Myanmar's repressive use of AI to counter "terrorism"

Submission to the UN Special Rapporteur on counter-terrorism and human rights – August 2025

Executive summary

The military in Myanmar is engineering an AI-powered digital dictatorship under the false pretext of national security and counter "terrorism". This is not merely a collection of surveillance tools but a core component of the military's campaign of repression, designed to automate and scale up atrocity crimes against the opposition.

Myanmar has become a laboratory for 21st-century authoritarianism, and this report details its architecture, enablers, and the profound human rights consequences. Our investigation reveals that the military is using AI-powered technology for several distinct, repressive functions:

1. **To profile and control the population**: AI powers a national biometric database designed to eliminate anonymity by fusing personal, travel, and financial data. This creates comprehensive profiles that make any dissident activity transparent to the state.
2. **To hunt opponents in real-time**: AI-powered facial recognition cameras scan public spaces to automatically identify and track dissenters against "wanted lists", turning everyday life into a state of constant, automated surveillance.
3. **To censor and isolate the nation**: A "Great Firewall" uses AI to intercept private communications, understand coded language, and map dissident networks. The system blocks tools of evasion like VPNs, pushing people into a closed, State-controlled space.
4. **To automate atrocity crimes**: A technological pipeline leads from digital identification to physical harm, facilitating arbitrary arrests, torture, and attacks. The trajectory is toward an automated "kill chain" where algorithms could make lethal decisions without human oversight, enabling extrajudicial killing.

The report argues that the military is using AI as a human rights violation multiplier, amplifying harm through unprecedented scale, speed, and predictive capacity. It automates bias, erodes due process, and creates a "black box" system where people cannot challenge the algorithmic decisions that lead to their arrest, torture, or death.

This digital tyranny is not a domestic creation; it is fuelled by a global accountability vacuum. An international supply chain of AI companies from China, India, Israel, and the West continues to provide the necessary hardware and software, bypassing weak and outdated export controls.

Simultaneously, social media platforms like Telegram and Meta serve as vectors for military-backed AI-generated doxing, harassment, and incitement.

With domestic legal remedies completely absent, this report calls for urgent international action. We provide concrete recommendations to establish a regulatory framework for AI, enforce mandatory corporate due diligence, and pursue international justice to hold both the junta and its corporate enablers accountable for their complicity in AI-enabled atrocity crimes.

Introduction

Since the coup of February 2021, the military has accelerated the construction of a digital dictatorship designed to crush all opposition. It is systematically integrating artificial intelligence (AI) into a vast surveillance ecosystem, justifying these actions under the guise of protecting national security and countering "terrorism". This legal pretext is used to arbitrarily label the entire anti-coup, pro-democracy opposition, including political leaders and civil society, as "terrorists," thereby weaponising the State's digital infrastructure against them.

This submission to the United Nations review details the specific components of this emerging system, from AI-powered surveillance cameras and a national biometric database to sophisticated spyware and interception tools.[1] It examines how this AI-powered infrastructure, supplied by a global network of foreign companies, is not a tool for legitimate security but a core component of the military's campaign of repression that directly enables atrocity crimes. Furthermore, this analysis identifies the specific violations of international human rights law exacerbated by AI, exposes the profound failure of accountability mechanisms, and proposes concrete recommendations to address these grave issues.

Inside Myanmar's AI-powered digital dictatorship

Myanmar's military provides a comprehensive and devastating case study of how a State can systematically weaponise AI and digital technologies to enable human rights violations under the guise of countering "terrorism". The emerging system is not a collection of disparate tools but a deliberately integrated ecosystem designed for total population control.

