UNREPRESENTED NATIONS & PEOPLES ORGANIZATION
unpo.org

UNPO Response to Call for Input – Protection of Human Rights Defenders in the Digital Age

March 2026

Submitting Organisation:

Stichting Unrepresented Nations and Peoples Organization (UNPO)

The Unrepresented Nations and Peoples Organization (UNPO) is an international, nonviolent, and democratic membership-based organisation. Its members include indigenous peoples, minorities, unrecognised States, and occupied territories that have joined together to defend their political, social, and cultural rights, as well as their right to self-determination.

Contact: Fluwelen Burgwal 58 2511CJ The Hague, Netherlands | unpo@unpo.org | https://unpo.org/

I. Introduction

- This submission is prepared by the Unrepresented Nations and Peoples Organization (UNPO), and examines the systemic use of digital technologies by states as deliberate instruments to suppress dissent, restrict civic spaces, and repress or intimidate human rights defenders (HRDs) from unrepresented communities.
- UNPO represents communities that frequently face restrictions on their rights to participation, representation and self-determination. When these rights are limited, communities often experience broader constraints on fundamental freedoms, such as freedom of expression, association and peaceful protest. HRDs from unrepresented communities play a critical role in documenting abuses and advocating for the rights of their communities and rely heavily on digital technologies. However, the same technologies are increasingly used by states to surveil activists, restrict communication, criminalise dissent and facilitate repression, both domestically and across borders.
- Although this submission draws on the experiences of certain UNPO members, including Uyghurs, Tibetans, Khmer-Krom, Baloch, Sindhi, communities from Gilgit-Baltistan, and communities in Iran including Kurds, Baloch, Ahwazi Arabs, and Southern Azerbaijanis, HRDs from various other UNPO member communities face similar challenges in the digital age. Furthermore, while HRDs are at direct and heightened risk from the digital threats documented in this submission, these dangers are not confined to formal activists alone. Journalists, lawyers, teachers, and family members of those who speak out against repressive states are equally exposed to surveillance, harassment, and retaliation.

II. Criminalising HRDs

- States regularly deploy vague or overly broad legal provisions, including national security legislation, counter-terrorism laws, blasphemy provisions, and cybercrime or online speech regulations, to criminalise HRDs for their online and offline activities, undermining their legitimacy and exposing them to legal harassment, detention and other forms of retaliation.
- HRDs from unrepresented communities, advocating for their fundamental rights, including self-determination are particularly vulnerable to such measures, which are used to limit dissent and suppress perceived threats to national stability or security.[1]
- In Pakistan, the Anti-Terrorism Act (ATA) has been widely misused by state authorities to silence Sindhi, Baloch, and Gilgit-Baltistan HRDs, many of whom engage in online advocacy to document enforced disappearances and other human rights violations.
- In China, Article 3 of the 2015 Counter-Terrorism Law provides a broad definition of *terrorism* that has been used to justify heightened surveillance, detention and persecution of Uyghur and Tibetan HRDs, including those communicating online with diaspora networks and international organisations.[2]
- In Viet Nam, Article 331 of the Penal Code has been used to prosecute Khmer-Krom HRDs for online expression. Documented instances include arrests, inadequate due

[1] UNPO. (2025). *Legal Warfare as a Tool of Repression.* https://unpo.org/wp-content/uploads/2026/01/UNPO-Report-Legal-warfare-as-a-tool-of-repression.docx.pdf
[2] UNPO. (2025). *Legal Warfare as a Tool of Repression.* https://unpo.org/wp-content/uploads/2026/01/UNPO-Report-Legal-warfare-as-a-tool-of-repression.docx.pdf

process during trials, and subsequent detention for posts on platforms like Facebook related to cultural events. In 2025, the UN Working Group on Arbitrary Detention concluded that these arrests were both arbitrary and discriminatory.[3]

- Frameworks such as the ATA, Viet Nam's Penal Code and the Counter-Terrorism Law have contributed to heightened persecution, state violence and legal harassment of unrepresented HRDs, restricting civic spaces and framing HRDs as criminals, foreign agents, or national security threats.[4]
- Furthermore, the threat of criminalisation produces a pervasive chilling effect, leading to self-censorship among HRDs who fear the consequences they may face personally as well as the implications for their family members.[5]

