February 8, 2022

Resist Myanmar's digital coup: stop the military consolidating digital control

One year ago, as the Myanmar military sent tanks down the streets and rounded up government officials and activists, it shut down the internet, mobile phone networks, radio, and television channels. As it plunged the country into a communications blackhole, the junta launched concerted assaults at already threadbare protections online to throttle expression and information-sharing. Today, the military is ramping up efforts to cement authoritarian control of online space, alongside violent crackdowns, and serious human rights violations. This is a digital coup, and the world must resist.

Internet shutdowns continue to be wielded to shroud serious human rights violations. Soon after the coup and lasting almost three months, the military imposed near-complete nationwide internet shutdowns — including nightly communications blackouts and online media and messaging platform bans. The people in Myanmar were not able to communicate with loved ones, share information, report on human rights violations, or seek help amidst an emergency. Contrary to the principles of net neutrality and the norm of a free internet, the junta lifted some disruptions to favor its own "white-list" of organisations and corporations that could access the internet, while the rest of the country suffered the consequences of these discriminatory and unequal shutdowns. The military continue to order regional shutdowns — particularly where active armed conflicts are ongoing, in attempts to conceal thousands of reports of assault, killings, arrests, detention, enforced disappearance, ill-treatment, torture, torching and gender-based violence committed by the junta.

Control of telecommunications providers and abuse of surveillance technology expands monitoring and targeting of individuals. Reuters recently reported that the Myanmar military had privately approved the sale of Telenor Myanmar to M1 Group and military-linked Shwe Byain Phyu Group — with the latter as a majority shareholder. Should the sale go ahead, three of the four telecommunications providers operating in Myanmar would be directly controlled by the junta — including Myanmar Posts and Telecommunications (MPT) and Telecom International Myanmar Company Limited (MyTel). It can also be assumed that thereafter, all operators in Myanmar — including the fourth, Ooredoo — will activate surveillance technology within their networks, noting Telenor's statement that its departure was due to "continued pressure" on operators to "activate intercept equipment and technology for the use of Myanmar authorities''. These targeted efforts will enable the

February 8, 2022

military to bring all network services under its stranglehold and escalate abuses of privacy and security rights, through surveillance and related efforts. Yet, disturbingly, not a single telecommunications sector actor has implemented urgent data protection and privacy safeguards needed to protect their customers. Telenor Group, in particular, had earned people's trust on the basis of their earlier commitments to human rights and public reporting on network shutdowns and military orders. These customers — including activists, journalists and other at-risk individuals — are now in danger of having their data transferred to a military-linked outfit through an irresponsible disposal of its business operations in Myanmar.

Legal tools are abused to stifle individuals' rights to expression, information, and privacy. By amending the Broadcasting Law and resurrecting a previously defeated Cybersecurity Law, the military will fortify censorship controls online. The amended Broadcasting Law effectively criminalises any speech deemed impermissible by the military on a wide range of media — including radio, television, audio and video social media posts, and websites — with up to three years' imprisonment. Meanwhile, the draft Cybersecurity Law provides overbroad censorship and regulatory powers to the authorities — including the Ministry of Defence with its notorious record of committing abuses amounting to serious international crimes — to censor online content, order the furnishing of individuals' personal data from internet service providers and control online platforms and services through onerous registration and licensing requirements. Not satisfied with the increasing trend of arrests for alleged illegal VPN usage, the draft Cybersecurity Law proposes to penalise VPN usage with up to three years' imprisonment, further extinguishing one of the last tools of protection and security available to the people of Myanmar.

Price hikes and onerous data provision requirements make it increasingly difficult for people to access the internet. In December 2021, in an attempt to price people out of telecommunication access, the military forced telecommunications operators to significantly hike up prices for data usage and phone calls, doubling the price of mobile data, and increasing the cost of phone calls by nearly a quarter — significantly impacting a population already struggling from a banking crisis. In January 2022, the increasing cost of connectivity was worsened by the junta's 10% tax hike on mobile data service providers — which then increased customers' prices further — and a 20,000 kyat (US$11) commercial tax on new SIM card activation, which exacerbated the already onerous requirements for SIM card registration. These manipulations now pose extortionate barriers to internet access for the average person in Myanmar, amidst a coup and a pandemic — when they need connectivity the most.

