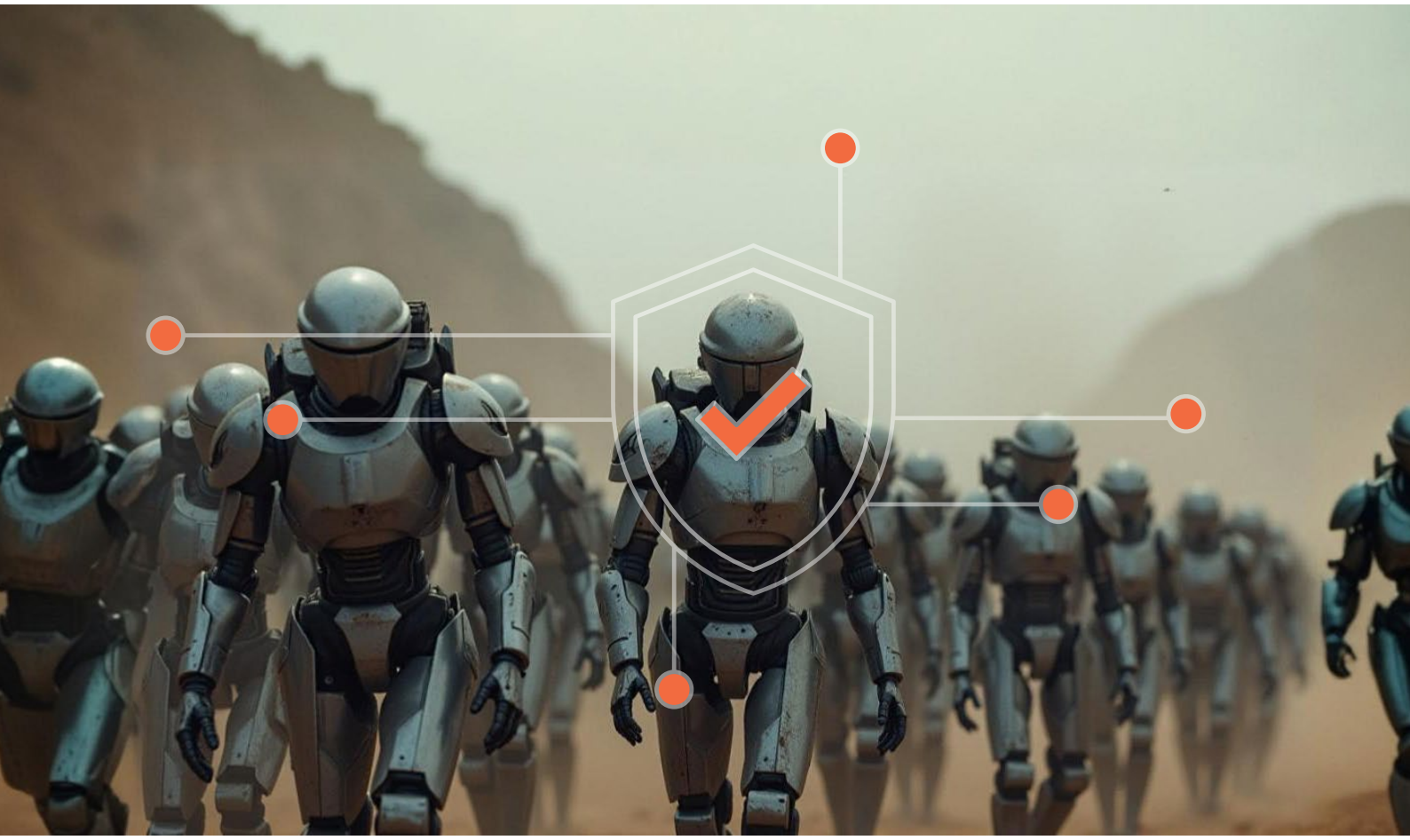


CLOSING THE GAP:

Protecting Activists from Authoritarian Use of AI

CLOSING THE GAP:
PROTECTING ACTIVISTS FROM AUTHORITARIAN USE OF AI

BRIDGING THIS DIVIDE IS ESSENTIAL NOT ONLY TO PROTECT HUMAN RIGHTS BUT TO ENSURE THAT AI EVOLVES IN WAYS THAT UPHOLD TRANSPARENCY, JUSTICE, AND FREEDOM.