The national database

The military is implementing a nationwide project to create an integrated biometric system mapping the entire population. The military justifies the project as necessary to tackle crime and protect national security.[2] The foundation of the project is the digitising of existing census data of up to 51 million individuals and collecting new biometric information, including

[1] UN OHCHR (2025), "Position Paper on the Human Rights Impacts of Using Artificial Intelligence in Countering Terrorism".
[2] Mizzima (2025), "China's Global Security Initiative and the Burma Junta's PSMS Surveillance"; Ministry of Information (2025), "Statement by General Maung Maung Aye".

fingerprints, iris scans, and face scans, along with personal details such as blood type, phone number, and email address.[3]

The system threatens to eliminate anonymity and create a central profile for every person, linking and cross-referencing disparate databases.[4] The integration of these databases transforms separate pools of data into a single, powerful weapon for control.[5]

The military has kept much of the project secret. State employees, external contractors, and businesses involved in building and operating the system face a wide range of criminal sanctions under the Official Secrets Act (1923) and Counter-Terrorism Law (2014) for disclosing any information. Nevertheless, some information about parts of the system has reached the public space, including the use of AI.

Digital system	Security justification	Potential AI functionality	Human rights risks
National registration identity card (NRIC, e-ID)	Identifying "terrorists" and applying discriminatory citizenship laws.	**Data fusion**: AI links an individual's unique identity to all other State-held data, creating a comprehensive profile.	**Privacy (Art. 17):** Eliminates anonymity and creates a permanent, State-controlled digital identity.
SIM card registration	Tracking "terrorists" and intercepting their communication.	**Network analysis and keyword scanning**: AI algorithms map social networks by analysing call data and automatically scan text messages for keywords like "protest" or "revolution".	**Freedoms of expression (Art. 19), association (Art. 22), and privacy (Art. 17):** Criminalises free communication and organisation, leading to collective targeting and arrests based on association.
Guest list management system (GLMS)	Tracking "terrorist" movements and identifying their support networks.	**Pattern-of-life analysis**: AI tracks an individual's movements by logging stays, learning "normal" behaviour and flagging any deviations as suspicious.	**Freedoms of movement (Art. 12) and association (Art. 22):** Creates a digital cage, making it nearly impossible for targeted individuals to travel, meet, or escape the country.
Myanmar advanced passenger processing system (MAPPS)	Tracking and preventing "terrorist" movements abroad.	**Predictive profiling**: AI analyses travel history to predict future movements and flag individuals at airports or border crossings, potentially based on their political or ethnic profile.	**Freedoms of movement (Art. 12) and non-discrimination (Art. 26):** Prevents targeted individuals from leaving the country and enables discriminatory targeting based on travel patterns.

[3] Engage Media (2023), "Digital dictatorship in Myanmar: Biometric data collection sparks fear among activists".
[4] APC (2024), "Digital struggle and resistance in the Myanmar revolution".
[5] IFEX (2025), "Myanmar military builds a surveillance state".

National service information management system (NSIMS)	Identifying and clearing potential military recruits.	**Automated targeting**: AI scans the national database to automatically identify and target individuals eligible for forced military conscription.	**Rights to life (Art. 6), liberty (Art. 9), and freedom of conscience (Art. 18):** Automates forced conscription into a military committing atrocity crimes, forcing individuals to participate in violence.
Person scrutinising and monitoring system (PSMS)	Identifying and apprehending "terrorists".	**Real time data fusion**: AI integrates data from all other systems in real-time, linking a face from a CCTV camera to an identity, phone records, and location history.	**Right to liberty (Art. 9):** Facilitates arbitrary arrest by providing a complete target profile and can be used to enable torture during interrogations.

The true power of these tools lies in their integration. Data from these disparate sources is fed into a central system, allowing the military to build a detailed and multifaceted profile of any individual. With a single scan of an identity card at a checkpoint, authorities can potentially pull up an individual's travel history, recent communications, financial transactions, and political affiliations. This blurring of the lines between physical and digital life makes it possible to profile, track, and target anyone deemed a threat, creating a pervasive system where every interaction with the State or a digital service becomes a potential point of capture.

The system is already being used and tested on a large scale. For instance, the national census in October 2024 was used to identify and track dissidents, with a particular focus on State employees who joined the Civil Disobedience Movement (CDM) after the coup.[6] With their identities flagged in the military's system and cross-referenced across databases, they face constant risk to their human rights.