III. Restrictive Legal Frameworks

- Legal frameworks, regulating cybercrime, security, and online content, have been used by states to target HRDs in digital spaces, enabling surveillance, data access and prosecution.
- In Pakistan, the Prevention of Electronic Crimes Act (PECA, 2016) contains broad provisions allowing authorities to access user data, monitor digital communications, and prosecute individuals for online speech. These provisions disproportionately affect Sindhi, Baloch, and Gilgit-Baltistan HRDs who rely on digital platforms to document human rights abuses and communicate with diaspora networks.[6]
- The Pakistan Telecommunication Authority (PTA), a government oversight body, reinforces this pattern. The PTA has powers to block or restrict online content and order internet shutdowns, contributing to increased censorship and surveillance in digital spaces.[7] In a context where enforced disappearances are a persistent concern for Sindh and Baloch communities, such surveillance capabilities increase the risks faced by unrepresented HRDs that may be identifiable through their online activities.[8]
- China operates an extensive state-controlled internet surveillance system, often referred to as the "Great Firewall." Under the 2017 Cybersecurity Law, companies are required to store user data within China and comply with obligations including data localisation, real-name registration requirements, and security agency cooperation obligations during

[3] WGAD Opinion, A/HRC/WGAD/2025/30. https://www.ohchr.org/sites/default/files/documents/issues/detention-wg/opinions/session102/a-hrc-wgad-2025-30-aev.pdf

[4] Quadri, S, S, A., Rehman, Z., Khan, M, T & Muhib, K. (2025). *The criminalization of human rights defenders: trends, tactics, and international responses*. Social Sciences Spectrum, 4(2), 756-773. https://doi.org/10.71085/sss.04.02.33

[5] UNPO. (2025). *Legal Warfare as a Tool of Repression.* https://unpo.org/wp-content/uploads/2026/01/UNPO-Report-Legal-warfare-as-a-tool-of-repression.docx.pdf

[6] UNPO. (2025). *Legal Warfare as a Tool of Repression.* https://unpo.org/wp-content/uploads/2026/01/UNPO-Report-Legal-warfare-as-a-tool-of-repression.docx.pdf

[7] U.S. Department of State. (2024). *2023 country reports on human rights practices: Pakistan.* https://www.state.gov/wp-content/uploads/2024/02/528267_PAKISTAN-2023-HUMAN-RIGHTS-REPORT.pdf

[8] UNPO. (2026). *Input on Enforced Disappearances in the Context of Transnational Repression.* https://unpo.org/wp-content/uploads/2026/02/UNPO-response-to-call-for-input-Enforced-Disappearances-in-the-Context-of-TNR.pdf

U.S. Department of State. (2024). *2023 country reports on human rights practices: Pakistan.* https://www.state.gov/wp-content/uploads/2024/02/528267_PAKISTAN-2023-HUMAN-RIGHTS-REPORT.pdf

investigations.[9] These measures facilitate extensive monitoring of online communications and have been used to identify and target Uyghur, Tibetan and Taiwanese HRDs, including individuals communicating with diaspora networks or international human rights organisations.

- Viet Nam's laws have granted authorities sweeping powers over digital communication, data flow, and online content, putting Indigenous Khmer-Krom HRDs at risk. Decree No. 147/2024 on Internet Services and Online Information requires platforms to verify user identities through phone numbers of national IDs, store users' personal data (which may be provided to authorities on request), and remove content labelled "illegal" within 24 hours when requested. Non-compliant platforms risk blocking or suspension. Article 331 of the Penal Code is routinely used to prosecute individuals for online expression deemed to "harm national interests".

IV. Internet Shutdowns

- Internet shutdowns and other forms of connectivity restrictions are strategically enforced by state authorities hindering the ability of HRDs to communicate with one another and with international organisations, access information, and document or report human rights violations.
- Pakistan has repeatedly imposed internet and mobile network shutdowns during periods of political unrest, protests, and security operations.[10] In August 2025, a province-wide mobile internet shutdown in Balochistan cut off over 14 million people. The blackout coincided directly with protests planned for the International Day of the Victims of Enforced Disappearance (30 August), preventing peaceful assembly and suppressing documentation of ongoing violations.[11] Balochistan is among the most affected by connectivity disruptions, often justified by authorities on security grounds related to ongoing insurgency and military operations. [12]
- Civil society organisations have documented localised internet disruptions during smaller political gatherings or online events organised by activist groups, restricting coordination and limiting the visibility of their advocacy.[13]
- In Iran, internet shutdowns have significantly increased in early 2026, in response to the new wave of protests, at one point cutting off over 90 million people, many from unrepresented communities, including Kurds, Baloch, Ahwazi Arabs and Southern

[9] Smith, Ross. (2021). *Corporate Violations of Human Rights: Addressing the Coordinated Surveillance and Persecution of the Uyghur People by the Chinese State and Chinese Corporations*, Georgia Journal of International and Comparative Law, 49(3). https://digitalcommons.law.uga.edu/gjicl/vol49/iss3/10

[10] U.S. Department of State. (2024). *2023 country reports on human rights practices: Pakistan.* https://www.state.gov/wp-content/uploads/2024/02/528267_PAKISTAN-2023-HUMAN-RIGHTS-REPORT.pdf