Artificial Intelligence (AI) is transforming societies around the globe, ushering in new possibilities for innovation and advocacy. However, it has also become a battleground between autocrats and activists. Authoritarian regimes, armed with vast resources and cutting-edge AI tools, have gained a significant upper hand in surveilling, targeting, and suppressing dissent. Meanwhile, activists often operate with limited resources, outdated technology, and delayed access to the training and tools they need to fight back.

This resource gap leaves activists vulnerable, prevents them from shaping the development of AI, and hinders their ability to counter oppression effectively. Bridging this divide is essential not only to protect human rights but to ensure that AI evolves in ways that uphold transparency, justice, and freedom. This article examines how autocrats exploit AI to maintain power, how activists are working to close the gap, and what must be done to empower movements with the resources, training, and support they need to reclaim AI as a force for promoting positive social change.

HOW AI IS WEAPONIZED AGAINST ACTIVISTS

Autocrats and oppressive governments are increasingly utilizing AI to monitor, target, and silence activists, undermine democratic processes, and consolidate power. Through mass surveillance, facial recognition, disinformation campaigns, predictive policing, online harassment, and electoral manipulation, AI has become a potent tool for authoritarian control.

Most notably, AI-powered facial recognition systems are a cornerstone of modern surveillance. Governments in countries like China have implemented vast networks of AI-driven cameras capable of identifying individuals in real time. The technology is often used to monitor public gatherings, protests, and even day-to-day activities, making it nearly impossible for activists to operate anonymously.

China has used AI technologies to target the Uyghur community under the guise of counter-terrorism.[1] Protesters in Hong Kong famously employed tactics like wearing masks, shining lasers at cameras, and using umbrellas to thwart facial recognition during demonstrations in 2019. Despite these efforts, reports emerged of individuals being arrested based on AI-assisted identification. In Russia, AI surveillance has been leveraged to monitor anti-government protesters. Moscow's expansive facial recognition network was reportedly used to track and detain individuals participating in anti-Putin demonstrations. The chilling effect of such technologies cannot be overstated, as they deter activism and dissent through fear of retribution.[2]

THROUGH MASS SURVEILLANCE, FACIAL RECOGNITION, DISINFORMATION CAMPAIGNS, PREDICTIVE POLICING, ONLINE HARASSMENT, AND ELECTORAL MANIPULATION, AI HAS BECOME A POTENT TOOL FOR AUTHORITARIAN CONTROL

1 https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450(SUM01)_EN.pdf

2 https://restofworld.org/2024/facial-recognition-government-protest-surveillance/

What is worse, the technology is being exported and shared around the world.[3]

Predictive policing tools powered by AI that analyzes data from various sources in order to forecast potential crimes or unrest are also a growing threat for activists. While this technology has legitimate uses, it has been widely criticized for perpetuating systemic bias and enabling authoritarian control. Activists often find themselves unjustly flagged as threats based on biased algorithms or intentionally manipulated data. In Egypt, for instance, the government has utilized AI to monitor social media for signs of dissent.[4] Keywords, hashtags, and online activity are analyzed to predict and preemptively suppress protests. Similarly, in Bahrain, activists have been targeted using spyware and AI-driven monitoring systems, leading to arrests and harsh penalties.

AI-generated disinformation is another weapon in the arsenal of oppressive regimes, and one that has received a lot of attention. Sophisticated algorithms can quickly create deepfake videos, fake social media accounts, and AI-generated content to spread propaganda, discredit activists, or sow confusion among opposition groups at a dizzying rate. For example, during protests in Myanmar following the 2021 military coup, AI-driven bots flooded social media platforms with pro-junta narratives and targeted harassment of activists. These campaigns aimed to drown out dissenting voices and fracture solidarity among protesters. Activists often face an uphill battle against such coordinated efforts, which undermine trust and amplify fear.

