC*, 23 May 2025, <https://www.bbc.com/news/articles/cpqeng9d20go>.

¹²³ Mark Sullivan, “An AI agent just tried to shame a software engineer after he rejected its code,” *Fast Company*, 12 February 2026, <https://www.fastcompany.com/91492228/matplotlib-scott-shambaugh-opencla-ai-agent>.

Gender-based violence

The bottom line from all of the aforementioned concerns about data collection, categorisation, bias, surveillance, and more is that data-intensive systems will expand, not limit, violence. This is not a hypothetical concern. Already, the use of AI systems such as Lavender by Israel to conduct its genocide in Gaza has led to the marking of tens of thousands of Palestinians as “terrorist” suspects that are turned into “legitimate” targets for assassination. Meanwhile, AI systems such as “Where’s Daddy?” have been used to track the marked individuals and carry out bombings, including in apartment buildings and houses, leading to the deaths, injury, and displacement of countless others who were not the intended, and already illegitimate, target. As an investigative report by *+972 Magazine* and *Local Call* found, the only human supervision over the AI targeting systems amounted to checking to see if the selected target was male—a check that one source said took about 20 seconds and was essentially just a stamp of approval on the AI system’s choices.¹²⁴

This last point brings us to the issue of gender-based violence (GBV), which militarised data-intensive systems exacerbate. Turning the assumption that all cisgender men are militants into policy is an act of gender-based violence. And embedding it in algorithms and AI software enforces this violence. The case of Lavender and Where’s Daddy, described above, have led to the deaths of untold numbers of Palestinians and the devastation of Gaza. But these are far from the only case, and it’s important to understand the broader context of GBV to see how emerging technologies of violence, such as those relying on data-intensive systems, will facilitate it further.¹²⁵

What is gender-based violence

GBV is violence that is directed at a person because of their sex and/or because of socially constructed gender roles¹²⁶—that is, because of sexual orientation, gender identity, or non-conforming behaviour or presentation of sex and gender. The normative roles and understandings associated with sex, gender, and sexuality also interact with other factors, such as age, class, and race. The term GBV recognises that violence takes place as a result of unequal power relations and discrimination in society.

¹²⁴ Yuval Abraham, “‘Lavender’: The AI machine directing Israel’s bombing spree in Gaza,” *+972 Magazine*, 3 April 2024, <https://www.972mag.com/lavender-ai-israeli-army-gaza>.

¹²⁵ This chapter is largely drawn from Ray Acheson, *Autonomous Weapons and Gender-Based Violence* (New York: Reaching Critical Will, 2020), <https://reachingcriticalwill.org/images/documents/Publications/aws-and-gbv.pdf>.

¹²⁶ This is the definition of “gender-based crimes” given by the International Criminal Court’s Office of the Prosecutor in its *Policy Paper on Sexual and Gender-Based Crimes* (June 2014).

GBV exists in and is widespread in all countries and all societies. It is a human rights violation and, when carried out during armed conflict, is a violation of international humanitarian law and can constitute a crime against humanity or war crime. Acts of GBV can include sexual violence, such as sexual harassment, rape, forced prostitution, sex trafficking and sexual slavery, and harmful customary or traditional practices such as female genital mutilation, forced marriages, and honour crimes; physical violence, such as murder, assault, domestic violence, human trafficking and slavery, forced sterilisation, and forced abortion; emotional and psychological violence, such as abuse, humiliation, and confinement; and socioeconomic violence, such as discrimination and/or denial of opportunities and services, and prevention of the exercise and enjoyment of civil, social, economic, cultural, and political rights.

The International Committee of the Red Cross explains that while these forms of violence can be perpetrated against any individual, they constitute GBV because they have differential gendered impacts. For example, forms of sexual violence are perpetrated differently against a person depending on their sex; the health consequences of sexual violence differ based on sex; causes of sexual violence differ based on sex, sexual orientation, or gender identity; and the societal impact and stigmatisation of sexual violence differs depending on these factors, too.¹²⁷

Men and boys constitute the majority of victims of violent death worldwide. According to the United Nations, half a million people die from armed conflict or armed violence every year. About 84 per cent of these are male and less than 16 per cent are female.¹²⁸ Men and boys are subject to GBV—including forced recruitment, arbitrary detention, sexual violence, or mass killing on the basis of sex.¹²⁹

In conflict, civilian men are often targeted—or counted in casualty recordings—as militants only because they are men of a certain age. According to a *New York Times* report from May 2012, in counting casualties from armed drone strikes, the US government reportedly records “all military-age males in a strike zone as combatants ... unless there is explicit intelligence posthumously proving them innocent.”¹³⁰ While men are not necessarily targeted solely because they are men, taking gender as a key signifier as identity and exacting harm on that basis constitutes gender-based violence. That is to say, if someone uses gender as a basis for assessing whether or not a person is targeted, or if an attack is allowed (are only men present?), or in determining the impact of an attack later (i.e. during casualty recording), then they are using the gender of that person not as the motivation for the attack but as a proxy for identifying militants, or “acceptable targets”. This erodes the protection that civilians should be afforded in conflict and violates many human rights, including the right to life and due process.¹³¹

This form of gender-based violence also has broader implications in the reinforcement of gender norms, including militarised masculinity. Assuming all military-age men to be potential or actual militants or combatants entrenches the idea that men are violent and thus targetable. This devalues men’s lives—it suggests men are relatively more expendable than women, nonbinary, or gender non-confirming people.

¹²⁷ *International Humanitarian Law and Gender-Based Violence in the Context of the Arms Trade Treaty*, International Committee of the Red Cross Working Paper, April 2019.

¹²⁸ *Women, Men and the Gendered Nature of Small Arms and Light Weapons*, United Nations Modular Small-arms-control Implementation Compendium (2018), 5.

¹²⁹ See for example R. Charli Carpenter, “Recognizing Gender-Based Violence Against Civilian Men and Boys in Conflict Situations,” *Security Dialogue* 37, no. 1 (2006): 83–103; R. Charli Carpenter, “Women, Children and Other Vulnerable Groups: Gender, Strategic Frames and the Protection of Civilians as a Transnational Issue,” *International Studies Quarterly* 49, no. 2 (2005): 295–344; and P. Viseur Sellers, “(Re)considering Gender Jurisprudence,” in *The Oxford Handbook of Gender and Conflict*, eds. Fionnuala Ní Aoláin et al (Oxford: Oxford University Press, 2018), 217–20.

¹³⁰ Jo Becker and Scott Shane, “Secret ‘Kill List’ Proves at Test of Obama’s Principles and Will,” *The New York Times*, 29 May 2012.

¹³¹ Ray Acheson et al, *Sex and drone strikes: gender and identity in targeting and casualty analysis*, Reaching Critical Will and Article 36, October 2014, <http://www.reachingcriticalwill.org/images/documents/Publications/sex-and-drone-strikes.pdf>.

It increases the vulnerability of men, exacerbating other risks adult civilian men face such as forced recruitment, arbitrary detention, and summary execution.¹³²

More broadly, the reinforcement of gender norms through targeting men as militants works against the establishment and sustainment of a more equitable society. Framing men as the militants, as the “protectors” of their communities willing to take up arms, in turn reinforces notions of women and others as weak, as needing this protection. This continues to enable the exclusion of women and LGBTQ+ people from authoritative social and political roles. It also reinforces the binary between women and men as weak and strong, as passive and violent, and refuses to acknowledge other identities and experiences that do not conform to this binary. Reinforcing militarised masculinities also reproduces the power asymmetries and gendered hierarchies that underpin many acts of gender-based violence against women, LGBTQ+ people, or gender non-conforming people.

It’s also important to note that the risk of gender-based violence is also heightened during and after conflict. War destabilises communities and exacerbates already existing gender inequalities and oppression of women, girls, LGBTQ+ people, and others who do not conform to societies’ standards of gender norms. Thus, when analysing the potential of a weapon system or a technology contributing to or facilitating gender-based violence, it is essential to consider the ways in which it might lower the threshold for the use of force or an act of violence, leading more and more communities into situations where gender-based violence, including sexual violence, is likely to increase throughout society at large.

Inside and outside of armed conflict, women, girls, and LGBTQ+ people are the primary targets for GBV. Most are killed by intimate partners or other family members.¹³³ “Non-intimate” GBV, including murder, sexual abuse, and sexual torture, is disproportionately targeted against women and girls.¹³⁴ LGBTQ+ people also face extraordinary levels of physical and sexual violence.¹³⁵ The US National Center for Transgender Equality notes that “more than one in four trans people has faced a bias-driven assault, and rates are higher for trans women and trans people of color.”¹³⁶

GBV and militarism

GBV is part and parcel of patriarchy, which produces a hierarchy among sexes and among hegemonic norms of gender identities and expressions. Patriarchy celebrates a “particular idealized image of masculinity in relation to which images of femininity and other masculinities are marginalized and subordinated.”¹³⁷ The culture of militarism plays an outsized role in determining what this masculinity looks like, through which primacy is awarded to “toughness, skilled use of violence, presumption of an enemy, male camaraderie, submerging one’s emotions, and discipline (being disciplined and demanding it of others).”¹³⁸

Military institutions engage actively in the processes of differentiating and “othering” that reinforces the ideal of gendered hierarchies. Turning men (and others) into warfighters requires breaking down their sense of ethics and morals and building up a violent masculinity that is lacking in empathy and glorifies

¹³² R. Charli Carpenter, “Recognizing Gender-Based Violence Against Civilian Men and Boys in Conflict Situations,” *Security Dialogue* 37(1), March 2006.

¹³³ *Global Study on Homicide: Gender-related Killings of Women and Girls* (Vienna: United Nations Office on Drugs and Crime, 2019), 10.

¹³⁴ *Understanding and Addressing Violence Against Women* (Geneva: World Health Organisation, 2012).

¹³⁵ “TMM Update Trans Day of Remembrance 2018—Press Release,” TvT Trans Murder Monitoring, Transgender Europe, 12 November 2018.

¹³⁶ “Issues: Anti-Violence,” National Center for Transgender Equality, <https://transequality.org/issues/anti-violence>.