The "Safe City" projects

The military is building specific AI-powered capacities upon the broader project to tackle national security threats, including "Safe City" initiatives in major urban centres.[7] The military is expanding the installation of CCTV systems in cities, including the capital, Naypyidaw, as well as Yangon and Mandalay, with plans for nationwide expansion across all 14 states and divisions.[8] These initiatives, some of which started before the coup, have been accelerated to strengthen the military's crackdown on dissent.[9]

The technology used is highly intrusive and uses artificial intelligence. The camera systems, supplied by Chinese technology businesses such as Huawei, Dahua, and Hikvision, are equipped

[6] Tech Policy Press (2025), "Fourth Year Under Myanmar Military's Digital Iron Curtain: A Reflection on Digital Repression and the Path Forward".
[7] Myanmar Now (2022), "Military council installs Chinese-made surveillance cameras in major cities".
[8] Myanmar Now (2020), "Nay Pyi Taw to install surveillance cameras at a cost of 4 billion kyats"; Asia Pacific Foundation of Canada (2022), "Myanmar's Military Government Installs Facial Recognition Cameras in Major Cities".
[9] Human Rights Watch (2021), "Myanmar: Facial Recognition System Threatens Rights".

with AI-powered facial recognition and licence plate recognition capabilities.[10] This allows authorities to automatically scan faces and vehicles in public spaces in real-time, checking them against "wanted lists" of dissidents, including civil society, journalists, and political opponents.[11] The purpose is to detect connections between targeted individuals, recognise and intercept cars and motorcycles, and identify safe houses and other gathering spots.[12] It turns public squares, streets, and community spaces into areas of constant, automated monitoring.

The military has amplified the power of this technology by simultaneously removing legal protections. On 13 February 2021, the military unlawfully suspended key sections of the Law Protecting the Privacy and Security of Citizens (2017), effectively removing protections against warrantless surveillance, search, and seizure.[13] In August 2025, it also suspended other sections of the law in the countdown to future elections.

The interception and censorship dragnet

To complete its digital surveillance state, the military has moved to seize complete control over the electronic flow of information and communication within the country. Human Rights Myanmar has termed this "The Great Firewall of Myanmar".[14] It has been achieved by embedding AI into censorship technology and telecommunications systems, enabling a more intelligent and automated form of repression that goes far beyond simple website blocking.

The core of this system is advanced surveillance technology, including interception gateways (LIGs), deep packet inspection (DPI), and spyware.[15] Systems like the Tiangou Secure Gateway (TSG) and Cyber Narrator from Geedge Networks provide Myanmar's interception infrastructure and rely on AI to make it truly powerful.[16] Instead of merely scanning for specific keywords like "revolution," AI models can perform semantic and sentiment analysis on intercepted traffic, and learn too. This allows the system to adapt to emerging trends and understand messages, flagging conversations that are critical of the regime even if they use coded language or sarcasm.[17] Furthermore, AI-driven network analysis can be used to map relationships between individuals, identifying influential organisers and entire dissident networks based on the frequency and patterns of their communication.

This AI-enhanced interception is paired with a dynamic and predictive censorship campaign. After banning popular digital platforms like Facebook, filtering media outlets, and targeting VPNs, the military uses AI-powered traffic analysis to enforce these blocks.[18] Rather than relying on static blocklists, AI systems identify the unique data signatures of encrypted VPN traffic in real-time, allowing them to block these tools of evasion as they are being used. This active enforcement is designed to push people away from the global internet and towards the military's favoured platforms such as Telegram and State-controlled MySpace Myanmar. Within