AI-GENERATED DISINFORMATION IS ANOTHER WEAPON IN THE ARSENAL OF OPPRESSIVE REGIMES

AI is also employed to censor dissenting voices online. In countries like Iran and Saudi Arabia, advanced AI systems are used to monitor and automatically delete content deemed critical of the regime.[5] In some cases, activists' accounts are flagged, suspended, or shadow-banned, limiting their ability to organize and spread awareness. For instance, during the 2022 protests in Iran sparked by the death of Mahsa Amini, activists reported widespread internet blackouts and algorithmic suppression of protest-related content on social media platforms. AI-driven censorship tools make it harder for activists to document and share human rights abuses.

AI is in addition being weaponized to supercharge online harassment, creating hostile digital environments that deter people from engaging in democratic processes. By deploying AI-driven bots and algorithms, regimes flood social media platforms with targeted harassment, trolling, and disinformation aimed at activists, journalists, and opposition figures. These campaigns are not only designed to intimidate individuals but also to sow division, erode trust in democratic institutions, and discourage public discourse. In Belarus, the government has employed AI-driven technologies to suppress dissent and control the narrative. For instance, state-sponsored online trolls have been used to harass independent media outlets, creating a climate of fear and self-censorship among journalists and activists.[6] These tactics not only intimidate activists but also deter the general populace from participating in democratic processes, fearing retribution.

Finally, though certainly not least, AI-driven disinformation campaigns flood social media with propaganda, fake news, and deepfakes, creating confusion and discrediting opposition candidates. In Zimbabwe's 2018 election, reports indicated that AI-powered bots were used to spread misinformation about voter registration deadlines, leading to voter suppression in opposition strongholds.[7] Similarly, in Russia, AI has been used to manipulate public opinion by amplifying state-sponsored narratives while silencing dissent, as seen in the 2021 parliamentary elections where bots and trolls discredited opposition leaders and fabricated narratives to justify election outcomes. In Venezuela, the government allegedly used AI to analyze voter data, gerrymander districts, and target individuals with pro-regime messaging to maintain control.

3 https://www.reuters.com/world/china/fears-digital-dictatorship-myanmar-deploys-ai-2021-03-18/

4 https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450(SUM01)_EN.pdf

5 https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf

6 https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence?utm_source=chatgpt.com

7 https://www.icfj.org/news/fact-checking-zimbabwes-election-how-online-misinformation-was-tracked-during-zimbabwes-long

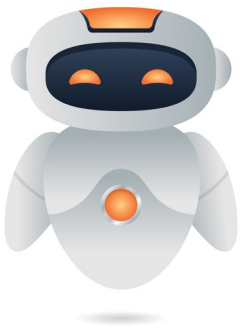
HOW ACTIVISTS ARE USING AI TO PROTECT THEMSELVES AND ADVANCE HUMAN RIGHTS

AS SURVEILLANCE INTENSIFIES, ACTIVISTS ARE USING AI-POWERED TOOLS TO ENHANCE THEIR DIGITAL SECURITY.

Despite these challenges, activists and movements worldwide are beginning to harness AI as a force for good. From encryption tools to AI-driven human rights documentation, innovative uses of AI are helping activists counter repression and protect their communities.

A key area is the use of AI for digital security and privacy. As surveillance intensifies, activists are using AI-powered tools to enhance their digital security. Encryption apps like Signal use AI to ensure secure communication, protecting activists from government surveillance. These tools encrypt messages end-to-end, making it nearly impossible for third parties to intercept or decipher communications. Additionally, AI is being used to detect spyware and malicious attacks. Tools like Amnesty International's Mobile Verification Toolkit help activists identify and mitigate risks from spyware like Pegasus, which has been used to target journalists, activists, and human rights defenders worldwide.

CHATBOTS AND AI-DRIVEN PLATFORMS ARE BEING USED TO AUTOMATE RESPONSES, PROVIDE RESOURCES, AND ENGAGE SUPPORTERS.



Activists are also leveraging AI to debunk disinformation and promote factual narratives. Fact-checking platforms like Full Fact and Logically use AI algorithms to analyze and verify claims, helping activists counter propaganda and build trust in their messages. For example, during the COVID-19 pandemic, activists used AI-driven fact-checking tools to combat misinformation about vaccines and public health measures. By identifying false narratives early, they were able to provide accurate information and hold governments accountable. In Asia, activists are also using AI to track Chinese disinformation across the region and better understand who is spreading it.