¹³⁷ Franck Barrett, “The Organizational Construction of Hegemonic Masculinity: The Case of the US Navy,” *Gender, Work and Organization* 3, no. 3 (1996).

¹³⁸ Cynthia Enloe, *Bananas, Beaches, and Bases* (Berkeley: University of California Press, 1990): 150.

strength as violence and physical domination over others portrayed as weaker. Hierarchy is fundamental to military training. Teaching human beings to kill other human beings “requires dehumanizing others by promoting the belief that another human is somehow a ‘lesser’ creature,” Cynthia Enloe explains. “One of the central forms of dehumanization promoted by military training and the culture of daily life in the military has been the supposed inferiority of women—that women are less than men.”¹³⁹

A culture of sexual violence—and impunity for perpetrators—is part of the military’s purposeful development of violent masculinities. One immediate consequence of this culture is that women in the military are often subject to sexual assault.¹⁴⁰ This also applies to the treatment of LGBTQ+ servicemembers. Participants in a study of queer soldiers in the US military reported experiencing discrimination, threats and intimidation, vandalism, sexual harassment, and physical assault, including sexual assault.¹⁴¹

The culture of violence inherent to the norms of militarised masculinities has implications for weapons culture and possession. Weapons—from small arms to nuclear bombs—are seen from this perspective as being essential to power. Whether the concern is having the biggest stockpile or the most high-tech capabilities, weapon possession and proliferation is treated as indicative of status: of being ready to “defend,” of being able to oppress and control.¹⁴² All weapons are part of this culture of gendered violence, and all weapons can be used to commit acts of GBV—including autonomous weapons, AI-enabled weapons, and other militarised data-intensive systems. Arguably, both the culture and commission of GBV are *inherent* to this technology.

GBV and the military use of data-intensive systems

Remote-controlled weapons such as armed drones exude the culture of sexual violence and impunity. According to a former Joint Strike Operating Command (JSOC) drone operator interviewed by *The Intercept*, one nickname given to armed drones is “Sky Raper”.¹⁴³ A nickname like this is about violent masculinities dominating and directing the conduct of soldiers—invulnerable warriors, immune from prosecution for rape and war crimes—on and off the battlefield. It reinforces the institutionalisation of rape as a tool of war. It helps the operators and developers of the weapon own the use of rape for domination and to defeat a target, while simultaneously participating in the normalisation of rape.¹⁴⁴ It also is an overt sexualisation of the nature of imperial violence: those operating weapons from far away deploy them unlawfully in other countries, penetrating their borders without their governments’ consent.

¹³⁹ Cynthia Enloe, “Beyond ‘Rambo’: Women and the Varieties of Militarized Masculinity,” *Women and the Military System*, edited by Eva Isaakson (New York: St. Martin’s Press, 1988), 71–93. Also see Penny Strange, *It’ll Make a Man of You: Feminist View of the Arms Race* (Nottingham: Five Leaves Publications, 1983). As Barrett, “The Organizational Construction of Hegemonic Masculinity,” p. 134, argues, integrating women in military isn’t going to “dilute the tough image associated with the ideology of masculinity.” They are often seen as having been cut a break by being “allowed” in without having to go through the same rigorous training as men.

¹⁴⁰ See <http://www.pbs.org/independentlens/films/invisible-war>.

¹⁴¹ Sitaji Gurung et al, “Prevalence of Military Sexual Trauma and Sexual Orientation Discrimination Among Lesbian, Gay, Bisexual, and Transgender Military Personnel: A Descriptive Study,” *Sexual Research and Social Policy* 15 (2018): 74–82.

¹⁴² See for example Carol Cohn, Felicity Hill, and Sara Ruddick, *The Relevance of Gender for Eliminating Weapons of Mass Destruction*, The Weapons of Mass Destruction Commission, No. 38 (2006); Anne Harrington de Santana, “Nuclear Weapons as the Currency of Power: Deconstructing the Fetishism of Force,” *The Nonproliferation Review* 16, no. 3 (2009): 325–345; Catherine Eschle, “Gender and Valuing Nuclear Weapons,” Working Paper for *Devaluing Nuclear Weapons: Concepts and Challenges*, University of York, Department of Politics, 20–21 March 2012; and Ray Acheson, “The nuclear ban and the patriarchy: a feminist analysis of opposition to prohibiting nuclear weapons,” *Critical Studies on Security* (30 April 2018), 1–5.

¹⁴³ Jeremy Scahill and Glenn Greenwald, “The NSA’s secret role in the U.S. assassination program,” *The Intercept*, 10 February 2014.

¹⁴⁴ Erin Corbett, “On Nicknaming Predators,” *The Feminist Wire*, 22 June 2015.

The “Sky Raper” represents the “white Western phallic power” enforcing power and masculinity over “the other”.¹⁴⁵

The imagery of rape and nonconsensual activities in this context is not an aberration. A culture of sexual violence—and subsequent immunity—is part of the culture of dominance and invulnerability that is part of the military’s purposeful development of violent masculinities and a “warrior ethos”.¹⁴⁶

This is part of why the argument that one of the advantages of autonomous weapons is that they “won’t rape” is so preposterous.¹⁴⁷ Such an assertion relies on an assumption that rape in warfare is something born of emotion, something that happens “in the heat of the moment”. But time and again, sexual violence in conflict is ordered by states and by armed groups alike. Rape and other forms of sexual – and gender-based violence have been a part of war throughout history and continue to be so during all of today’s conflicts, to the point where it has been officially recognised as a weapon of war.¹⁴⁸

There is also no technical barrier to an autonomous weapon or data-intensive weapon system being used to commit an act of sexual violence. A machine that can be programmed to manoeuvre inside of urban areas and engage in combat with humans can also be programmed to inflict sexual violence against them. As Charli Carpenter notes, “If I can imagine a machine inflicting lethal violence on a human being through projectile, I have no problem whatsoever imagining a machine forcibly penetrating” a human body.¹⁴⁹

There are also other ways to commit sexual and GBV with data-intensive systems. Grok, the chatbot developed by Elon Musk’s company xAI, has been used extensively to generate sexualised images of women and children. According to a WIRED review of the chatbots’ publicly posted live output, Grok is used every few seconds to create images of women in bikinis or underwear in response to user prompts on X.¹⁵⁰ This technology isn’t new—harmful AI image generation technology has been used to digitally harass and abuse women for years.¹⁵¹ But the ongoing use of Grok “to create vast numbers of nonconsensual images marks seemingly the most mainstream and widespread abuse instance to date,” notes WIRED. “Unlike specific harmful nudity or ‘undress’ software, Grok doesn’t charge the user money to generate images, produces results in seconds, and is available to millions of people on X—all of which may help to normalize the creation of nonconsensual intimate imagery.”¹⁵²

¹⁴⁵ Jasbir K. Puar and Amit Rai, “Monster, Terrorist, Fag: The War on Terrorism and the Production of Docile Patriots,” *Social Text* 20, no. 3 (2002): 137.

¹⁴⁶ See for example Cynthia Enloe, *Bananas, Beaches, and Bases* (Berkeley: University of California Press, 1990); Penny Strange, *It’ll Make a Man of You: Feminist View of the Arms Race* (Nottingham: Five Leaves Publications, 1983); Franck Barrett, “The Organizational Construction of Hegemonic Masculinity: The Case of the US Navy,” *Gender, Work and Organization* 3, no. 3 (1996); and Maya Eichler, “Militarized Masculinities in International Relations,” *Brown Journal of World Affairs*, Volume XXI, Issue I (Fall/Winter 2014).

¹⁴⁷ This argument was made by certain participants at the Convention on Certain Conventional Weapons Meeting of Experts on Lethal Autonomous Weapon Systems in May 2014. See Ray Acheson, “Meaningful deliberation,” *CCW Report* 1, no. 4 (16 May 2014): 1.

¹⁴⁸ See for example UN Security Council Resolution 1820 (2008) and the Rome Statute of the International Criminal Court (1998).

¹⁴⁹ Charli Carpenter, “‘Robot Soldiers Would Never Rape’: Un-packing the Myth of the Humanitarian War-Bot,” *Duck of Minerva*, 14 May 2014.

¹⁵⁰ Matt Burgess and Maddy Varner, “Grok is Pushing AI ‘Undressing’ Mainstream,” *WIRED*, 6 January 2026, <https://www.wired.com/story/grok-is-pushing-ai-undressing-mainstream>.

¹⁵¹ See Paresh Dave and Matt Burgess, “Microsoft Hosted Explicit Videos of This Startup Founder for Decades. Here’s How She Got Them to Take it Down,” *WIRED*, 20 February 2025, <https://www.wired.com/story/deepfake-survivor-breeze-liu-microsoft>; Matt Burgess, “A Deepfake Porn Bot Is Being Used to Abuse Thousands of Women,” *WIRED*, 21 October 2020, <https://www.wired.com/story/a-deepfake-porn-bot-is-being-used-to-abuse-thousands-of-women>; and Megan Farokhmanesh, “The Debate on Deepfake Porn Misses the Point,” *WIRED*, 1 March 2023, <https://www.wired.com/story/deepfakes-twitch-streamers-qtcinderella-atric-pokimane>.

¹⁵² Matt Burgess and Maddy Varner, “Grok is Pushing AI ‘Undressing’ Mainstream,” *WIRED*, 6 January 2026, <https://www.wired.com/story/grok-is-pushing-ai-undressing-mainstream>.

In the midst of global public outrage about Grok, then Pentagon announced that it would integrate Grok alongside Google's generative AI engine in its unclassified and classified networks. Secretary of "War" Pete Hegseth said he would "make all appropriate data" from the military's IT systems available for "AI exploitation." He also said data from intelligence databases would be fed into AI systems. Hegseth said his vision for military AI systems means that they operate "without ideological constraints that limit lawful military applications," before adding that the Pentagon's "AI will not be woke."¹⁵³ Musk specifically pitched Grok as an alternative to what he described as "woke AI".

