Resisting Myanmar's surveillance state

An advocacy strategy for civil society

ARTICLE 19

ARTICLE 19

72–82 Rosebery Ave
London EC1R 4RW
UK
www.article19.org

T: +44 20 7324 2500
F: +44 20 7490 0566

E: info@article19.org
W: www.article19.org

Tw: @article19org
Fb: facebook.com/article19org

ARTICLE 19 is an international think–do organisation that propels the freedom of expression movement locally and globally to ensure all people realise the power of their voices.

Together with our partners, we develop cutting-edge research and legal and policy analysis to drive change worldwide, lead work on the frontlines of expression through our 9 regional hubs across the globe, and propel change by sparking innovation in the global freedom of expression movement. We do this by working on 5 key themes: promoting media independence, increasing access to information, protecting journalists, expanding civic space, and placing human rights at the heart of developing digital spaces.

ARTICLE 19 would appreciate receiving a copy of any materials in which information from this report is used. The report was developed as a part of the **Engaging Tech for Internet Freedom (ETIF)** initiative, under funding from the US Bureau of Democracy, Human Rights, and Labor. ARTICLE 19 bears the sole responsibility for the content of the document.

Contents

Executive summary

The surveillance of online communications poses significant concerns for the right to freedom of expression and privacy and other human rights. Myanmar currently lacks a comprehensive legal framework preventing its junta, the State Administration Council (SAC), from violating human rights. Instead, the SAC devises legal tools to surveil people and suppress their right to privacy. Since the February 2021 military coup, the SAC has passed, amended, or resurrected laws and regulations to allow it to intercept information without safeguards and oversight, violating the right to freedom of expression and privacy of the people of Myanmar. The military also uses arbitrary powers to collect data from information and communication technology (ICT) providers and to deploy hacking and online monitoring software for mass surveillance.

The ICT sector has an important role to play in protecting the right to freedom of expression and privacy online, and it is essential that it fulfils its responsibility to respect human rights and humanitarian law. For ICT providers and companies selling dual-use technology, the risk of impacting human rights in Myanmar is extremely high. In the conflict-affected Myanmar context, businesses must meet a heightened human rights due diligence (HRDD) standard that includes conflict-sensitivity analysis.

This report:

- describes the current state of surveillance in Myanmar and the junta's ability to acquire personal data from ICT companies to violate people' rights;
- examines the challenges that the current regulatory framework poses to ICT companies to respect the right to privacy and other human rights in their operations; and
- suggests a strategy for civil society organisations (CSOs) working on Myanmar to engage with responsible businesses.

ARTICLE 19 suggests that CSOs should take the following steps:

Recommendation 1: Engage with the international community

Recommendation 2: Work with the Freedom Online Coalition

Recommendation 3: Raise awareness about freedom of expression, privacy, and data protection among the people of Myanmar

Recommendation 4: Secure personal data and financial transactions

Recommendation 5: Discuss risks related to human rights with local businesses

Recommendation 6: Use international standards and industry-led initiatives to engage with companies operating in Myanmar

Recommendation 7: Develop a coordinated strategy for advocacy with companies

Recommendation 8: Identify and engage with responsible companies which are human rights-centred

Recommendation 9: Advocate for responsible investment and respect for human rights

Recommendation 10: Ask businesses to carry out a heightened human rights due diligence process

Recommendation 11: Stress the importance of conflict analysis and local expertise

Recommendation 12: Participate in meaningful consultation with responsible businesses

We also suggest that businesses should take the following steps:

Recommendation 13: Harness leverage to influence government and business relationships

Recommendation 14: Discuss divestment options and responsible exits

Introduction

Digital technology was late in arriving to Myanmar. Investment in the information and communications technology (ICT) sector began with the rapid growth of smartphone and internet access starting in 2012. Myanmar joined a global economy driven by the intrusive data collection practices of a few large companies. While this data economy raises profound questions about human rights in any context, it becomes a matter of life and death in highly authoritarian regimes. In Myanmar, the junta uses personal data and information shared online by the people of Myanmar to violate the rights to privacy and freedom of expression on a scale not previously imaginable and in a manner that can have life-threatening consequences. In 2022, UN human rights experts condemned the Myanmar military junta's attempts to establish a 'digital dictatorship'.