[11] UNPO. (January 5, 2026). *Iran Faces New Wave of Protests as Economic Crisis Deepens.* https://academy.unpo.org/iran-faces-new-wave-of-protests-as-economic-crisis-deepens/

[12] The New Humanitarian. (March 2, 2026). *In security-minded Pakistan, Gen Z protesters find no outlet for their discontent.* https://www.thenewhumanitarian.org/opinion/2026/03/02/security-minded-pakistan-gen-z-protesters-find-no-outlet-their-discontent

[13] Amnesty International. (October 9, 2025). *The Pakistani government shut down the internet. I couldn't even tell my family I was safe.* https://securitylab.amnesty.org/latest/2025/10/the-pakistani-government-shut-down-the-internet-i-couldnt-even-tell-my-family-i-was-safe/

Azerbaijanis.[14] On 28 February 2026, a near total internet shutdown was imposed. While infrastructure damage from regional tensions has contributed to disruptions, the Iranian regime has deliberately and consistently used shutdowns to suppress dissent, limit information flows, and control political narratives.[15]

- These internet shutdowns isolate HRDs, reduce external oversight, and increase the vulnerability of unrepresented communities by limiting their ability to document abuses, share information with international organisations and journalists, and seek assistance.

V. Digital Surveillance

- Advances in digital technologies have significantly expanded states' capacity to monitor and counter the activities of HRDs. Digital tools, including interception of digital communications, surveillance of online platforms, open-source data and cyber attacks, are used to identify, locate, and track HRDs, enabling intimidation, threats against family members, and coercion to abandon activism.
- The use of biometric and facial recognition technologies has further expanded surveillance capabilities, with systems developed to specifically identify individuals belonging to particular ethnic groups. In China, the Public Security Bureau of Shanghai reportedly developed software capable of detecting Uyghurs through facial recognition cameras in public spaces.[16] Applications such as WeChat further require registration through personal identification and biometric data, including facial scans or voice samples, allowing authorities to monitor communications and identify users. Individuals from Uyghur communities have also reportedly been targeted because of digital communications with relatives living in the diaspora. In East Turkestan, residents have been required to install the JingWang mobile application, which scans devices for files considered prohibited by authorities and transmits device data to government services.[17]
- Technologies provided by private companies, including Hikvision, Huawei, China Electronics Technology Corporation, and iFlytek, have supplied facial recognition systems, artificial intelligence surveillance tools, and monitoring technologies used by state authorities.[18] The proliferation of these technologies significantly increases the capacity of governments to identify and track HRDs and may contribute to broader

[14] UNPO. (January 5, 2026). *Iran Faces New Wave of Protests as Economic Crisis Deepens*. https://academy.unpo.org/iran-faces-new-wave-of-protests-as-economic-crisis-deepens/
Amnesty International. (January 23, 2026). *Iran: Authorities unleash heavily militarized clampdown to hide protest massacres*. https://www.amnesty.org/en/latest/news/2026/01/iran-authorities-unleash-heavily-militarized-clampdown-to-hide-protest-massacres/

[15] Access Now. (March 11, 2026). *Connect the population: Access Now demands end to Iran's continued internet blackout amid war*. https://www.accessnow.org/press-release/iran-connect-the-population-statement/

[16] UNPO. (2026). *Input on Enforced Disappearances in the Context of Transnational Repression.* https://unpo.org/wp-content/uploads/2026/02/UNPO-response-to-call-for-input-Enforced-Disappearances-in-the-Context-of-TNR.pdf

[17] Smith, Ross. (2021). *Corporate Violations of Human Rights: Addressing the Coordinated Surveillance and Persecution of the Uyghur People by the Chinese State and Chinese Corporations*, Georgia Journal of International and Comparative Law, 49(3). https://digitalcommons.law.uga.edu/gjicl/vol49/iss3/10

[18] Smith, Ross. (2021). *Corporate Violations of Human Rights: Addressing the Coordinated Surveillance and Persecution of the Uyghur People by the Chinese State and Chinese Corporations*, Georgia Journal of International and Comparative Law, 49(3). https://digitalcommons.law.uga.edu/gjicl/vol49/iss3/10

patterns of repression, including surveillance, intimidation, and other human rights violations.