In July 2025, Grok also caused controversy after it made antisemitic comments that praised Adolf Hitler and shared several antisemitic posts.¹⁵⁴

Thus, there are multiple ways that data-intensive systems can be used to commit or facilitate sexual violence, gender-based violence, ethnic violence, or racialised violence. And technology itself does not possess any moral guardrails. Unlike a human soldier, data-intensive systems, if programmed to rape, generate sexual images, or create racist outputs, would not hesitate to do so. The arguments about "emotion" in human soldiers work both ways—if we recognise that human soldiers have the capacity to rape out of "revenge" or anger, we can also recognise that they have the capacity to refuse an order to commit sexual assault. This is a capacity that an autonomous weapon or data-intensive weapon system would not have.

Furthermore, the nature of the technology makes accountability inherently difficult. The belief that a government, soldier, police officer, or federal agent can act with impunity is nothing new. But technologies like armed drones, autonomous weapon systems, and other militarised data-intensive systems amplify the *expectation of impunity*. They help turn impunity into a norm, regardless of international law, human rights, or human well-being. This in turn risks fortifying the culture of impunity for violence, in particular sexual violence. Immunity for sexual violence thrives on the patriarchal pursuit of dominance and control—which in turn underpins the development of these technologies.

Projecting power without vulnerability

The ability to project "influence without projecting vulnerability in the same ratio has favoured the development of aerospace capabilities resting firmly in the ever-evolving foundation of modern technology," wrote Major General Charles D. Link of the US Air Force in 2001.¹⁵⁵ The quest for "deploying military force regardless of frontiers" and "extending imperial power from the center over the world that constitutes its periphery"¹⁵⁶ long precedes the consideration of data-intensive weapon systems. But this mission of "projecting power without projecting vulnerability" could find its purest expression in autonomous weapons and data-intensive military systems.

This increasing separation of distance between the perpetrator of violence and the victim of violence that militarised data-intensive systems perpetuate has implications for the culture of militarised masculinities and patriarchal dominance that has led us here in the first place.

While drones require an operator and their commander to take fly the machine, analyse data it or other systems collect, and take decisions about firing upon targets, autonomous weapons, AI weapons, and other data-intensive weapon systems would be programmed to identify, select, and engage targets. They would complete the separation of human body from battlefield.

¹⁵³ Konstantin Toropin and David Klepper, "Pentagon is embracing Musk's Grok AI chatbot as it draws global outcry," AP News, 12 January 2026, <https://apnews.com/article/artificial-intelligence-pentagon-hegseth-musk-7f99e5f32ec70d7e39cec92d2a4ec862>.

¹⁵⁴ The Associated Press, "Musk's xAI scrubs inappropriate posts after Grok chatbot makes antisemitic comments," AP News, 10 July 2025, <https://apnews.com/article/elon-musk-chatbot-ai-grok-d745a7e3d0a7339a1159dc6c42475e29>.

¹⁵⁵ Charles D. Link, "Maturing Aerospace Power," *Air and Space Power Journal*, 4 September 2001.

¹⁵⁶ Grégoire Chamayou, *A Theory of the Drone* (New York: The New Press, 2014), 12.



This not only has a horrific impact on the dignity of those killed, but will also further entrench the culture of violence. Among other things, the sense of “power” displayed through detached, mechanised violence inherent to an autonomous weapon system will likely reinforce the hegemonic norms of militarised masculinities. The “warrior ethos”—unemotional, detached, serious, and rational—will be perfected through the machine.

Recognising the inherent ability of militarised data-intensive systems to facilitate GBV is important to understanding both the technical potential of these weapon systems as well as their potential to exacerbate the broader culture of GBV and the impunity afforded to perpetrators of such violence. In this expansive view, the military use of data-intensive systems threatens to exacerbate GBV and discrimination, and to reinforce the culture of militarised masculinities and the associated subordination of women and LGBTQ+ people, racialised people, people with disabilities, and others. The ways in which technologies of remote violence such as drones and surveillance already impact upon the lives of marginalised and oppressed people need to be considered. The development and use of weapon systems that enable governments, non-state armed groups, or others to programme a machine to target people based on gender will lead to GBV. It will also further entrench gender essentialisms and intersectional discrimination. In this way, the military use of data-intensive systems will not only facilitate physical violence against certain individual people or groups but will also exacerbate structural violence against women, LGBTQ+ people, Black, Indigenous, other people of colour, people with disabilities, and more.

By automating violence, data-intensive systems expand violence, and by expanding violence, these systems implicate more and more people in the destabilising effects and aftershocks of violence and to the amplification of underlying structural discrimination and inequalities. Furthermore, the increasing use of data-intensive systems to “discover” targets as well as track and attack them, will “increase suspicion, enmity and will strain relations, not mitigate them,” warns academic Elke Schwarz. “And this is precisely where we are right now with expanding and escalating tensions across the globe.”¹⁵⁷

¹⁵⁷ Elke Schwarz, “The (im)possibility of responsible military AI governance,” *Humanitarian Law & Policy*, 12 December 2024, <https://blogs.icrc.org/law-and-policy/2024/12/12/the-im-possibility-of-responsible-military-ai-governance>.

Environmental damage

There are several gendered impacts associated with the environmental harm caused by data-intensive systems. In addition to harm directly caused to the environment by the use of these systems, there are also many other impacts associated with their energy and water consumption, as well as the extraction of minerals necessary for their development. With the growing militarisation of these systems, it is expected that these harms will be exacerbated, as more natural resources are needed for their development and use.

As environmental and ecological damage increases and the climate crisis intensifies, armed violence and conflicts are raging globally. Conflicts over water, land, and food security are increasing; and as people flee regions facing climate disasters, food shortages, and armed violence, they are met with violence at the borders of the countries most responsible for generating this harm in the first place. The expanding and escalating tensions across the globe are only aggravated by environmental harms from militarised data-intensive systems.

Energy and water consumption

Data-intensive systems require massive amounts of energy to operate. The training and deployment of these systems occur mainly in data centres, which are large facilities that house computing infrastructure. These facilities require an enormous amount of energy to function, as well as water to cool down their computers. With the expansion of data-intensive systems, most notably those based on AI technologies, there has been a boom in the construction of data centres worldwide.

Research shows that AI is far more energy-intensive than typical cloud-based applications. According to a study by Goldman Sachs, a ChatGPT query needs nearly ten times as much electricity to process as a Google search.¹⁵⁸ Data centres are already being used to support systems for military operations, policing, immigration enforcement, including facial recognition, decision support systems, autonomous weapons, and many other technologies that generate, collect, and/or analyse vast amounts of data¹⁵⁹.

¹⁵⁸ "AI is poised to drive 160% increase in data center power demand," Goldman Sachs, 14 May 2024, <https://www.goldmansachs.com/insights/articles/AI-poised-to-drive-160-increase-in-power-demand>.

¹⁵⁹ Marco Di Donato, "AI-Enabled Weapons Systems and the Environment: The Overlooked Costs of AI-Driven Warfare," EJIL: Talk!, 8 December 2025, <https://www.ejiltalk.org/ai-enabled-weapons-systems-and-the-environment-the-overlooked-costs-of-ai-driven-warfare>.

Even more energy and water will be consumed by these systems as they are adopted worldwide, with dire consequences for the planet.

The US military is already the largest carbon emitter on the planet.¹⁶⁰ Within the US government, the Pentagon is already among the top users of computing power. The Carnegie Endowment for International Peace notes that The Pentagon's IT arm, the Defense Information Systems Agency, "manages 40,000 servers containing 38 petabytes of storage and serves millions of users."¹⁶¹ The more AI and related technologies the military uses, the more data centres it will need to build, the more energy these centres will require for construction and operation, the more water they will consume, the more minerals will be extracted, and the more harm they will cause to the planet and local communities. As activist Koohan Paik-Mander writes, "It's Manifest Destiny for data."¹⁶²

The electricity and water consumption of data centres results in several environmental harms, which can have specific gendered impacts. For example:

- Energy consumption by data centres, which heavily relies on the burning of fossil fuels, further deepens the climate crisis, which amplifies existing gender inequalities.
- Data centres can exacerbate existing inequalities in communities that already suffer from energy poverty and marginalisation, and women may be disproportionately affected by the consequences of energy and water scarcity.
- Pollution from data centres disproportionately affects women and LGBTQ+ individuals in surrounding communities due to limited access to healthcare and systemic marginalisation.
- The intended reliance in nuclear power to provide energy for data centres perpetuates gender harms associated with the nuclear production chain.

We will analyse each of these impacts separately.

Fossil fuels, the climate crisis, and gender inequality

The International Energy Agency estimates the electricity consumption from data centres has grown 12 per cent per year over the last five years, currently amounting to around 415 terawatt hours (TWh), which represents 1.5 per cent of global electricity consumption in 2024.¹⁶³ This projection is expected to double by 2030, with data centres representing 3 per cent of total global electricity consumption—the equivalent of Japan's current total electricity consumption.

In some regions, the energy consumption of data centres is even more striking. In Virginia, United States, for example, data centres comprise 25 per cent of the electric load.¹⁶⁴ In Ireland, data

¹⁶⁰ Neta C. Crawford, *Pentagon Fuel Use, Climate Change, and the Costs of War*, Watson Institute for International and Public Affairs, Brown University, 12 June 2019, <https://home.watson.brown.edu/news/2019-07-01/pentagon-fuel-use-climate-change-and-costs-war>.

¹⁶¹ Daniel Nasaw, "The Promises and Perils for Sustainability in the U.S. Military's Adoption of AI," Carnegie Endowment for International Peace, 29 May 2024.

¹⁶² Koohan Paik-Mander, "As China and the U.S. Race Toward A.I. Armageddon, Does it Matter Who Wins?" *CounterPunch*, 7 February 2025, <https://www.counterpunch.org/2025/02/07/as-china-and-the-u-s-race-toward-a-i-armageddon-does-it-matter-who-wins>.

¹⁶³ International Energy Agency, "Energy demand from AI," 2025, <https://www.iea.org/reports/energy-and-ai/energy-demand-from-ai>.

¹⁶⁴ "Powering Intelligence: Analyzing Artificial Intelligence and Data Center Energy Consumption," EPRI, 2024, https://www.wpr.org/wp-content/uploads/2024/06/3002028905_Powering-Intelligence_-_Analyzing-Artificial-Intelligence-and-Data-Center-Energy-Consumption.pdf.

centres currently account for 21 per cent of the country's total electricity consumption¹⁶⁵—which is more electricity than consumed by all its urban homes combined¹⁶⁶—with estimates that they will consume a third of the Ireland's electricity by 2026. Nevertheless, they continue to be built not only in these places, but worldwide.