This report is aimed at civil society activists in and outside of Myanmar who have had to consider how to engage with tech companies in these extremely challenging circumstances. It is informed by interviews and consultations with them.

First, it describes the problem of the nature of the data economy and the ability of the State Administration Council (SAC) to use it for surveillance and human rights violations. While society-wide predictive data analysis is currently beyond its capacity, the regime has already purchased the technology to enable this, and it has deployed hacking and spyware to target individuals. It has imposed mandatory registration of mobile devices' International Mobile Equipment Identity (IMEI) numbers and SIM cards, opening the door to further allow surveillance.

This is all possible because rule of law and human rights protection mechanisms have never been established in Myanmar. Governance has always been characterised by impunity, as there has never been a functioning judicial system based on fair trial standards that is capable of independent oversight of the government and security forces. The rule of law was already weak before the February 2021 military coup, and there are no human rights safeguards related to data protection and privacy, or freedom of expression more generally.

Second, the report underscores the alarming extent to which Myanmar's legislation falls short of meeting international human rights standards. Since the February 2021 military coup, the risks to human rights stemming from digital technology and data protection have escalated dramatically, demanding urgent and unwavering attention. Personal data held by companies, if obtained by the Myanmar military, 'can lead to detention or torture, and even death'. It can also lead to violations of freedom of expression. In contexts such as these, ICT providers are more likely to contribute to violations of international human rights and humanitarian law and must therefore exercise heightened human rights due diligence (HRDD). While some businesses in the telecom sector in Myanmar have conducted HRDD, few have factored in the specific risks associated with conflict, instability, poor rule of law, and lack of effective human rights oversight. Fewer still contemplate the rights of users in the event of the military gaining direct access to data by law or military decree.

Those tech companies who do seek to respect human rights are faced with legal demands based on national legislation that contravenes human rights standards. The private sector needs to determine whether it can use its leverage to push for reforms to regulations that do not currently contain human rights safeguards. The report describes the heightened responsibilities of companies in a conflict context, reflected in a heightened HRDD process. ICT businesses must consider their presence, leverage, and impact on conflict and wider society, not just the direct human rights impact of their operations.

Third, the report outlines an advocacy strategy for engaging with ICT companies, based on extensive interviews with Myanmar civil society organisations (CSOs) and other forms of stakeholder consultation. It suggests ways in which civil society can engage with ICT companies and play a role in HRDD processes during ICT investments, operations, and company exits, going beyond mere superficial consultation. It recommends accountability campaigns to target non-cooperative ICT companies, and leveraging partnerships with those willing to participate in HRDD. Responsible businesses and civil society share an

interest in preventing government interference in ICT data and promoting robust data protection laws with oversight.[1]

Finally, ARTICLE 19 advises collaboration between civil society, the private sector, and the international community to push for a rule-of-law-focused ICT sector, safeguarding freedom of expression, privacy, and human rights in the digital age.

[1] While ARTICLE 19 does not use the term 'responsible businesses' but refers to companies' willingness to respect human rights, we use it in this report as it is widely used by CSOs in Asian countries with authoritarian contexts instead of human rights language to avoid government scrutiny. 'Responsible businesses' generally refers to companies that make efforts to positively impact society, the environment, and the economy through ethical governance, minimizing environmental harm, contributing to social welfare, sustainable economic support, stakeholder engagement, and exceeding legal standards. In the Asia-Pacific, countries like Thailand, Japan, and Pakistan have developed national action plans to promote responsible business practices. These initiatives emphasise ethical governance, environmental stewardship, and social responsibility, aligning with international frameworks such as the UN Guiding Principles on Business and Human Rights.