- Viet Nam's mandatory identity verification requirements under Decree 147/2024 have effectively ended online anonymity, leaving Khmer-Krom HRDs unable to document abuses or organise safely without risking exposure to state authorities.
- Uyghur HRDs have further been subjected to malicious smear campaigns, including the use of deepfakes and disinformation, designed to discredit their advocacy and undermine their legitimacy.[19] Sindhi women HRDs in Pakistan have similarly reported gendered online harassment campaigns involving fake social media accounts, defamatory content, and attacks on their personal reputation intended to discredit their activism and discourage their participation in public life.[20]

VII. Transnational Repression

- Digital surveillance capabilities have enabled states to expand repression beyond borders, monitoring and targeting diaspora activists in third countries. This has concerning implications for the safety of unrepresented diaspora HRDs, as "advances in surveillance technology, facial recognition and digital platforms have expanded states' capacity to identify, locate, monitor, intimidate and target individuals abroad. Digital transnational repression now plays a central role in facilitating enforced disappearances by enabling states to locate and coordinate action against dissidents in exile".[21]
- Uyghur, Tibetan, and Taiwanese HRDs have repeatedly been targeted by cyber-espionage campaigns.
- In 2025, senior members of the World Uyghur Congress (WUC) received emails encouraging them to download and test a Uyghur-language typing tool. Subsequent analysis by Citizen Lab (University of Toronto) found that the software contained a "Windows-based malware capable of conducting remote surveillance against its targets", enabling attackers to monitor victims' devices and communications.[22]
- In the same year, the UK National Cyber Security Centre (NCSC) issued warnings regarding two surveillance softwares, MOONSHINE and BADBAZAAR, which have been used to target Uyghur, Tibetan, and Taiwanese communities. These applications are capable of collecting sensitive personal data and remotely activating microphones and cameras on infected devices.[23]
- Such cyber attacks and digital threats occur within a broader pattern of transnational repression implicating the safety of unrepresented HRDs. Chinese authorities use

[19] World Uyghur Congress. (September 22, 2025). *World Uyghur Congress Condemns Malicious Smear Campaign Targeting Executive Committee Chair Rushan Abbas*. https://www.uyghurcongress.org/en/world-uyghur-congress-condemns-malicious-smear-campaign-targeting-executive-committee-chair-rushan-abbas/

[20] UNPO. (2025). *Legal Warfare as a Tool of Repression.* https://unpo.org/wp-content/uploads/2026/01/UNPO-Report-Legal-warfare-as-a-tool-of-repression.docx.pdf

[21] UNPO. (2026). *Input on Enforced Disappearances in the Context of Transnational Repression.* https://unpo.org/wp-content/uploads/2026/02/UNPO-response-to-call-for-input-Enforced-Disappearances-in-the-Context-of-TNR.pdf

[22] The Citizen Lab. (2025). *Weaponized Words. Uyghur Language Software Hijacked to Deliver Malware.* https://citizenlab.ca/research/uyghur-language-software-hijacked-to-deliver-malware/

[23] Central Tibetan Organisation. (April 9, 2025). *NCSC Shares Technical Details of Spyware Targeting Uyghur, Tibetan and Taiwanese Groups*. https://tibet.net/ncsc-shares-technical-details-of-spyware-targeting-uyghur-tibetan-and-taiwanese-groups/

coercive "involuntary returns" through Operation Sky Net to force individuals abroad back to China, with. These methods increasingly bypass legal avenues like extradition, instead employing unregulated, illegal covert operations, and rely on digital surveillance to locate and identify targets abroad.[24]

VIII. Conclusion and Recommendations

- Digital technologies have become central instruments of repression against HRDs from unrepresented nations and peoples, operating across a spectrum from domestic criminalisation and surveillance to cross-border cyber-espionage.
- For communities whose rights to representation and self-determination are already denied, digital repression is not merely an additional burden, it eliminates one of the only remaining means of reaching international audiences and securing accountability.
- In light of the above, UNPO makes the following recommendations to the Office of the High Commissioner for Human Rights:
    - **Address the misuse of legislation to criminalise digital activism** - call on States to review and amend counter-terrorism, cybercrime and national security legislation containing vague provisions that enable the criminalisation of HRDs.
    - **Highlight the human rights impact of internet shutdowns** - call on States to refrain from imposing internet shutdowns, mobile network disruptions or platform blocking that hinder the work of HRDs and prevent the documentation of human rights violations. Particular attention should be given to shutdowns imposed during peaceful protests, including the shutdown in Balochistan (August 2025) and Iran (February 2026).
    - **Strengthen corporate accountability in preventing digital repression** - encourage technology companies to strengthen human rights due diligence in line with the UN Guiding Principles on Business and Human Rights, particularly regarding the development and export of surveillance technologies and the protection of HRDs using digital platforms.
    - **Address the use of digital technologies in transnational repression** - highlight the growing role of digital technologies in enabling transnational repression against diaspora HRDs and encourage States to investigate cyber-espionage and online intimidation targeting activists abroad, while ensuring protection for those at risk.

[24] UNPO. (February 9, 2022). *Operation Sky Net and China's Growing Transnational Repression*. https://unpo.org/operation-sky-net-and-chinas-growing-transnational-repression/