[10] Asia Pacific Foundation of Canada (2022), "Myanmar's Military Government Installs Facial Recognition Cameras in Major Cities".
[11] Human Rights Watch (2021), "Myanmar: Facial Recognition System Threatens Rights".
[12] Asia Pacific Foundation of Canada (2022), "Myanmar's Military Government Installs Facial Recognition Cameras in Major Cities".
[13] Human Rights Watch (2021), "Myanmar: Facial Recognition System Threatens Rights".
[14] Human Rights Myanmar (2024), "The great firewall of Myanmar".
[15] Business and Human Rights Resource Centre (2023), "Statement calls out companies for allegedly helping junta build an attack & surveillance infrastructure; incl. company statements".
[16] Justice for Myanmar (2024), "The Myanmar junta's partners in digital surveillance and censorship".
[17] IFEX (2025), "Myanmar military builds a surveillance state".
[18] Freedom House (2024), "Freedom on the net Myanmar"; APC (2024), "Digital struggle and resistance in the Myanmar revolution".

such a closed system, AI can be used not just to block external information but to analyse behaviour, identify dissenters, and amplify pro-military propaganda.

This system is supported by the military's consolidation of control over the country's physical telecommunications infrastructure. By creating an environment of extreme pressure and risk, the military forced foreign businesses like Norway's Telenor to leave, leaving all major providers under direct or indirect military control.[19] This control ensures that the AI-powered infrastructure needed is fully compliant with the military's orders.

AI's impact on digital rights

The military's deployment of AI is not merely an incremental upgrade to its existing capabilities to target dissent under the banner of countering "terrorism". It is a fundamental transformation that acts as a human rights violation multiplier. AI amplifies the harm of digital repression through several interconnected vectors.

Multiplier vector	Description	Human rights risks
Scale	Expands surveillance from targeting individuals to monitoring entire populations simultaneously.	Enables mass violations of the right to privacy (Art. 17) and creates a chilling effect on the freedoms of expression (Art. 19), assembly (Art. 21), and association (Art. 22).
Speed	Operates at a velocity that makes meaningful human review or oversight of its decisions impossible.	Undermines the right to an effective remedy (Art. 2) and principles of due process (Art. 9) as violations occur faster than they can be challenged.
Prediction	Allows the state to act pre-emptively against individuals based on an algorithmic assessment of future risk.	Erodes the presumption of innocence (Art. 14.2) and the right to liberty (Art. 9), shifting to pre-emptive control.
Automated bias	AI systems trained on historically prejudiced data automate and legitimise discrimination.	Entrenches and scales up violations of the right to non-discrimination (Art. 26), providing a false justification for biased actions.
Automated error	A single flaw in an algorithm or dataset can be replicated millions of times, leading to systemic, mass-produced errors.	Leads to mass wrongful targeting and detention, undermining the right to liberty and security of

[19] Chiang Mai University (2025), "Navigating Coup Dynamics in Myanmar's Digital Era: The Responsibilities of Private Companies in Managing State Digital Assets".

		person on an industrial scale (Art. 9).
Opacity	The "black box" nature of many AI systems makes it impossible to scrutinize their decision-making processes.	Destroys the right to a fair trial (Art. 14), as individuals cannot challenge evidence they cannot understand.

Together, these vectors create an environment where the military can enforce compliance and punish dissent with a significant degree of automated efficiency. The use of this AI-powered system to counter "terrorism" has resulted in severe violations across a spectrum of human rights.

Privacy, expression, and association

The military has already laid the groundwork for mass surveillance. It uses real-time facial recognition from CCTV cameras to identify and track protesters, and AI-powered monitoring tools to identify dissenters online. Financial surveillance systems are used to track money being sent to opposition movements.[20] At least 1,657 people were arrested between March and May 2025 using AI-powered targeting technology.[21] The fusion of data creates a powerful chilling effect, eroding the right to privacy (ICCPR Art. 17) and systematically suppressing the freedoms of expression (Art. 19), assembly (Art. 21), and association (Art. 22) by making people justifiably afraid to communicate, organise, or protest.

The military is likely to evolve this system from one of reactive surveillance to one of pre-emptive social control. By applying AI to conduct sophisticated "pattern-of-life" analysis on location data, communication metadata, and financial transactions, the military will be able to predict who is likely to support the opposition. Furthermore, the military will likely use AI to create and spread hyper-realistic propaganda and disinformation at a scale and speed that is impossible to counter, completely dominating the information environment. This would create a digital panopticon where the mere thought of opposition carries the risk of State intervention.