The problem: Surveillance and human rights violations in Myanmar

The nature of the data-driven economy means that governments can now easily monitor individuals in public spaces and online. Governments can combine a range of resources, from software to analyse social media data, to hacking tools and mandatory data retention laws allowing them to directly access the vast personal data amassed by ICT providers, to facial recognition surveillance for profiling people. Many governments allow for 'lawful intercepts' by law enforcement agencies and can request or compel companies to provide direct access to user data. While direct access arrangements vary, they all restrict the ability of ICT companies to scrutinise, question, and provide user notice or public transparency regarding government access to data, removing an important level of safeguards for users' rights. Governments can use the data they collect or surveillance services offered by companies to identify their critics, resulting in the arrest and detention of human rights defenders, journalists, and activists, or they can use these tools to disproportionately target minorities and marginalised communities. Authorities often use dual-use intercept spyware, justified as being needed for counter-terrorism, to clamp down on critical or dissenting views. Data-driven systematic mass surveillance, combined with predictive analytics identifying and assessing individual behaviour, without safeguards, can amount to a violation of the right to privacy and freedom of expression. This has considerable chilling effects on how people exercise these and other rights, including the right to peaceful assembly.

Myanmar's military regime is no exception. Since 2018, the Myanmar military has been acquiring hacking and online surveillance technology. These purchases include MacQuisition forensic software that can hack Apple products and MSAB Field units that can extract content from devices. Telecom and internet service providers have been ordered to install intercept spyware that would allow a government to eavesdrop on the communications of citizens to control political opponents, prevent protests, and cut off dissent. In 2020, Norway's Telenor warned the public that it was concerned about previous government office plans to 'directly access each operator and ISP's [internet service provider's] systems without case-by-case approval'. It noted that Myanmar did not have sufficient laws and regulations to protect customers' rights to privacy and freedom of

expression. Other companies, however, have contributed to the SAC's capabilities. Dual-use surveillance technology made by Israeli, US, and European companies was sold to Myanmar, despite sanctions after the military's crimes against Rohingya Muslims in 2017. In the years preceding the coup, the military employed two private surveillance companies to monitor regime opponents – Israel's Cellebrite between 2016 and 2018 and German company Finfisher in 2019. Israel's Cognyte Software won a tender to sell intercept spyware to Myanmar Post and Telecommunications (MPT) a month before the coup, despite Israel claiming it had stopped defence technology transfers to Myanmar following a 2017 ruling by Israel's Supreme Court, according to a legal complaint filed in January 2023. The military likely used extraction technology purchased from Israeli, US, and Swedish companies to access data from the devices of people protesting against the 2021 coup.

Since the coup, the regime now regularly monitors private electronic communications through online and digital surveillance. Pro-democracy supporters, activists, and journalists have been arbitrarily arrested, tortured, and killed. In response to online opposition, the military has suspended internet and mobile services, blocked social media, stripped the licences of independent online news outlets, forced service providers to hand over personal data, and taken control of the telecommunications infrastructure. The regime has established a series of regulatory orders for mandatory registration of SIM cards and mobile devices' IMEI, opening the door to the unconstrained tracking of people's locations, communications, and other personal data. Those who refuse to register are cut off from services. The military now has an arsenal of digital weapons to use against its opponents, pro-democracy activists, peaceful protesters, and human rights defenders. It has purchased technology that enables it to collect digital data, hack passwords, clone phones, track signals, gather social media intelligence, and process large amounts of data. The regime is also seeking technical assistance from China to develop biometric smart IDs. Critics say the system will be used to monitor opponents.