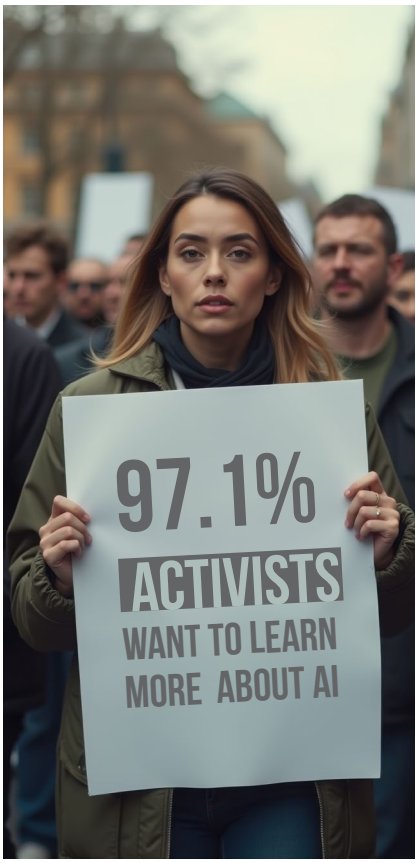
CHATBOTS AND AI-DRIVEN PLATFORMS ARE BEING USED TO AUTOMATE RESPONSES,

Increasingly, AI is playing a crucial role in documenting human rights abuses and gathering evidence for accountability. HURIDOCS uses AI to organize, analyze, and verify evidence of human rights violations. These platforms help activists and organizations build robust cases against perpetrators. In Syria, AI-driven tools have been used to analyze satellite imagery and social media content to document war crimes.[8] Similarly, during the Rohingya crisis in Myanmar, AI was employed to analyze patterns of violence and corroborate survivor testimonies, aiding international advocacy efforts.

AI is in addition transforming how activists engage with audiences. Machine learning algorithms can analyze social media trends, helping movements tailor their messages for maximum impact. Chatbots and AI-driven platforms are being used to automate responses, provide resources, and engage supporters. In Venezuela, AI journalists were created to raise awareness about the deteriorating situation following the July 2024 election. Also in 2024, an AI candidate was created for parliamentary elections in Belarus to raise awareness of the risks opposition and rights activists face in the country.

8 https://www.wsj.com/articles/ai-emerges-as-crucial-tool-for-groups-seeking-justice-for-syria-war-crimes-11613228401

THE RESOURCE IMBALANCE:
WHY AUTOCRATS HAVE THE UPPER HAND



While there are increasing examples of how activists are experimenting with and using AI, a significant challenge is the stark resource imbalance between oppressive regimes and grassroots movements. Autocratic governments often have access to vast financial and technological resources, allowing them to develop, deploy, and refine AI tools at scale. These regimes partner with private tech firms, fund cutting-edge research, and integrate AI into state security apparatuses with little oversight or transparency.

In contrast, activists and human rights defenders frequently operate with limited funding, outdated tools, and insufficient training in emerging technologies. The lag in support is critical: it often takes a year or more after new technologies become widely available for activists to receive the necessary resources, training, and tools to counteract their misuse. A case in point is digital security, an issue for many years, but one in which support for grassroots activists still lags. This delay allows autocrats to consolidate their advantage, stifling dissent before activists can adapt. And the need is palpable: In a recent CANVAS survey of activists and partners around the world, 97.1% of respondents said that they want to learn more about how to use AI for their work and how AI can be used to strengthen civil society and democratic engagement. And 91% of respondents want continuous education opportunities in AI.

AI SYSTEMS ARE RARELY DESIGNED WITH HUMAN RIGHTS, TRANSPARENCY, OR FAIRNESS AS PRIORITIES

The delay in providing activists with AI training and resources has profound implications. This includes missed opportunities to shape AI development as frontline activists are often left out of critical conversations about how AI should be developed and deployed. This exclusion means that AI systems are rarely designed with human rights, transparency, or fairness as priorities. And, without early access to tools and training, activists struggle to counter new forms of surveillance, disinformation, and censorship as they arise, leaving them vulnerable to emerging threats. Activists with inadequate AI literacy and resources are in addition less able to leverage technology for advocacy, outreach, and movement-building. This limits their ability to inspire and mobilize international support, reducing global impact.