The electric energy consumed by data centres is produced from different means, including fossil fuels, nuclear energy, and renewable sources. In the United States and China, the largest data centre markets today, most of the electricity consumed by data centres is produced from fossil fuels.¹⁶⁷ In the United States, 40 per cent of the electricity for data centres comes from gas, followed by 24 per cent from renewables, 20 per cent from nuclear power, and 15 per cent from coal.¹⁶⁸ In China, 70 per cent of the data centre electricity supply comes from coal, followed by renewables with nearly 20 per cent, nuclear close to 10 per cent, and natural gas accounting for the remainder.¹⁶⁹ Worldwide, the International Energy Agency estimates that fossil fuels currently meet almost 60 percent of data centres' energy demand.¹⁷⁰

In light of this, experts have been warning that data centre growth is jeopardising the energy transition.¹⁷¹ First because it increases power demand, and second because it prevents states from reducing their reliance on fossil fuels. Even before the AI boom, from 2020 to 2022 the real emissions from the company-owned data centres of Google, Microsoft, Meta, and Apple are about 662 per cent higher than officially reported.¹⁷² Morgan Stanley has projected data centre emissions globally to accumulate to 2.5 billion metric tons of CO₂ equivalent by 2030.¹⁷³ Some companies claim they will rely on fossil fuels as a temporary “bridge” until greener solutions become available, however, as scholars from the University of Michigan highlight, “In practice, this transition is often delayed or abandoned altogether, resulting in the direct commissioning of new fossil fuel power plants to keep these facilities online.”¹⁷⁴ There have been reports in the United Kingdom and Germany of data centres that planned to use renewable energy, before turning to fossil fuels to fill the gap.¹⁷⁵

Furthermore, as Greenpeace has documented, “Microsoft, Google, and Amazon all have connections to some of the world's dirtiest oil companies for the explicit purpose of getting more oil and gas out of the ground and onto the market faster and cheaper.”¹⁷⁶ In other words, writes scholar and physicist M.V.

¹⁶⁵ Matt G. O'Neill, “Data Centres in Ireland: The State of Play,” The Institute of International and European Affairs, 18 December 2025, <https://www.iiea.com/blog/data-centres-in-ireland-the-state-of-play>.

¹⁶⁶ Jillian Ambrose, “Ireland's datacentres overtake electricity use of all urban homes combined,” The Guardian, 23 July 2024, <https://www.theguardian.com/world/article/2024/jul/23/ireland-datacentres-overtake-electricity-use-of-all-homes-combined-figures-show#:~:text=Ireland%27s%20energy%20Dhungry%20datacentres%20consumed,to%20the%20Central%20Statistics%20Office>.

¹⁶⁷ International Atomic Energy Agency, “Energy supply for AI,” 2025, <https://www.iaea.org/reports/energy-and-ai/energy-supply-for-ai>.

¹⁶⁸ Ibid.

¹⁶⁹ Ibid.

¹⁷⁰ International Atomic Energy Agency, “Energy and AI,” 10 April 2025, <https://www.iaea.org/reports/energy-and-ai>.

¹⁷¹ Kezia Rice, “‘The New Oil’: How Data Centres Threaten Climate Protection—And What We Can Do About It,” RESET Digital for Good, 17 November 2025, <https://en.reset.org/the-new-oil-how-data-centres-threaten-climate-protection-and-what-we-can-do-about-it/#h-energy-grids-are-under-pressure-while-consumer-bills-rise>.

¹⁷² Isabel O'Brien, “Data center emissions probably 662% higher than big tech claims. Can it keep up the ruse?” The Guardian, 16 September 2024, <https://www.theguardian.com/technology/2024/sep/15/data-center-gas-emissions-tech>.

¹⁷³ “Global data center industry to emit 2.5 billion tons of CO₂ through 2030, Morgan Stanley says,” Reuters, 3 September 2024, <https://www.reuters.com/markets/carbon/global-data-center-industry-emit-25-billion-tons-co2-through-2030-morgan-stanley-2024-09-03>.

¹⁷⁴ Terry Nguyen and Ben Green, “What happens when data centers come to town?,” Ford School Science, Technology and Public Policy, University of Michigan, July 2025, <https://stpp.fordschool.umich.edu/sites/stpp/files/2025-07/stpp-data-centers-2025.pdf>.

¹⁷⁵ Kezia Rice, op. cit.

¹⁷⁶ “Greenpeace Report: Oil in the Cloud,” Greenpeace, 19 May 2020, <https://www.greenpeace.org/usa/oil-in-the-cloud>.

Ramana, “the business models adopted by these tech behemoths depend on fossil fuels being used for longer and in greater quantities.”¹⁷⁷

The increasing reliance on fossil fuels further deepens the climate crisis, which has several gendered impacts.¹⁷⁸ The climate crisis disproportionately affects women by exacerbating systemic inequalities. The UN estimates that by 2050, climate change may push up to 158 million more women and girls into poverty (which, in their binary calculation, is 16 million more than the total number of men and boys).¹⁷⁹ Even today, the UN points out that 47.8 million more women face food insecurity and hunger than men.¹⁸⁰ In addition to women being more likely to live in poverty,¹⁸¹ they also live in areas with limited access to emergency services, housing and clean air.¹⁸² Women are also disproportionately impacted by disasters and natural hazards.¹⁸³

Patriarchal norms dictating women's roles and access to resources impacts how they are affected by climate change. For example, UN Women highlights that women depend more on, and yet have less access to, natural resources.¹⁸⁴ In many regions, women bear responsibility for securing food, water and fuel for their families. They are more likely to rely on climate dependent natural resources for food and work,¹⁸⁵ and have domestic responsibilities tying them to the home.¹⁸⁶ They also tend to be caregivers for children, older and disabled family members. As affirmed by the Clean Air Fund, these conditions makes them more prone to the effects of climate change: “When hazardous air pollution levels shut schools, childcare responsibilities often fall on mothers, impacting their ability to work and generate income.¹⁸⁷ These conditions make responding to,¹⁸⁸ evacuating from,¹⁸⁹ migrating away¹⁹⁰ or recovering from climate disasters, like wildfires,¹⁹¹ more difficult.”¹⁹²

177 M.V. Ramana, “Dangerous Hype: Big Tech’s Nuclear Lies,” *CounterPunch*, 1 November 2024, <https://www.counterpunch.org/2024/11/01/big-techs-nuclear-lies>.

178 UN Women, “How gender inequality and climate change are interconnected,” 21 April 2025, <https://www.unwomen.org/en/articles/explainer/how-gender-inequality-and-climate-change-are-interconnected#:~:text=The%20climate%20crisis%20is%20not,less%20access%20to%2C%20natural%20resources>.

179 UN Women, “The Gender Snapshot 2025,” 2025, <https://www.unwomen.org/en/resources/gender-snapshot>.

180 Ibid.

181 OXFAM, “Why the majority of the world’s poor are women,” <https://www.oxfam.org/en/why-majority-worlds-poor-are-women>.

182 Sarah Hamidi, “Gender Disparities in the Wake of the Los Angeles Wildfires,” Feminist Majority Foundation, 21 January 2025, <https://feminist.org/news/gender-disparities-in-the-wake-of-the-los-angeles-wildfires>.

183 Alvina Erman, Sophie Anne De Vries Robbé, Stephan Fabian Thies, Kayenat Kabir, Mirai Maruo, “Gender Dimensions of Disaster Risk and Resilience,” International Bank for Reconstruction and Development / The World Bank, 202, <https://wrds.unwomen.org/sites/default/files/2021-11/Gender-Dimensions-of-Disaster-Risk-and-Resilience-Existing-Evidence.pdf>.

184 UN Women, “How gender inequality and climate change are interconnected,” 21 April 2025, <https://www.unwomen.org/en/articles/explainer/how-gender-inequality-and-climate-change-are-interconnected#:~:text=The%20climate%20crisis%20is%20not,less%20access%20to%2C%20natural%20resources>.

185 International Organisation for Migration, “3 ways in which gender equality interlinks with climate migration as an adaptation strategy – Exploring the links between migration, the environment and SDG 5,” <https://environmentalmigration.iom.int/blogs/3-ways-which-gender-equality-interlinks-climate-migration-adaptation-strategy-exploring-links-between-migration-environment-and-sdg-5?ref=hir.harvard.edu>.

186 Summer Rose, “Women at Risk: The Gendered Dimension of Climate Change and Migration in West Africa,” *Harvard International Review*, 5 February 2025, <https://hir.harvard.edu/women-at-risk-the-gendered-dimension-of-climate-change-and-migration-in-west-africa/#:~:text=Women's%20representation%20facilitates%20stronger%20gender,gender%2Dsensitive%20climate%20change%20legislation>.

187 Diane Archer, “Understanding the gendered impacts of air pollution in the world of work,” SEI, 24 November 2020, <https://www.sei.org/perspectives/gendered-impacts-air-pollution-work>.