Since the coup, ICT service providers have come under pressure from the military to provide direct access to user data. In 2022, Norway's Telenor sold its operations, citing human rights and business concerns, and subsequently Qatar's Ooredoo also announced its decision to sell. With the sale of the last two internationally owned telecom operators,

the military gained the power to activate intercept surveillance across networks to spy on unencrypted calls, messages, and web traffic, as well as to track users. Customers in Myanmar must now use ICT providers MPT and Mytel, which are controlled by the regime or military-aligned entities. ICT customers risk having their data transferred to a military-linked provider. Businesses have supplied surveillance tools to military-controlled ministries and some continue to sell dual-use technology. Myanmar's nascent online surveillance system depends on China and Russia and on companies that will sell to and work with authoritarian states. For example, Chinese telecommunications company Huawei reportedly supplied cameras and other equipment to companies involved in the junta's efforts to roll out surveillance networks in major cities. It has been reported that Russia is assisting the junta to develop its 'golden firewall'. The regime has also received assistance from Iran. Software from the US-based companies DataWalk and VMware enables big data and police IT systems, while the World Bank-financed spectrum monitoring system allows the military to track activists and journalists. Mantra Softech, an Indian biometric solutions provider, is developing a biometric border access control system, being piloted at airports since 2022.

The SAC also increasingly scrutinises online financial transactions and banking. Financial service companies have been ordered to conduct stricter verification processes, including photographing customers and recording their name, address, phone number, and National Registration Card. In 2022, the military reportedly ordered banks to increase surveillance efforts by 'installing CCTV or secretly taking pictures' of those buying and selling mobile banking accounts. The Central Bank of Myanmar, controlled by the military since the coup, is pressuring private banks to comply through directives which are not made public. In April 2023, thousands of Kanbawza Bank (KBZ) customers reportedly lost access to their accounts and others are facing arrest for helping resistance groups. KBZ may be sharing the location of its customers with the military, as the bank is obliged to comply with the junta's directives. It has long-standing ties with the Myanmar military and has partnered with the military conglomerate Myanmar Economic Holdings Limited on mining and energy ventures. In 2018, the bank entered into a partnership with Huawei to develop KBZPay, launched the following year. These data collection and amalgamation initiatives proceed without the oversight that could be provided by privacy and data protection laws and safeguards and institutions to uphold human rights.

Myanmar's legal framework

Any limitations on the right to freedom of expression and privacy must meet a strict test stipulated in the international human rights standards and must be subject to independent oversight. They must be 'provided by law', must pursue one of the legitimate aims explicitly enumerated in the international treaties, and must be necessary and proportionate to achieve the aim in question. The OHCHR has expressed concern that many states continue to surveil public and online communications in contravention of legal principles as data protection laws are often missing, vague, or inadequate. This is the case in Myanmar.

Since the coup, the SAC has passed, amended, or resurrected laws and regulations violating the rights to freedom of expression and privacy of individuals in Myanmar. There have always been significant risks to privacy and freedom of expression rights in Myanmar due to both the lack of safeguards in the legal framework applicable to tech companies and legal provisions that are vague or otherwise inconsistent with international human rights standards. This includes laws – or the lack of them – on issues such as lawful interception, cybersecurity, data protection, and cybercrime.

For example:

- The Law Protecting the Privacy and Security of Citizens (2017, amended 2021; Privacy Law) includes several provisions incompatible with international human rights standards. The amendments grant the SAC increased authority by suspending or eliminating previously existing safeguards, allowing unchecked searches, seizures and arrests, and extended detentions without judicial oversight. The changes particularly affect Section 5 (search, seizure, and arrest without civilian observation), Section 7 (indefinite detention without habeas corpus), and Section 8 (reducing individual privacy rights).

- The Electronic Transaction Law (2004, amended 2021) allows companies' licences to be suspended or cancelled if they fail to comply with government-imposed conditions – including requests to turn over information on the identity of users.

- The Draft Cyber Security Law (2022) gives the military complete access to personal data, creating a serious risk that ICT companies can be required to hand over sensitive user data to the government in violation of users' privacy, without due process or independent oversight.