Discrimination

The use of technology to incite hatred against minority groups is well-documented in Myanmar, particularly the use of social media algorithms to amplify anti-Rohingya content.[22] Pro-military groups already engage in doxing and harassment, especially on rarely policed platforms like Telegram, and automated tools that mimic real users are used to amplify these attacks. This, combined with the known inaccuracies of facial recognition technology for ethnic minorities, has created a high risk of discriminatory targeting.

The military is positioned to use AI to create a system of automated apartheid. By training AI on its biased data, the military can build predictive profiles that equate ethnicity with a threat level. This could be used to automatically deny services, restrict movement at smart checkpoints, or

[20] Democratic Voice of Burma (2025), "At least 4 people were arrested in Karenni through PSMS in May".
[21] People's Spring (2025), "Military council is starting arrests using the technology of personal investigation and monitoring system".
[22] Global Witness (2021), "Algorithm of harm: Facebook amplified Myanmar military propaganda following coup".

disproportionately target minority communities for violent "counter-terrorism" operations. AI could also be used to generate automated, personalised harassment and doxing campaigns against any individual flagged as a threat, creating a digital environment of constant fear and intimidation.

Life, liberty, and security

The military currently operates a technological pipeline that leads directly to arbitrary detention and atrocity crimes. An individual identified by CCTV at a protest or through their online activity can be detained or attacked. Interrogations involve torture based on data extracted from phones using AI, in the hope of cracking networks and forcing confessions.[23] In Myanmar's conflict zones, the increasing use of drones for indiscriminate attacks on civilian areas already constitutes a serious violation of international humanitarian law.[24] Internet shutdowns frequently imposed prior to an attack are designed to stop people from warning each other and to hide human rights violations being committed.[25]

The logical progression in Myanmar is towards greater autonomy in lethal systems. The military is likely seeking AI technology that can create semi-autonomous weapons systems, particularly in drone technology, capable of attacking targets with minimal human oversight. The military's lack of financial resources is likely to drive it towards cheaper, less reliable, and therefore more dangerous technology. Furthermore, the integration of AI could lead to the creation of an automated "kill chain", where an algorithm assigns a threat score to individuals in real-time. Based on this score, the system could make autonomous decisions about who to arrest, detain, or even target for lethal action, completely removing due process and creating a system of AI-enabled extrajudicial killing.

The enablers of AI-powered repression

The military's AI-powered authoritarian response to "terrorism" is not built in a vacuum. It is enabled by a network of State and private actors who provide the legal cover, technological components, and digital platforms necessary for AI-powered repression to function.

Using the law to legitimise AI-powered repression

The military has systematically weaponised the country's legal framework to provide a false appearance of legitimacy for its AI-powered counter "terrorism" response. Myanmar's laws are not just about general digital control but are designed to authorise the mass data collection that is essential to train and operate AI surveillance and censorship models. A key instrument in this effort is the Cybersecurity Law (2025), officially enacted in January 2025 and operational in July 2025.[26] Its mandate for service providers to store user data for up to three years, localise their

[23] U.S. State Department (2021), "Burma 2021 human rights report".
[24] The Guardian (2025), "Myanmar military junta using European technology for drone attacks, report says".
[25] Tech Policy Press (2025), "Fourth Year Under Myanmar Military's Digital Iron Curtain: A Reflection on Digital Repression and the Path Forward".
[26] Human Rights Myanmar (2025), "Myanmar's cyber law a serious threat to privacy, speech, and security".

digital servers within the country, under threat of vague criminal sanctions, will create a vast, legally-sanctioned reservoir of data for AI analysis.