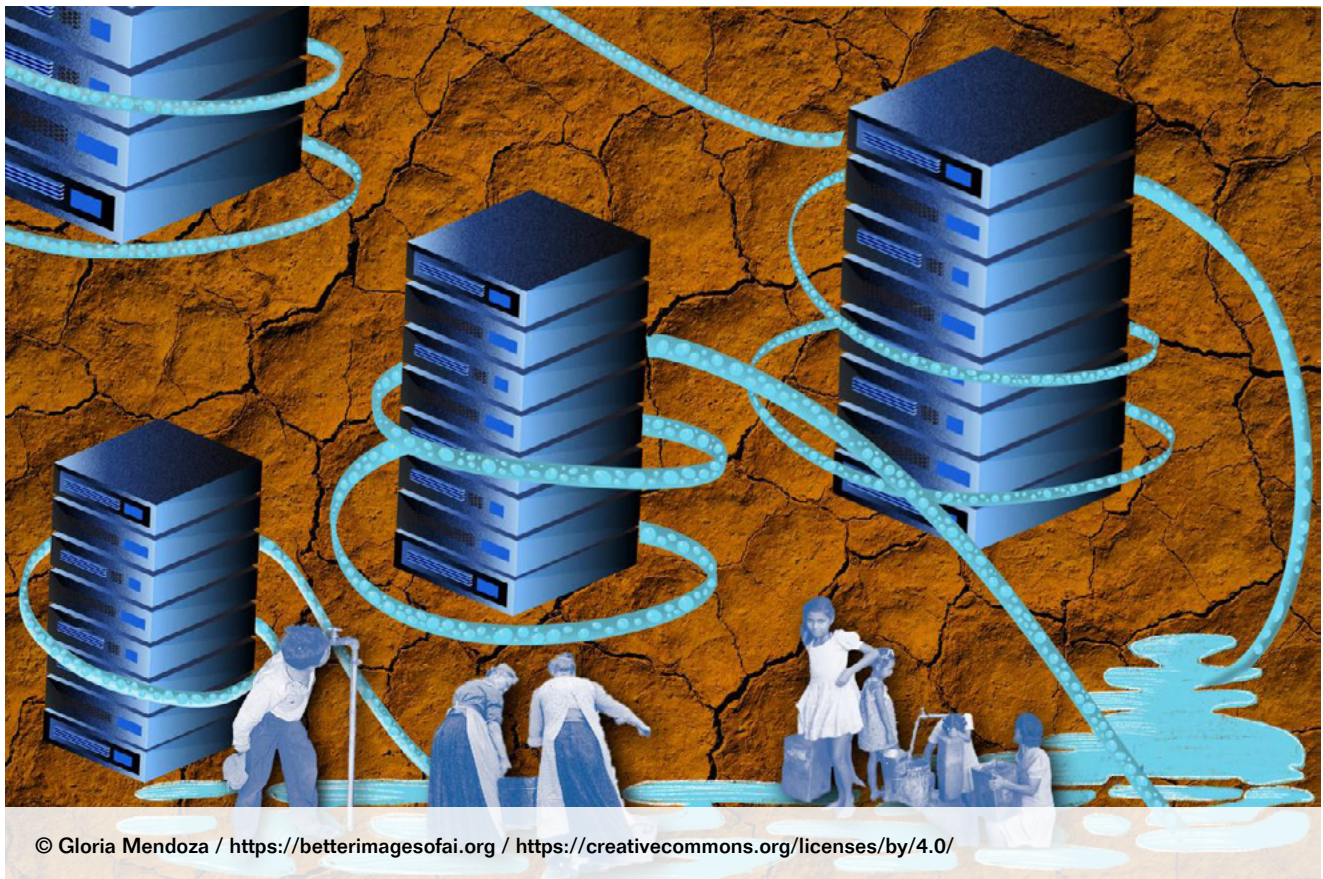
188 Summer Rose, op cit.

189 Gender Equity Policy Institute, “The Promise of Gender Inclusive Climate Action,” January 2024, <https://thegepi.org/the-promise-of-gender-inclusive-climate-action>.

190 International Organisation for Migration, op. cit.

191 Ibid.

192 Jess Taylor, “The unequal impact of air pollution on women,” Clear Air Fund, 7 March 2025, <https://www.cleanairfund.org/news-item/impact-of-air-pollution-on-women>.



Studies also show that the climate crisis is intensifying the social and economic stresses that are fuelling increased levels of violence against women and girls.¹⁹³ The impacts of climate change escalate tensions in fragile and conflict-affected settings, which leads to increased levels of gender-based violence.¹⁹⁴

In all these cases, the impacts are different according to other layers of systemic inequalities. Indigenous and Afro-descendent women and girls, older women, LGBTQ+ people, women and girls with disabilities, migrant women, and those living in rural, remote, conflict, and disaster-prone areas can bear exacerbated impacts from climate change.

Water and energy scarcity

Data centres require enormous amounts of water for cooling. With the expansion of the use of AI and data-intensive systems more broadly, the demand for data centres can have a significant impact on the water availability for the local population, especially in locations that already suffer from water and energy scarcity. For example, in Nigeria, only 36 per cent of the urban population and 21 per cent of the rural population had access to safe drinking water in 2022.¹⁹⁵ Additionally, while the urban population has 100 per cent electricity access, only 21 per cent of the rural population had electricity access in 2021, according to the World Bank. Nevertheless, in 2023, there were 10 data centres in Lagos, Nigeria, each using a significant amount of water for cooling and electricity generation.

¹⁹³ Spotlight Initiative, "Colliding Crises: How the climate crisis fuels gender-based violence," April 2025, <https://spotlightinitiative.org/publications/colliding-crises-how-climate-crisis-fuels-gender-based-violence>.

¹⁹⁴ UN Women, "South Sudan: Women Weathering Climate Impact and Increased Violence," 21 November 2024, <https://africa.unwomen.org/en/stories/feature-story/2024/11/south-sudan-women-weathering-climate-impact-and-increased-violence>.

¹⁹⁵ Ava Strasser and Rosemary Idem, "The Gender-Energy Nexus in the AI Era: Challenges and Opportunities," Sustainable Energy for All, 2024, https://www.seforall.org/system/files/2024-08/SEforALL_Gender_AI_report.pdf.

Nigeria is not an isolated case; on the contrary, data centres are being built in many other locations that suffer from water scarcity. In Chile, which is facing a decades-long drought, a local court suspended the construction of a Google data centre after locals discovered it would extract more than 7 billion litres of water annually.¹⁹⁶ In Arizona, United States, also a dry region, a city council in Arizona rejected a proposal for an Amazon data centre following public outcry over its potential water use.¹⁹⁷ In Brazil, there are more than 180 data centres already commissioned, representing an increase of 330 per cent in requests for data centres to access the Brazilian electrical grid.¹⁹⁸ Brazil is considered attractive by tech companies to build their data centres there because nearly 80 per cent of its electricity supply comes from renewables. However, around a third of the 195 data centres being built or already in operation are in the state of São Paulo, which already faces challenges with water scarcity. The city of Vinhedo, for example, declared a “water emergency” in 2024, and had to implement water rationing among the population. Despite this, the two data centres that operate in the city were not affected.¹⁹⁹ Other requests for the commission of data centres in Brazilian cities include the city of Caucaia, in Ceará, which experiences frequent water crises, and Eldorado do Sul, in Rio Grande do Sul, which faced catastrophic floods last year.²⁰⁰

Many Indigenous populations are particularly affected by data centres and have been at the forefront of the struggle against their construction. In the Nevada desert in the United States, several companies are building new data centres, despite concerns of the Pyramid Lake Paiute, a Native American tribe that data centres’ demands could decimate already scarce resources.²⁰¹ In Canada, the Sturgeon Lake Cree Nation issued an open cease and desist letter against the construction of a massive data centre in their drought-stricken region of Alberta, warning that they had not been consulted by either the province or the municipality.²⁰² The Anacé, an Indigenous group in Brazil, brought a formal complaint before federal authorities, asking them to halt the development of a TikTok data center being built on their land.²⁰³ Its leaders say their right to consultation—guaranteed under an international agreement—was violated, and that their concerns about the project’s water consumption are being ignored. Their concern is that the daily water consumption estimate of 30,000 litres disclosed by the developer is too low in comparison to similar projects.

In addition to causing water scarcity, data centres also increase local electric utility rates by driving up overall energy demand.²⁰⁴ This can strain grid capacity and force utilities to invest in costly infrastructure upgrades. The local population ends up being affected, as these costs are passed on to residents through higher rates.

¹⁹⁶ Claudia Urquieta and Daniela Dib, “U.S tech giants are building dozens of data centers in Chile. Locals are fighting back,” *Rest of World*, 31 May 2024, <https://restofworld.org/2024/data-centers-environmental-issues>.

¹⁹⁷ Yana Kunichoff, “Tucson City Council rejects Project Blue data center amid intense community pressure,” *Arizona Luminaria*, 6 August 2025, <https://azluminaria.org/2025/08/06/tucson-city-council-rejects-project-blue-amid-intense-community-pressure>.

¹⁹⁸ “Brazil Data Centers,” *Data Center Map*, <https://www.datacentermap.com/brazil>.

¹⁹⁹ Laura Scofield, “SP: Data centers multiplicam-se em plena escassez hídrica,” *Outras Mídias*, 9 December 2025, <https://outraspalavras.net/outrasmidias/sp-data-centers-multiplicam-se-em-plena-escassez-hidrica/>.

²⁰⁰ Jorge C. Carrasco, “Brazil wants to be a sustainable data center hub. Environmentalists are skeptical,” *Rest of the World*, 3 July 2025, <https://restofworld.org/2025/brazil-data-center-environmental-risk>.

²⁰¹ Dara Kerr, “The AI boom is heralding a new gold rush in the American west,” *The Guardian*, 4 December 2025, <https://www.theguardian.com/technology/2025/dec/04/nevada-ai-data-centers>.

²⁰² Sturgeon Lake Cree Nation, “Open Letter: Sturgeon Lake Cree Nation Concerns over AI Data Centre in Traditional Territory,” 13 January 2024, <https://www.sturgeonlake.ca/wp-content/uploads/2020/07/13-01-25-Chief-Sunshine-Open-Letter-Premier-Smith-Re-O-Leary.pdf>.

²⁰³ Laís Martins, “Indigenous group in Brazil takes TikTok to court over planned data center,” *Rest of World*, 8 September 2025, <https://restofworld.org/2025/brazil-indigenous-group-sues-tiktok-data-center>.

²⁰⁴ Terry Nguyen and Ben Green, op. cit.

The water and energy scarcity caused by data centres in certain communities can impact women disproportionately. Around 1.8 billion people in the world live in households without water supplied on the premises.²⁰⁵ Women and girls are usually responsible for fetching water and when this resource is scarce, they need to travel further and work harder.²⁰⁶ Energy poverty also affects women differently due to economic disparities, physiological vulnerabilities, health implications, and sociocultural dynamics.²⁰⁷ Women are at higher risk of energy poverty due to the gender pay gap and greater likelihood of living alone at older ages.²⁰⁸ Factors such as employment status, marital status, and socioeconomic background shape energy needs and vulnerabilities.²⁰⁹ For example, in Europe, data from 2022 shows that single mothers and other single women are more likely to have difficulties paying their energy bills than single men.²¹⁰ This is often due to the lower average incomes and a higher prevalence of low-paid, part-time, or precarious work.