- The Telecommunications Law (2013, amended 2017) contains broad provisions without safeguards on several issues, including lawful interception. Under Section 77, the Ministry of Transport and Communications (MOTC) has wide discretion to direct a licence holder to intercept communications on the basis of public interest. There is no definition of 'public interest', and no clarification as to what constitutes a lawful interception request. The MOTC must seek government approval to request an interception under Section 75, but there is no clarification of what form government approval would take (e.g., an executive order or parliamentary resolution).

- The Regulations Implementing the 2014 Counterterrorism Law (2023) allow the military to actively intercept all online activities and to order network providers to hand over personal data on people's location and communications.

- The Regulations on Obtaining Information and Communications (2022) empower several security and law-enforcement bodies to conduct lawful interception. Article 2(f) defines 'targets' as 'telephone number, IMEI, IMSI, Cell-ID, IP address, user account or user ID, MAC address, IM account or IM ID, non-IM account or non-IM ID, VoIP account or VoIP ID, account and IDs that are used for social media/social network, email address and website addresses which are required to be intercepted to acquire information and communication in a lawful manner'. These data points would together help provide total surveillance.

- The Financial Institutions Law (2016) establishes the Central Bank's duty to promote consumer protection and the financial capability of banking and financial consumers, and for this purpose empowers it to promote and consolidate consumer 'data collection'.

ICT companies in Myanmar and their responsibilities

Without adequate legal safeguards or the independent oversight mechanisms required to limit the right to freedom of expression and privacy in line with international standards, the SAC is likely to continue using arbitrary powers to collect data from ICT providers and to deploy hacking and online surveillance software for mass surveillance. This heightens the role played by private businesses and their responsibility to respect human rights. According to the UN Guiding Principles on Business and Human Rights (UNGPs), businesses have a responsibility to respect human rights. This rests on a 'do no harm' principle that requires ongoing HRDD to identify, prevent, mitigate, and account for adverse human rights impacts.

The presence and role of business in high-risk or conflict areas has always been a human rights concern, and the military coup intensified scrutiny of businesses' role in Myanmar. The UNGPs call for a tailored and appropriate business response, proportionate to the human rights risk: the higher the risk, the more complex – or heightened – the action expected. For businesses in Myanmar, this means undertaking an ongoing, enhanced HRDD process.

Heightened HRDD is not only a response to a crisis: it is a preventive mechanism. A heightened HRDD process will identify additional, unforeseen risks associated with weak or non-existent state structures, complicated business relationships, the presence and role of other actors linked to a given conflict, and the heightened severity of potential human rights abuses. For ICT providers and companies selling dual-use technology, there is an extremely high risk of negative human rights impacts such as surveillance and detention – targeting by the SAC in Myanmar is a vivid example. ICT companies investing in Myanmar must be able to demonstrate the steps undertaken to identify and mitigate the human rights risks in the specific context. Moreover, ICT companies must formulate a public policy on benchmarked, responsible exits by comparing specific aspects of a public problem and then acting. They should, in particular, consider protection of users' freedom of expression and privacy, whether impacted by content moderation, contractual provisions, legal or technical limitations on the sale of products to governmental clients, legal and regulatory compliance, local staff safety, or the possibility of service restrictions and blockage.

The Office of the UN High Commissioner for Human Rights (OHCHR) recommends that states 'ensure that victims of human rights violations and abuses linked to the use of surveillance systems have access to effective remedies'. Access to remedy constitutes the third pillar of the UNGPs. Data-protection law should include the right to an effective remedy against a data controller or data processor, including compensation for damage suffered, and liability. In Myanmar there is no specific judicial oversight process laid out in law. The lack of a data-protection framework means there is no process for seeking redress or compensation in cases of unauthorised sharing or use of personal data or other violations of data privacy. Some laws related to various industry sectors protect against the disclosure of confidential information, but the authorities have not taken action under any of these provisions over breach of privacy or unauthorised disclosure of confidential information. The Privacy Law creates no general offence of interfering with the constitutional right to privacy, although there appears to be room to make a complaint under Section 6.