Harassment and dissemination of incitement to violence online propagates fear and insecurity. Reports continue to emerge of military and military-linked personnel appropriating social media

February 8, 2022

platforms to post hate speech and incite violence against individuals supporting opposition to the coup. From even before the coup, content moderation failures on platforms like Facebook and YouTube had accelerated hate speech and incitement to violence online. Pressure from civil society forced Facebook to take down hundreds of military-linked accounts and strengthen its mitigation measures. After being blocked from Facebook, increasing numbers of military and military-linked actors are now abusing less responsive services and platforms to amplify a regime of fear and abuse online, including through death threats on TikTok, and doxxing on Telegram. In contrast, the junta are conducting stop-searches of individuals' devices which often result in arrests, detention, and assault, with impunity. While tech platforms meander in their mitigation measures, privacy and security violations proliferate.

With a year of concerted effort to control and manipulate the online and offline lives of millions of people in Myanmar as groundwork, today, the junta's digital coup is more violent and aggressive than ever — aimed at crushing remnants of the already razed rights to privacy, expression, information, association, and security. As the world watches on, the Myanmar military is very close to its goal of consolidating absolute control of digital spaces.

The international community, technology companies, platforms, and network providers must stand with the people of Myanmar and resist the digital coup. We have an obligation to hold the Myanmar military accountable for the serious human rights violations it continues to commit. The international community must:

1. **Publicly condemn the Myanmar junta's continued attacks on civic space and push back against assaults on rights — including to freedom of expression, information, association, privacy and security;**

2. **Support calls for targeted sanctions against the military and against military-linked individuals and businesses, including sanctions aimed at restricting the sale and supply of dual-use surveillance technology;**

3. **Pressure companies to uphold international standards on responsible business;**

February 8, 2022

4. **Continue and expand support for civil society, humanitarian and other actors working to defend human rights within Myanmar.**

Telecommunications and technology companies in Myanmar must:

---

5. **Immediately implement data protection and privacy safeguards to resist increasing attempts to extend surveillance, censorship, and abuse of rights;**

---

6. **Conduct due diligence and pursue genuine public engagement when creating or changing their policies on data protection, content moderation, and others, pursuant to international human rights standards; and**

---

7. **Implement policies informed by genuine public engagement and based on international human rights standards.**

Every day, the people of Myanmar continue to suffer escalating attacks in an environment of repression and violence. The coup is offline and online. The international and business community must resist. Continued inaction costs lives.

ORGANIZATIONS

Access Now
Advocacy Initiative for Development (AID)
ARTICLE 19
ASEAN Intergovernmental Commission on Human Rights (AICHR) Indonesia
Asia Justice and Rights (AJAR)
Association for Progressive Communications
Athan
Censored Planet
CIVICUS: World Alliance for Citizen Participation
Digital Rights Collective

February 8, 2022

Digital Rights Foundation, Pakistan
Digital Rights Kashmir
ELSAM (Institute for Policy Research and Advocacy)
Fortify Rights
Foundation for Media Alternatives
Free Media Movement, Sri Lanka
Human Rights Activists in Iran (HRA)
International Service For Human Rights (ISHR)
Internet Protection Society, Russia
Justice for Myanmar
Lawyers' Rights Watch Canada
Last Mile4D
Legal Initiatives for Vietnam
Manushya Foundation
Open Net Association
Open Observatory of Network Interference (OONI)
Organization of the Justice Campaign
PEN America
Ranking Digital Rights
Robert F. Kennedy Human Rights
SAFEnet - Southeast Asia Freedom of Expression Network
Sassoufit Collective
South Asia Media Defenders Network (SAMDEN)
Transformative Justice Collective
Wikimedia Community User Group Uganda
Wikimédia France
WITNESS
Women of Uganda Network (WOUGNET)
Women ICT Advocacy Group (WIAG)
World Pulse
Zaina Foundation

For more Information, please contact:

Dhevy Sivaprakasam | **Asia Pacific Policy Counsel at Access Now** | dhevy@accessnow.org