Pollution

Data centres create air pollution resulting in significant respiratory-related health consequences.²¹¹ They release ambient air pollutants, including PM2.5 and nitrogen oxides (NOx), which are often called “silent killers”²¹² because they can penetrate deep into the lungs and are linked to a variety of health outcomes, such as asthma, lung cancer, heart attacks, and even premature deaths.²¹³ These air pollutants are released by coal and other fossil fuel power plants, which provide electric energy for the operation of data centres, but they are also released by backup generators. The vast majority of data centre backup generators are powered by diesel, which release a large amount of tiny air pollutants.²¹⁴

In Shelby County, Tennessee, United States, a large data centre reportedly emits between 1,200 and 2,000 tons of NOx annually²¹⁵ from on-site gas turbines. A study by researchers at the University of Tennessee, Knoxville, found that the peak nitrogen dioxide level rose by 79 per cent after the data centre began operating,²¹⁶ raising serious public health concerns. In Boxtown, Memphis, a predominantly Black community also faces serious health impacts²¹⁷ due to Colossus, a huge data centre built by Elon Musk that is fuelled by 35 gas turbines. The turbines have been pumping out level of emissions that have been exacerbating health issues of an already marginalised area. Both cases of Tennessee and

²⁰⁵ World Health Organisation, “Women and girls bear brunt of water and sanitation crisis – new UNICEF-WHO report,” 6 July 2023, <https://www.who.int/news/item/06-07-2023-women-and-girls-bear-brunt-of-water-and-sanitation-crisis---new-unicef-who-report>.

²⁰⁶ Ibid.

²⁰⁷ Mariëlle Feenstra, “Reframing Energy Poverty through a Gender Lens: A Call for Inclusive Policy Solutions,” 24 March 2025, <https://fsr.eui.eu/reframing-energy-poverty-through-a-gender-lens-a-call-for-inclusive-policy-solutions>.

²⁰⁸ Ibid.

²⁰⁹ European Parliament, “International Women’s Day: the gender aspects of energy poverty,” 27 February 2023, <https://www.europarl.europa.eu/topics/en/article/20230224STO76403/international-women-s-day-the-gender-aspects-of-energy-poverty>.

²¹⁰ Ibid.

²¹¹ Shaolei Ren and Adam Wierman, “Mitigating the Public Health Impacts of AI Data Centers,” *Harvard Business Review*, 5 November 2025, <https://hbr.org/2025/11/mitigating-the-public-health-impacts-of-ai-data-centers>.

²¹² UNICEF, “The silent killer: over 100 daily deaths of children under five linked to air pollution in East Asia and the Pacific,” 6 February 2025, <https://www.unicef.org/eap/press-releases/silent-killer-air-pollution>.

²¹³ World Health Organisation, “Air pollution,” https://www.who.int/health-topics/air-pollution#tab=tab_1.

²¹⁴ Department of Ecology State of Washington, “Diesel pollution from data centers,” <https://ecology.wa.gov/air-climate/air-quality/data-centers>.

²¹⁵ Ariel Wittenberg, “‘How come I can’t breathe?’: Musk’s data company draws a backlash in Memphis,” *Politico*, 5 June 2025, <https://www.politico.com/news/2025/05/06/elon-musk-xai-memphis-gas-turbines-air-pollution-permits-00317582>.

²¹⁶ Andrew R. Chow, “‘We Are the Last of the Forgotten’: Inside the Memphis Community Battling Elon Musk’s xAI,” *Time*, 13 August 2025, <https://time.com/7308925/elon-musk-memphis-ai-data-center>.

²¹⁷ Ibid.

Memphis demonstrate that data centres exacerbate harm to communities by being built in areas that are already economically disadvantaged and that have long struggled with poor air quality.

In line with this, a 2024 paper from researchers at the University of California, Riverside and Caltech found that data centres could contribute to 600,000 asthma-related symptom cases by 2030 in the United States, with overall public health costs exceeding 20 billion USD.²¹⁸ As put by Cecilia Marrinan, “in regions already burdened by public health challenges stemming from environmental racism and gentrification, these troubling health impacts will disproportionately affect communities of colour and exacerbate existing health disparities.”²¹⁹

The pollution caused by data centres has differentiated gendered impacts. Air pollution has a uniquely damaging effect on women’s health.²²⁰ Those living in polluted areas have a greater breast cancer risk.²²¹ Certain chronic health conditions, like asthma, are more common in women than in men. Air pollution has also been found to increase women’s risk of heart disease.²²²

Gender norms and power relations also influence access to health services. A 2019 report by the World Health Organisation found that gender norms and power relations influence women’s access to health services and timely diagnosis, while harmful notions of masculinity increase men’s risk-taking and reduce their willingness to use health services.²²³

Additionally, women and girls often face greater barriers than men and boys to accessing health information and services.²²⁴ These barriers include restrictions on mobility, lack of access to decision-making power, lower literacy rates, discriminatory attitudes of communities and healthcare providers, and lack of training and awareness amongst healthcare providers and health systems of the specific health needs and challenges of women and girls. Studies also show that heterosexism, transphobia and homophobia are barriers to healthcare service access, with high numbers of LGBTQIA+ people reporting they experience discriminative behaviour when seeking healthcare, including stigma, denial or refusal of healthcare, and verbal or physical abuse.²²⁵

Nuclear power

Due to the public exposure of the astronomical energy consumption of data centres, Microsoft, Google, and Amazon announced they were going to invest in nuclear power as a “green” source of energy. But nuclear power is not green, emission free, or environmentally friendly. Its use can result in catastrophic accidents, as seen with Chernobyl and Fukushima, and its every day operation results in environmental contamination and extreme water consumption. Additionally, nuclear power requires uranium mining, fuel processing, and radioactive waste storage—each of which brings its own harms to local communities and the planet. Uranium mining and waste storage are usually imposed upon

²¹⁸ Yuelin Han, Zhifeng Wu, Pengfei Li, Adam Wierman, Shaolei Ren, “The Unpaid Toll: Quantifying and Addressing the Public Health Impact of Data Centers,” Cornell University, <https://arxiv.org/abs/2412.06288>.

²¹⁹ Cecilia Marrinan, “Data Center Boom Risks Health of Already Vulnerable Communities,” Tech Policy Press, 12 June 2025, <https://www.techpolicy.press/data-center-boom-risks-health-of-already-vulnerable-communities/>.

²²⁰ Jess Taylor, op cit.

²²¹ Jamie DePolo, “Long-Term Exposure to Fine-Particle Air Pollution Increases Breast Cancer Risk,” Brestcancer.org, <https://www.breastcancer.org/research-news/air-pollution-breast-cancer-risk>.

²²² Kristin A. Miller, David S. Siscovick, M.P.H., Lianne Sheppard, Kristen Shepherd, Jeffrey H. Sullivan, Garnet L. Anderson, and Joel D. Kaufman, “Long-Term Exposure to Air Pollution and Incidence of Cardiovascular Events in Women,” The New England Journal of Medicine, 1 February 2007, <https://www.nejm.org/doi/full/10.1056/NEJMoa054409>.

²²³ European Institute for Gender Equality, “Gender Equality Index 2021: Health,” https://eige.europa.eu/publications-resources/toolkits-guides/gender-equality-index-2021-report/gender-and-intersecting-inequalities-access-health?language_content_entity=en.

²²⁴ World Health Organisation, “Gender and health,” https://www.who.int/health-topics/gender#tab=tab_1.

²²⁵ European Institute for Gender Equality, op cit.

Indigenous Peoples, often without their knowledge or consent, leading to contamination of traditional food, water sources, and impacting culture, land use, and the health of humans and animals. Uranium mining can also result in several gendered social impacts, including on reproductive health, gender-based violence around mining sites, and shifts in community dynamics due to the presence of large numbers of non-community men.²²⁶

Beyond the harms generated by nuclear power, it is also not a “green” solution to climate change. First, nuclear energy is not carbon-neutral—all the processes to generate nuclear power use other sources of energy and consume vast amounts of water. Emissions from nuclear are lower than fossil fuels but much higher than renewables when life cycle and opportunity cost emissions are considered. In addition, nuclear reactors frequently face shutdowns, meaning they are not always producing the promised amount of energy.

Second, the timelines for building and bringing nuclear power reactors online (upwards of a decade) are beyond the timelines for addressing climate change.²²⁷ Small modular reactors are yet to be proven—everywhere they have been tried they have resulted in unplanned shutdowns or reduced power outputs, or have used chemically corrosive materials leading to other environmental harms. As Ramana argues,

*Because nuclear power has been portrayed as clean and a solution to climate change, announcements about it serve as a flashy distraction to focus public attention on. Meanwhile, these companies continue to expand their use of water and draw on coal and especially natural gas plants for their electricity. This is the magician’s strategy: misdirecting the audience’s attention while the real trick happens elsewhere. Their talk about investing in nuclear power also distracts from the conversations we should be having about whether these data centers and generative AI are socially desirable in the first place.*²²⁸

Mineral extraction

The hardware necessary for the operation of data-intensive systems relies on the extraction of minerals, including cobalt, lithium, or rare earths. The extraction of these minerals is associated with several gendered harms, including health and environmental harms from mining operations disproportionately affecting women and LGBTQ+ individuals in surrounding communities due to limited access to healthcare and systemic marginalisation; and increased exposure to gender-based violence and human rights violations at mining sites.

The growing use of data-intensive systems has led to an increasing demand for critical minerals.²²⁹ The extraction and processing of these critical minerals often entail large-scale mining operations, leading to air pollution, deforestation, water contamination, and long-term ecological pollution. These consequences can have disproportionate impact on women. For example, in the Democratic Republic of the Congo (DRC), industrial and artisanal mining of cobalt and copper have been found to pose

²²⁶ For details on these and other harms of the nuclear industry, please see Ray Acheson, “Nuclear Industry,” in *Petrobromance, Nuclear Priesthood, and Police Repression* (New York: Women’s International League for Peace and Freedom, 2024), pp. 16–60, <https://www.reachingcriticalwill.org/resources/publications-and-research/publications/17206-petrobromance-nuclear-priesthood-and-police-repression-feminist-confrontations-of-violent-industries-and-movements-to-abolish-them>.