A handful of judicial and quasi-judicial cases have been filed against ICT companies in relation to HRDD and data-protection breaches in Myanmar.

As mentioned above, following the 2021 coup some ICT companies divested, citing human rights impacts. In July 2021, 'after considering all possible alternatives and events', Telenor decided to leave Myanmar and sell its operations there to M1 Group – a sale approved by the Myanmar Investment Commission in March 2022. According to international non-governmental organisation SOMO (the Centre for Research on Multinational Corporations), M1 Group is 'infamous for its business activities in countries with violent totalitarian and extremist regimes'. In July 2021, a complaint was filed against Telenor with the Norwegian National Contact Point under the Organisation for Economic Co-operation and Development (OECD) Guidelines. It alleged non-compliance with responsible disengagement as set out in the Guidelines, including failure 'to conduct appropriate risk-based due diligence' and 'to prevent or mitigate adverse human rights impacts potentially arising from the sale of its Myanmar operations'. The parties have been engaged in mediation since June 2022 and have arrived at a preliminary memorandum of understanding (MoU).

Separately, in February 2022, a Myanmar citizen filed a complaint against Telenor before the Norwegian Data Protection Authority, seeking to halt the transfer of control over sensitive user data. The complaint contends that the sale would violate the privacy of Telenor's 18 million customers in Myanmar. The complainant viewed Telenor as responsible for the data processing happening in Myanmar because it is subject to the EU General Data Protection Regulation (GDPR) and because it exercises effective influence over how its subsidiary in Myanmar processes customer data. Finally, in March 2022, Justice for Myanmar accused Telenor of having violated EU sanctions and aligned Norwegian sanctions on Myanmar by installing and maintaining a lawful interception gateway, which Telenor purchased from Germany company Utimaco and integrated into its system in 2018.

In January 2023, an application for a criminal investigation into the activities of Israeli company Cognyte Software and officials from the Ministry of Defence and Ministry of Foreign Affairs was filed with Israel's Attorney General over their allegedly 'aiding and abetting crimes against humanity in Myanmar'. In 2020, Cognyte had won a tender to provide lawful interception equipment to MPT in Myanmar. Documents leaked to Justice for Myanmar show that MPT issued Cognyte with a purchase order in December 2020, with work scheduled for completion by early June 2021. The system would allow the Myanmar military to tap calls in real time, aiding and abetting its atrocities. Cognyte's Myanmar partner is Khine Thitsar, an ICT business involved in surveillance, including lawful interception. In October 2023, the German state prosecutor's office launched a criminal investigation into ND SatCom, a German company, for supplying communications equipment to the Myanmar military, including after the coup. Since at least 2016, ND SatCom has provided significant support for the Myanmar army's satellite communications system, including 5G hardware and software.

In September 2022, Ooredoo, the last remaining telecom company operating in Myanmar not owned by or connected to the military junta, announced its decision to exit Myanmar and sell its local operations to Nine Communications, a Singapore-based subsidiary of Link Family Office and military-linked Nyan Win. Several NGOs reached out to Ooredoo Group's CEO before the sale to push for constructive engagement and dialogue with stakeholders to address the human rights risks of the sale, but the company did not

acknowledge their communications. Other foreign companies continue to operate in Myanmar's telecom sector. Mobile operator Mytel (trading under the company Telecom International Myanmar) is part of the Myanmar military's business network providing technology and surveillance capabilities. Mytel's shareholders are military conglomerate Myanmar Economic Corporation, Myanmar National Telecom Holdings, and Viettel, the largest shareholder – a high-tech arms manufacturer owned by the Vietnamese Ministry of National Defence and involved in tech transfer with the Myanmar military. MPT is a joint operation with Japanese companies KDDI and Sumitomo. Justice for Myanmar has pointed out that MPT's efforts to install and activate lawful interception technology are evidence of the failure of KDDI and Sumitomo, through their KDDI Summit Global Myanmar joint venture, to meet their business and human rights responsibilities. In 2021, KDDI and Sumitomo Corporation expressed 'deep concern' about lawful interception in Myanmar and stated that they 'are not subject to direct instructions from the regulatory authority with regard to interception based on the telecommunications laws of Myanmar'. The companies' statements failed to outline the steps they would take to end their direct connection to the junta's human rights violations.