The Cybersecurity Law (2025) is reinforced by a Lawful Interception Framework promulgated in March 2023 as an addendum to the Counter-Terrorism Law (2014), and which gives a military-controlled committee unchecked power to feed real-time data directly into AI systems for monitoring and analysis.[27] Together, these laws, combined with the critical suspension of the Law Protecting the Privacy and Security of Citizens (2017), create a situation where fundamental rights are suspended by decree.[28] They are a clear example of "rule by law", where legal instruments are crafted not to protect people but to provide a legal pretext for an AI-powered authoritarian State, completely violating the principles of legality, necessity, and proportionality required under international human rights law.

The international supply chain

The military's technological ambitions are made possible by a global, largely unregulated market for digital and AI-powered repression technology.

- **Chinese state-affiliated private businesses** have provided the large-scale infrastructure for the military's AI-powered surveillance and censorship systems.[29] This includes Huawei, Dahua, and Hikvision for the Safe City CCTV and facial recognition systems; Geedge Networks for the deep packet inspection (DPI) firewall; and China National Electronics Import & Export Corporation (CEIEC) for location tracking systems.[30] Such businesses can act as proxies for foreign states, importing authoritarianism and exploiting legal loopholes.
- **Indian businesses** associated with India's Aadhaar system, the world's largest biometric identity programme, have reportedly provided expertise and data-collecting tools to the military.[31]
- **Western businesses** have reportedly supplied more specialised AI tools. This includes AI-powered digital forensic, surveillance, drone, and phone-hacking technology from firms like Sweden's MSAB, Canada's OpenText and Magnet Forensics, X1 and Datawalk from the U.S., and the Israeli businesses Cellebrite and Elbit.[32]

This transfer of technology demonstrates how easily existing sanctions and export controls are bypassed, particularly as AI software and complex algorithms are often not properly classified as "dual-use" goods, creating a significant loophole. Sales are reportedly conducted through complex supply chains that hide the final end-user, allowing manufacturers to claim

[27] IFEX (2025), "Myanmar military builds a surveillance state".
[28] Human Rights Watch (2021), "Myanmar: Facial Recognition System Threatens Rights".
[29] Justice for Myanmar (2024), "The Myanmar junta's partners in digital surveillance and censorship".
[30] Asia Pacific Foundation of Canada (2022), "Myanmar's Military Government Installs Facial Recognition Cameras in Major Cities".
[31] Tech Policy Press (2025), "Fourth Year Under Myanmar Military's Digital Iron Curtain: A Reflection on Digital Repression and the Path Forward".
[32] Carnegie Endowment for International Peace (2023), "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses"; Justice for Myanmar (2021), "Justice For Myanmar publishes details of Myanmar's tools of digital surveillance and repression"; Organized Crime and Corruption Reporting Project (2021), "Myanmar Security Forces Using Western Surveillance Tech Against Civilians"; Business and Human Rights Resource Centre (2021), "Use of MSAB digital forensic tools in Myanmar exposes gap between EU tech investment & regulation".

ignorance.[33] The ease with which the military can acquire these AI technologies reveals the failure of current export controls and corporate accountability systems.

The role of telecommunications operators is also critical, as they control the infrastructure through which data flows. The post-coup exits of foreign firms in Myanmar like Telenor and Ooredoo are highly significant, as the transfer of their sensitive user data to military-linked owners provides the primary fuel for the military's AI models, putting millions of people at risk of being targeted by algorithmic analysis.[34]

The role of algorithmic platforms in amplifying harm

Social media platforms remain a key arena where AI directly enables the military's crackdown on opposition movements under the pretext of countering "terrorism". The failures of these platforms are not simply matters of policy but are rooted in the very AI systems that drive their business models, which are exploited by the military to identify, vilify, and target dissent.

Meta (Facebook's parent company) is a prime example. Its core business model is driven by an engagement-based AI recommendation algorithm. In the context of Myanmar, this system has repeatedly amplified inflammatory, discriminatory, and pro-military propaganda.[35] This is not a new problem as Meta has admitted its algorithms substantially contributed to the spread of anti-Rohingya hate prior to the 2017 atrocity crimes.[36] Even after banning the military, its core AI continued to promote harmful content, demonstrating a fundamental vulnerability that allows the military and its proxies to shape the narrative and create a permissive environment for their crackdown.[37]

Furthermore, social media platforms' reliance on AI for content moderation is often inadequate.[38] These automated systems consistently fail to understand the linguistic and cultural nuances of local languages, allowing problematic content such as coded hate and incitement against dissenters or minorities to evade detection.[39] This creates a safe space for pro-military actors to operate.