LEVELING THE PLAYING FIELD

To level the playing field, the global community must prioritize providing activists with the tools, training, and resources they need to protect themselves and harness AI effectively. Indeed, activists need comprehensive training programs to understand AI technologies, identify threats, and adopt best practices for digital security. Organizations like Access Now, Witness, and Tactical Tech are already making strides in this area, but these efforts need to scale globally and their inclusion in all donor programs, especially those that support grassroots activists, should be a priority.

Governments, NGOs, and philanthropic organizations should also offer grants to fund activist-led projects that develop AI tools for human rights advocacy. This includes but is not limited to tools for documenting abuses, countering disinformation, and evading surveillance. As a new technology, donors should support activists and movements to explore, create, and experiment with a variety of AI tools. Activists also need access to emergency funding and technical assistance when targeted by AI-driven repression. This could include legal support, access to secure technologies, or relocation assistance for those at risk.

Platforms that facilitate collaboration between technologists, human rights defenders, and civil society groups can also accelerate the development of AI solutions. Partnerships between activists and AI developers are crucial for creating tools that address real-world challenges. To this end, CANVAS partners with the University of Virginia to organize the People Power Academy, which features experts and leaders from the frontlines of authoritarian use of technology sharing insights into cutting-edge advocacy tools. Activists must also be included in policy discussions about AI governance. This ensures that AI systems are designed with transparency, accountability, and human rights in mind.

By providing activists with early access to AI tools, training, funding, and collaboration opportunities, the global community can empower them to counter repression and ensure that AI serves as a force for liberation and not repression.

A CONTEST OF SKILLS OVER CONDITIONS

ULTIMATELY, AI WILL NOT DETERMINE THE OUTCOME OF STRUGGLES BETWEEN REPRESSION AND FREEDOM- PEOPLE WILL.

The interplay between AI and activism underscores a fundamental truth: technology is neither inherently good nor bad—it is a reflection of the values and intentions of those who wield it. While autocratic regimes use AI to suppress dissent and consolidate power, activists are finding innovative ways to turn the tide, leveraging the same tools to fight for justice, equality, and human rights.

At the same time, no amount of resources can ever fully level the playing field between authoritarians and grassroots activists and movements. States will always have significant advantages- more money, more data, more computing power, and more institutional control- just as they have police, military, judicial systems, and much more at their disposal. Yet history is full of examples of less resourced and underdog movements using the tools available to them to outmaneuver and pull the pillars of support out from autocrats- even those who seemed invincible. Now, AI is simply another tool at their disposal.

This suggests another fundamental truth: the real battleground is not raw technological capability. Nor is it about using AI for AI's sake, but understanding how it works and strategically integrating it into a movement's broader goals. Indeed, AI is not an arms race between activists and authoritarians; rather, it is a contest of skills over conditions- one where adaptability, creativity, and strategic application matter more than sheer power, since conditions rarely favor a movement until it is able to force changes in their operating context. This aligns with broader research on how nonviolent movements succeed despite lacking vast resources.

While authoritarians use AI for surveillance and control, activists can harness it for agility and disruption- automating security, evading censorship, uncovering disinformation, amplifying resistance, and strategically undermining authoritarian pillars of support. What makes AI so powerful in these efforts is its ability to enhance efficiency- allowing activists to do more, faster, and at scale. And, in asymmetric struggles where governments have superior resources, efficiency is often the deciding factor. AI doesn't just help activists fight back- it is another tool that allows them to outmaneuver repression in ways that were previously impossible.

Ultimately, AI will not determine the outcome of struggles between repression and freedom- people will. The activists who understand how to wield AI strategically, leveraging its strengths while mitigating its risks, will be better positioned to challenge authoritarian power and drive social change. The key is not to match the scale of authoritarian AI but to outthink, outpace, and outmaneuver it.