A civil society engagement strategy: ARTICLE 19's proposal

CSOs – community organisations, local NGOs, trade unions, activists, human rights defenders, aid workers, and community leaders – and journalists in Myanmar have long faced harassment and persecution. Since the coup, their work has become even more dangerous. The military has made legislative changes to create a tougher operating environment. For example, the Organisation Registration Law introduced in October 2022 makes it mandatory for NGOs and CSOs to register with local authorities and share details on sources of funding and areas of operation. It also prohibits the provision of services to those the SAC deems its opponents in areas outside the junta's control. CSOs generally operate with little international support. Yet, they are adopting strategies to remain safe and effective. The Special Rapporteur on human rights in Myanmar has described 'the essential and awe-inspiring work being done by Myanmar CSOs in the most challenging of circumstances'. CSOs in Myanmar are vital for the struggle against serious human rights violations by the military – including the rights to freedom of expression and privacy – and against increasingly widespread surveillance and multiple attacks on fundamental freedoms.

Over a 12-month period we conducted extensive interviews with stakeholders in and outside Myanmar. All activists, company representatives, human rights experts, and members of CSOs we spoke to stressed that there is little hope for human rights advocacy with the current military regime and that public engagement in Myanmar faces nearly insurmountable challenges. Through discussions with the CSOs, it would be beneficial to jointly determine the future they want for Myanmar.

Yet even in extremely challenging contexts – and Myanmar is perhaps the most challenging one for CSOs – there are prospects for finding some space for productive civil society engagement with ICT. Networks and alliances, including with the international community, donors, and NGOs, are significant. But goals need to be realistic, recognising the importance of small steps and establishing the building blocks of better governance. They also need a longer-term focus that considers what the ICT legal framework and businesses should look like after a civilian government resumes.

With these considerations in mind, ARTICLE 19 recommends the following avenues for coordinated civil society action on protection of the right to privacy and freedom of expression in Myanmar. Subsequently, we offer two recommendations for businesses.

Recommendations for civil society

Recommendation 1: Engage with the international community

For decades, global efforts to address systematic human rights abuses in Myanmar have been hindered by political, economic, and strategic challenges, preventing a unified stance against the military.

The ASEAN Digital Masterplan 2025 highlighted the priority need for better regulation to protect privacy, but regional trends show countries adopting increasingly illiberal ICT laws violating digital rights. The patchy regional adherence to human rights law and the absence of regional human rights protection mechanisms mean that there is little pressure on Myanmar's military rulers to conform to any emerging standards protecting data and human rights. In this situation, much depends on the extent to which businesses uphold their responsibility to respect human rights. Civil society can play an important role by advocating for businesses to adhere to these standards and driving positive change. The Special Rapporteur on the situation of human rights in Myanmar has called on the international community 'to view Myanmar civil society as a vital partner in addressing the crisis in the country'.

Given the political sensitivities around Myanmar diplomacy, we recommend that CSOs coordinate and adopt creative strategies for advocacy with the international community. The obvious points of intervention are via the United Nations Independent Investigative Mechanism for Myanmar, special procedures such as the Universal Periodic Review, the Special Rapporteur on the situation of human rights in Myanmar, Special Rapporteur on privacy, and Special Rapporteur on freedom of expression. The UNGPs can serve as a baseline for advocacy because they reinforce the fundamental importance of multilateral, multi-stakeholder approaches to protect against, prevent, and remediate human rights impacts associated with business. The UN Working Group on Business and Human Rights has made a statement calling for businesses to conduct heightened HRDD in Myanmar.