²²⁷ M.V. Ramana, “Continued Propaganda About AI and Nuclear Power,” *CounterPunch*, 13 March 2025, <https://www.counterpunch.org/2025/03/13/continued-propaganda-about-ai-and-nuclear-power>.

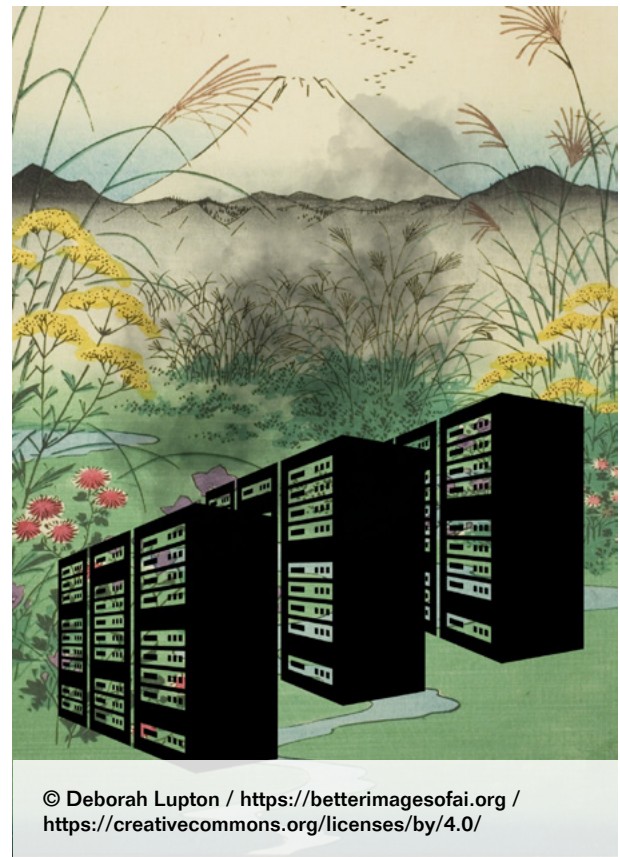
²²⁸ M.V. Ramana, “Dangerous Hype: Big Tech’s Nuclear Lies,” *op. cit.*

²²⁹ Marco Di Donato, “AI-Enabled Weapons Systems and the Environment: The Overlooked Costs of AI-Driven Warfare,” *EJIL: Talk!*, 8 December 2025, <https://www.ejiltalk.org/ai-enabled-weapons-systems-and-the-environment-the-overlooked-costs-of-ai-driven-warfare>.

risks to the reproductive health of women.²³⁰ Additionally, women and gender non-confirming people are disproportionately impacted by the instability caused by the extraction of minerals.²³¹ Gender-based violence is widespread in mining sites, often perpetrated by police, military, or private security personnel who are tasked with protecting mining operations.²³²

The increase in the development of militarised data-intensive systems has already sparked concern of international bodies. The African Commission on Human and Peoples' Rights has underscored the need to respect and protect fundamental human rights in the extraction of resources destined for AI military technology development.²³³

The extraction of minerals for militarised data-intensive systems also tends to perpetuate colonial practices. A large part of the minerals used in such technologies are often sourced from the African continent,²³⁴ or from Indigenous lands²³⁵ in other continents. These extractive practices are not only problematic in themselves—as they reinforce economics inequalities, fuel conflicts, and damage the environment—but are also problematic because marginalised populations from the Global Majority are often at the receiving end of the use of militarised data-intensive systems. They are not the actors developing militarised data-intensive systems; on the contrary, they are the ones against who those systems are used. As the expert Adebayo Okeowo warns in a policy paper, systems using these extracted resources “may later be deployed in ways that further destabilise the very regions from which they originated. It is, as it were, frying a pig in its own fat.”²³⁶



²³⁰ Didier Makal, Denise Mahelo, “Cobalt mining for green energy risks women’s reproductive health in DRC,” *Mongabay*, 18 November 2024, <https://news.mongabay.com/2024/11/cobalt-mining-for-green-energy-risks-womens-reproductive-health-in-drc>.

²³¹ Sophie Richard, “A Guide to Gender and Mining,” German Federal Ministry for Economic Cooperation and Development (BMZ), 2024, <https://womenandmining.org/wp-content/uploads/2024/05/Guide-to-Gender-and-Mining.pdf>.

²³² UN Women, “Extractive Industries, Gender and Conflict in Asia Pacific,” March 2020, https://asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAsia/Docs/Publications/2020/03/ap-PVE-BLS19313_UNW_A2J-Publications_NRM_WEB.pdf.

²³³ African Commission on Human and Peoples’ Rights, “Submission Commissioner Solomon Ayele Dersso Focal Point on the ACHPR Study on AI and Other Technologies on Lethal Autonomous Weapon Systems To The United Nations Secretary-General in Terms of Un General Assembly Resolution 78/241,” May 2024, [https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_\(2024\)/78-241-African_Commission-EN.pdf](https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_(2024)/78-241-African_Commission-EN.pdf).

²³⁴ African Commission on Human and Peoples’ Rights, “Working Group on Extractive Industries, Environment and Human Rights Violations – 83OS,” 28 May 2025, <https://achpr.au.int/en/intersession-activity-reports/extractive-industries-environment-and-human-rights-violations-0>.

²³⁵ Muriel Alarcón, “Chile’s lithium boom promises jobs and money — but threatens a critical water source,” *Grist*, 26 March 2025, <https://grist.org/energy/chile-lithium-mining-salt-flat-water>.

²³⁶ Adebayo Okeowo, “The Human Rights Implications of Extracting Minerals and Personal Data from Africa for the Development of Military AI,” GC REAIM Expert Policy Note Series, May 2025, <https://hcass.nl/wp-content/uploads/2025/05/Okeowo.pdf>.

A feminist approach to the militarisation of data-intensive systems

In order to address the harms posed by the militarisation of data-intensive systems, it is necessary to understand the context in which they are being developed and used. As we showed in the first chapter, the religious and fascist ideologies defended by those behind these technologies influences why and how they are developed, and against who they are used. Grounded in the colonial philosophy of “Manifest Destiny,” data-intensive systems are key in operationalising the practice of “othering” through the categorisation and control of certain populations on the basis of gender, race, immigration status, class, among other identifiers. This shows how much of the militarisation of these systems is rooted in colonialism, racism, and patriarchy.

These ideologies also indicate that the actors promoting the use of these technologies within militaries, police, and border and immigration enforcement have specific ideas about why violence is necessary, what forms of harm and lethality are permissible, and against whom. Under the argument that certain populations need to be protected from other people or countries, they create new weapons and tools of violence. Militarisation becomes the main answer to issues that did not need a military response. This notion is further advanced due to the involvement of the private sector, which obtains ever-increasing profits with the creation of new weapons and systems. As we explained, venture capitalists’ involvement in war tends to exacerbate this situation, as the benefits they get from war can jeopardise efforts to prevent it.

In chapter two, we explored how data-intensive systems reinforce and amplify existing inequalities. Bias in data sets, design, and use can each lead to violent outcomes for certain groups of people, especially with the widespread adoption of these systems in warfare, law enforcement, and border control. They can lead, for example, to wrongful arrests because of misidentification. However, even if data-intensive systems were accurate, they can still be discriminatory due to their use targeted at historically marginalised communities. The disproportional deployment of these technologies against black communities in societies marked by structural racism is an example of this. This indicates that in addition to challenging the biases embedded in these systems, it is also necessary to challenge the biases that underpin policing and warfare institutions that use these technologies.

Additionally, it is necessary to include in this analysis the harms caused by the ways in which data is acquired in the first place. Data-intensive systems require “massive surveillance infrastructure that support their functionality and their constant demand for data.”²³⁷ And marginalised populations face harm yet again by being disproportionately subjected to surveillance. They not only are constantly surveilled—violating their rights to privacy and freedom of expression—but the data extracted without their consent is used to control and oppress them. When applied to the militarisation of data-intensive systems, this practice translates into their intensified use against women and gender-non confirming people, migrants, racialised communities, and people under military occupation. Our report highlights many examples of this.

In the third chapter, we analysed how data-intensive systems can be used to commit or facilitate gender-based violence (GBV). We rejected arguments that this would not be possible from a technical perspective; for example, some systems could be programmed to rape, others can generate sexual images without consent—as we are already seeing with the large language model Grok. Additionally, there are many instances in which data-intensive systems can have a facilitating role, particularly during and after conflicts, when the risk of GBV is already heightened.

We also investigated how norms of militarised masculinity that permeates the development and use of data-intensive systems can also result in GBV. Analysing cases related to drones and to decision-support systems, we highlighted that taking gender as key signifier of identity and exacting harm on that basis constitutes GBV. Additionally, the practice of targeting men as militants reinforces gender norms that frame men as “protectors” that are willing to take up arms, while women and others are weak and in need of this protection. These same gender norms also influence a culture of violence that sees the possession of militarised data-intensive systems as indicative of status; those who have it are able to protect, defend, oppress, or control those who don’t.

Overall, we argued that militarisation of data-intensive systems risks exacerbating GBV and discrimination, and reinforces harmful gender norms. The main purpose for the militarisation of these systems is to expand violence, which inevitably leads not only to physical violence against certain groups of people, but also to the exacerbation of structural violence and discrimination against them.

The structures that uphold patriarchy and gender inequality also affect how women, gender non-conforming people, and LGBTQ+ people experience the environmental harm caused by data-intensive systems. In chapter five, we demonstrated that the energy and water consumption by these systems, which heavily relies on the burning of fossil fuels, further deepens the climate crisis, which amplifies existing gender inequalities. Additionally, data centres can exacerbate existing inequalities in communities that already suffer from energy poverty and marginalisation. Women, gender non-confirming, and LGBTQ+ people are also disproportionately affected by the pollution caused by data centres. We also found that the intended reliance on nuclear power to provide energy for data centres perpetuates gender harms associated with the nuclear production chain. Finally, the hardware necessary for the operation of data-intensive systems relies on the extraction of minerals, which is associated with several gendered harms, including health and environment harms, as well as exposure to gender-based violence at mining sites.