As Meta has become a more hostile space for the military, this activity has migrated to platforms with even weaker moderation controls, such as Telegram. This has become a primary channel for pro-military forces to conduct doxing campaigns and issue death threats against dissenters. By allowing these coordinated harassment campaigns to flourish, the platforms become essential tools for the military's repressive counter "terrorism" strategy.[40] Their core AI systems are not passive conduits for information but active enablers of the military's information war.

---

[33] Organized Crime and Corruption Reporting Project (2021), "Myanmar Security Forces Using Western Surveillance Tech Against Civilians".
[34] Chiang Mai University (2025), "Navigating Coup Dynamics in Myanmar's Digital Era: The Responsibilities of Private Companies in Managing State Digital Assets".
[35] Amnesty International (2022), "Myanmar: Facebook's systems promoted violence against Rohingya; Meta owes reparations".
[36] New York Times (2018), "Facebook Admits It Was Used to Incite Violence in Myanmar".
[37] Chiang Mai University (2025), "Navigating Coup Dynamics in Myanmar's Digital Era: The Responsibilities of Private Companies in Managing State Digital Assets".
[38] Amnesty International (2022), "Myanmar: Facebook's systems promoted violence against Rohingya; Meta owes reparations".
[39] Carnegie Endowment for International Peace (2023), "Facebook, Telegram, and the Ongoing Struggle Against Online Hate Speech".
[40] Carnegie Endowment for International Peace (2023), "Facebook, Telegram, and the Ongoing Struggle Against Online Hate Speech".

The AI accountability gap

The military's AI-powered repression thrives in an environment of legal and regulatory failure. This accountability gap allows all actors, including both States and businesses, to act with near-total impunity, systematically violating human rights without consequence.

The lack of domestic oversight for AI

Within Myanmar, there is no possibility of legal accountability for AI-powered repression.[41] The military controls all branches of government, meaning there is no independent body capable of investigating human rights violations or even defining "terrorism". This problem is magnified when the harm is caused by AI. For the thousands of victims of AI-enabled violations, the domestic legal system offers no hope of remedy because it is fundamentally unequipped to address their claims. Regulatory institutions are dominated by current and former military officers who lack relevant backgrounds. Judges are not trained in technology, and there are no specialist courts. What limited evidentiary requirements exist are based on static print-outs, even for digital cases. Judicial institutions are unwilling to consult experts and, if they do, only seek advice from prejudiced law enforcement technical teams. It is also impossible to have due process when the primary evidence against a person is the output of a secret, opaque algorithm. There is no way to challenge algorithmic bias or error within a system that denies even the most basic principles of due process.

The weakness of international sanctions against AI

International accountability mechanisms have proven completely ineffective at stopping the flow of AI-powered repression technology. Existing arms embargoes and sanctions regimes are designed to control the transfer of physical hardware, not intangible software, algorithms, and datasets. AI systems are often not classified as "military" or "dual-use" goods, creating a significant loophole that technology companies exploit.[42] This lack of accountability creates a system of incentives that encourages the sale of AI technology to repressive regimes.[43] The financial benefit of selling a facial recognition system or a digital forensic tool to a regime like Myanmar's currently carries a very low chance of legal or financial penalty. This market logic will continue to fuel AI-powered repression until the consequences for complicity are made sufficiently severe.