The variety of harms caused by data-intensive systems suggests that strategies against them must be diverse, collective, creative, and multifaceted. There are already several initiatives taking place that tackle this issue from different perspectives. Groups have been opposing the constructions of data centres worldwide; in the United States, communities shut down or delayed the construction of at least

²³⁷ Privacy International, “How Data Drives the Militarisation of Tech,” 12 September 2025, <https://www.privacyinternational.org/long-read/5667/how-data-drives-militarisation-tech>.

20 data centre projects between April and June 2025, totalling 98 billion USD in value.²³⁸ In addition to the opposition to data centres, people are also organising against tech's social impact in multiple ways, including public protest, legal action, scholarly critique, and grassroots advocacy. Workers of tech companies have been active in protesting against their companies' unethical policies.²³⁹ Some groups have mapped and opposed technologies being employed in borders,²⁴⁰ others have investigated the harms of facial recognition technologies and called for a ban on them.²⁴¹ Organisations around the world are engaged in AI governance with the aim of preventing further human rights violations.²⁴² The Stop Killer Robots campaign has been advocating for a prohibition on autonomous weapons systems.²⁴³ This all shows that the resistance to the militarisation of data-intensive systems is already taking place, in both the local and international level, by a multitude of actors.

An important lesson from feminist thinking is that we must challenge the normalisation of militaristic values. Cynthia Enloe warns that "militarization does not always take on the guise of war" and that "many people can become militarized in their thinking, in how they live their daily lives, in what they aspire to for their children on their society, without ever wielding a rifle or donning a helmet."²⁴⁴ As she argues:

*Militarization is a step-by-step process by which a person or a thing gradually comes to be controlled by the military or comes to depend for its well-being on militaristic ideas. The more militarization transforms an individual or a society, the more that individual or society comes to imagine military needs and militaristic presumptions to be not only valuable but also normal.*²⁴⁵

This kind of thinking embedded in society values results in some people believing that the militarisation of data-intensive systems is inevitable. It is not. As Ray Acheson argues, we do not need to weaponise artificial intelligence and other technologies, especially when the risks are higher than any hypotheticals about positive benefits.²⁴⁶ "States should seriously question why the integration of AI into military systems is being considered at all, and work to stop it," states Acheson.²⁴⁷ Military tech companies might defend their development because they directly profit from it, and heavily militarised states might purchase and use these systems claiming they are necessary for security. But it does not have to be this way. States can refuse to engage in an arms race, and can chose to invest instead on collective care and environmental regeneration, which will prove to be far more effective in achieving safety and security and the overall wellbeing of populations. These are not unrealistic ideas; what is unrealistic is to think that the militarisation of data-intensive systems will benefit humanity.

²³⁸ Data Center Watch, "Q2 2025 update: 125% Surge in Data Center Opposition," March 2025–June 2025, <https://www.datacenterwatch.org/q22025>.

²³⁹ Kelvin Chan and Wyatt Grantham-Philips, "Google fires more workers who protested its deal with Israel," AP News, 23 April 2024, <https://apnews.com/article/google-israel-protest-workers-gaza-palestinians-96d2871f1340cb84c953118b7ef88b3f>.

²⁴⁰ "Migration + Tech Monitor," <https://www.migrationtechmonitor.com>.

²⁴¹ Amnesty International, "Ban the Scan," <https://banthescan.amnesty.org>.

²⁴² "EU #Protect Not Surveil," <https://protectnotsurveil.eu>.

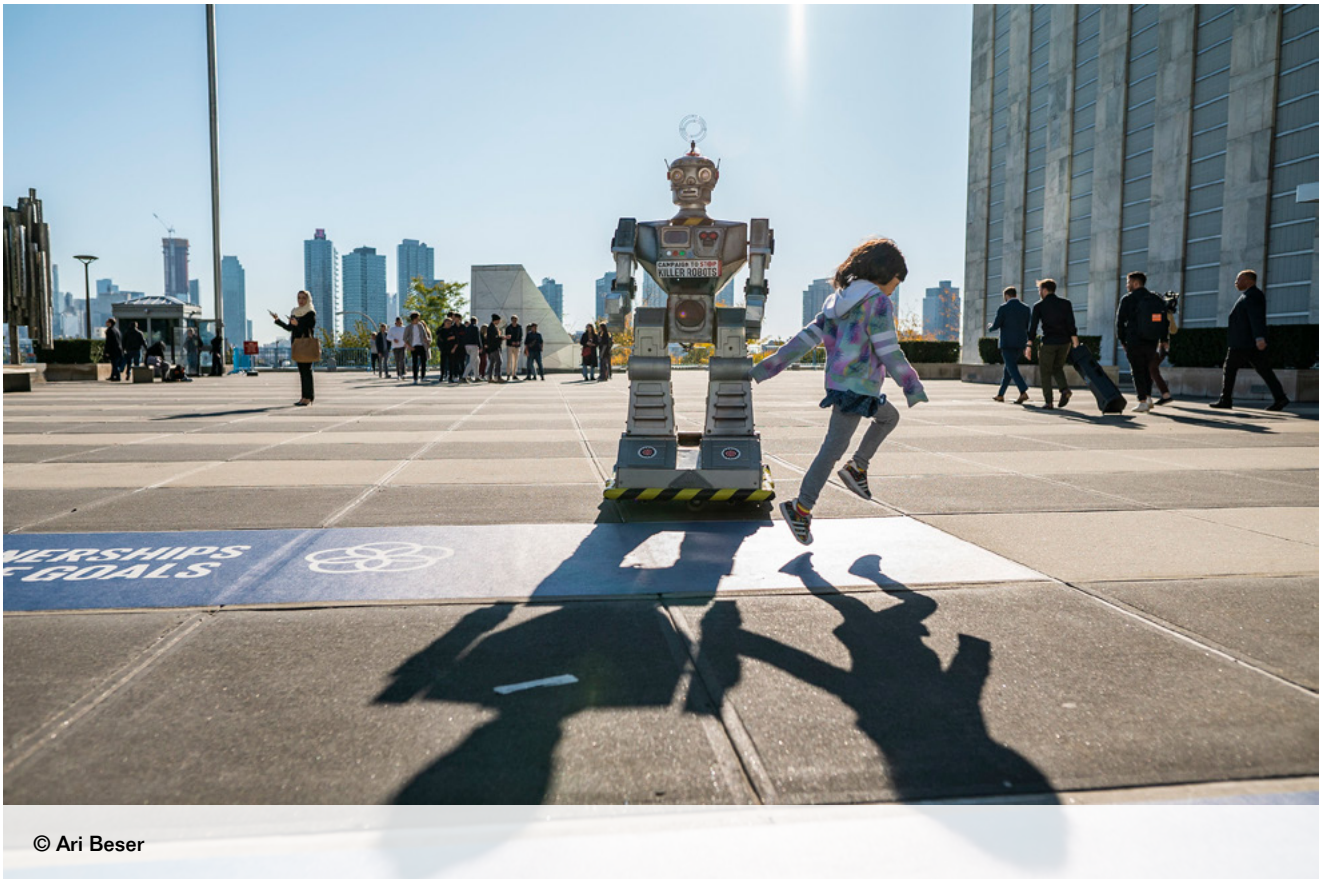
²⁴³ "Stop Killer Robots," <https://www.stopkillerrobots.org>.

²⁴⁴ Cynthia Enloe, *Manoeuvres—The International Politics of Militarizing Women's Lives* (Berkeley: University of California Press, 2000) p. 2.

²⁴⁵ Cynthia Enloe, *Manoeuvres*, p. 3.

²⁴⁶ Ray Acheson, "Presentation on the Legal and Humanitarian Implications of Bias in Military AI," Reaching Critical Will, 27 October 2025, <https://reachingcriticalwill.org/news/latest-news/18078-presentation-on-the-legal-and-humanitarian-implications-of-bias-in-military-ai>.

²⁴⁷ Ibid.



Tressie McMillan Cottom affirmed in a recent lecture that “when the people try to sell you the idea that the future is already settled, it is because it is deeply unsettled.”²⁴⁸ She argues that the promise of an artificial intelligent future is a collective anxiety that wealthy powerful people have about how they will be able to control people in the future. “If they can get us to accept that the future is already settled, that AI is already here, that the end is already here, then we will create that for them. My most daring idea is to refuse,” she says, adding that “refusing is actually the more hopeful, expansive vision of the future than the one that is telling us that the future is already settled and decided.”²⁴⁹ Indeed, by challenging the militarist values that influence our thinking, as put by Enloe, we see that the militarisation of data-intensive systems is not necessary; and by refusing to accept that our future is settled, and that these technologies are inevitable, as propose by Cottom, we can organise a resistance against these systems.

Intersectional feminism offers us an approach to do this. It directly opposes the colonial, racist, patriarchal and capitalist ideals that some people are more deserving of rights than others—which, as demonstrated in this report, are core ideological components to the militarisation of data-intensive systems. By grounding our resistance on the idea that everyone is free and equal and deserving of dignity and justice, we are able to set a course towards a more equitable future, where the profits of war do not dictate how society operates, and fight instead for a future where the wellbeing of people and the planet are always our main goal.

²⁴⁸ Tressie McMillan Cottom, “Daring Ideas for the Future – series in Detroit,” Urban Consulate, 17 December 2025, <https://www.instagram.com/reels/DSX3vFYDxxJ>.

²⁴⁹ Ibid.

Reaching Critical Will (RCW) is a project founded in 1999 to coordinate and enhance the engagement of activists and organisers in the work for disarmament at the United Nations.

RCW works for disarmament and the prohibition of many different weapon systems; confronting militarism and military spending; and exposing gendered aspects of the impact of weapons and disarmament processes with a feminist lens.

RCW also monitors and analyses international disarmament processes, providing primary resources, reporting, and civil society coordination at various UN-related forums.

www.reachingcriticalwill.org
disarm@wilpf.org



Reaching Critical Will