Failure of due diligence

The UN Guiding Principles on Business and Human Rights (UNGPs) establish an authoritative global standard requiring all businesses to respect human rights. This entails a responsibility to avoid causing or contributing to adverse human rights impacts and to prevent or mitigate impacts that are directly linked to their operations, products, or services through their business

[41] Free Expression Myanmar (2023), "Myanmar military's 'justice' system".
[42] The Guardian (2025), "Myanmar military junta using European technology for drone attacks, report says".
[43] The Guardian (2025), "Myanmar military junta using European technology for drone attacks, report says".

relationships.[44] To meet this responsibility, businesses must conduct ongoing human rights due diligence to identify, prevent, and mitigate the human rights risks associated with their products, particularly concerning end-use by State clients.[45] Businesses must conduct heightened due diligence when operating in conflict-affected contexts.[46]

The continued sale of certain AI technology to regimes with well-documented records of gross human rights violations, such as the military, represents a manifest failure of this due diligence process. Public statements on human rights by companies like Huawei and Hikvision are rendered meaningless by their business practices.[47] This failure places these businesses in a zone of significant legal risk. Under international law, complicity in a crime can arise from knowingly providing practical assistance or encouragement that has a substantial effect on the commission of that crime.[48] By providing the very tools of repression to a military actively engaged in a campaign of terror, with full knowledge of its conduct, these businesses risk being held legally complicit in the crimes against humanity being committed.

No international remedy for victims of algorithmic harm

The complete absence of accessible domestic remedies makes the role of international justice essential.[49] For the people of Myanmar, accountability can only come from the outside. This demand must extend beyond State actors to include the corporate enablers of the military's AI-powered crimes. The legal actions and calls for reparations directed at Meta by Rohingya groups serve as an important precedent, establishing the principle that technology companies can and should be held responsible for the human rights harms their AI business models contribute to.[50] Any meaningful framework for remedy must address the entire network of complicity, from the companies that build the AI models to the platforms that deploy them and the states that weaponise them.

Conclusion

The situation in Myanmar presents a clear and comprehensive example of how a State can use artificial intelligence as a weapon under a counter "terrorism" and national security pretext to systematically violate human rights and enable the commission of atrocity crimes. The military's digital dictatorship is not just an addition to its campaign of repression, but is a core component of it. This technological system is used to violate the full range of human rights, from privacy and expression to the fundamental right to life, with a complete absence of oversight, due diligence, or remedy.

[44] United Nations Global Compact (2011), "Guiding Principles for Business and Human Rights".
[45] United Nations Development Programme (2021), "Human Rights Due Diligence: An Interpretive Guide".
[46] United Nations Development Programme (2022), "Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts: A Guide".
[47] Huawei (2025), "Respecting Human Rights"; Hikvision (2025), "Global human rights policy".
[48] United Nations Global Compact (2025), "Principle Two".
[49] Free Expression Myanmar (2023), "Myanmar military's 'justice' system".
[50] Amnesty International (2022), "Myanmar: Facebook's systems promoted violence against Rohingya; Meta owes reparations".

Recommendations

- **Create a dedicated regulatory framework**: Recommend an international legal framework to govern the sale, transfer, and use of AI and surveillance technologies in counter-terrorism contexts. This should establish a presumption against providing such tech to States like Myanmar that disregard the rule of law and human rights.
- **Mandate human rights due diligence**: Urge all States to enact and enforce mandatory human rights due diligence laws for tech companies. This must require businesses to assess, mitigate, and remedy the human rights impacts of their products, with significant legal and financial penalties for non-compliance.
- **Strengthen export controls and sanctions**: Expand the "dual-use" goods definition in export controls to explicitly include advanced surveillance software, data-processing tech, and components for autonomous weapons. Sanctions must target not only State perpetrators but also corporate intermediaries in the supply chain of repression.
- **Support digital resistance and civil society**: Call on States and tech companies to provide direct technical, financial, and political support to civil society, journalists, and human rights defenders in countries like Myanmar. This includes developing secure communication networks and digital security tools to help people resist repression and document abuses.
- **Prioritise international justice**: Prioritise international accountability for AI-enabled atrocity crimes where the domestic rule of law has collapsed. This includes supporting ICC investigations, encouraging universal jurisdiction in national courts, and finding new legal avenues to hold both State and corporate actors accountable.