Recommendation 2: Work with the Freedom Online Coalition

The Freedom Online Coalition brings together states sympathetic to human rights, freedom of expression, and the right to privacy. Coalition members work closely to coordinate diplomatic efforts and engage with civil society and the private sector to support internet freedom worldwide. The OHCHR puts forward the Freedom Online Coalition as an example of collaboration aimed at achieving a multilateral consensus on internet freedoms.

So far the Freedom Online Coalition has not sought to engage with CSOs in Myanmar despite some members being active in the country. We believe that CSOs could lobby the coalition and its members to coordinate diplomacy at the international level regarding Myanmar and apply some of the standards it has adopted, such as the Guiding Principles on Government Use of Surveillance Technologies.

Recommendation 3: Raise awareness about freedom of expression, privacy, and data protection among the people of Myanmar

The role of ICT businesses, data protection, privacy, and their impact on freedom of expression and human rights is an issue everywhere, but in Myanmar public awareness remains low, particularly among older users. This has begun to change following the Telenor Myanmar sale, and many people have switched to virtual private networks (VPNs) to access blocked websites such as Facebook.

Further, in Myanmar culture, privacy can be perceived negatively, as being apart from the community. It is not a word that translates easily into Myanmar language. The Myanmar Centre for Responsible Business (MCRB) notes that lack of awareness and understanding combined with the absence of a legal framework for data protection can result in people placing themselves and others at risk. There is therefore an urgent need for people to be aware that their data is not protected and that the military is monitoring online data to suppress opposition. The capabilities of the military are improving rapidly, and it is important for CSOs to understand the issue not only for privacy protection but also for the right to expression.

Recommendation 4: Secure personal data and financial transactions

It is important that the people of Myanmar, with the assistance of CSOs, take proactive measures to safeguard their personal data against surveillance technologies and the changing legal landscape. Given the challenges posed by a dispersed civil society, limited internet access in remote or ethnic areas, and the prevalence of military-controlled networks, raising awareness is a critical task. To effectively address this, local initiatives may benefit from the support of international CSOs.

Activists use both formal and informal digital networks within Myanmar for communication. It would be highly useful for them to understand the importance of data 'in motion', such as communications through encrypted platforms, which are challenging to monitor and relatively secure, and be mindful that data 'at rest' – contacts, search histories, financial transactions, and location data stored on devices such as phones or computers – is highly vulnerable to hacking, seizure, or forensic analysis. Despite its growing capability to access data through ICT providers, the military still relies on such methods to uncover sensitive information. Minimising the amount of data stored on physical devices and regularly formatting, resetting, or replacing these devices, can prevent the retention of activists' sensitive data 'at rest' and mitigate the potential risks of devices falling into the wrong hands.

Financial transactions are also increasingly under scrutiny as the military seeks to restrict funding for opposition groups and activities. Its current focus is on forensic analysis of seized devices and utilising data collected by banks and other digital finance service providers to target opposition groups and their supporters. We recommend that CSOs based in Myanmar assess the risks of using digital financial transactions and work towards ensuring activists are well informed about these fundamental threats to data protection and privacy.

Recommendation 5: Raise risks related to human rights with local businesses

It is important to promote collective action by businesses, guided by the principles outlined in the Global Network Initiative (GNI). An approach that emphasises collective influence over individual efforts holds significant potential to bring about positive change to Myanmar.

To this end, we recommend that CSOs in Myanmar actively engage in promoting awareness about freedom of expression, privacy, and data protection issues within local businesses. To achieve this, we propose the establishment or revitalisation of a Digital Rights Forum specifically designed to drive awareness initiatives in the community. This forum, to be conducted online regularly, would provide an opportunity to discuss international standards and national concerns in a way that is relatable and pertinent, identify best practices, and advocate for heightened HRDD processes. Additionally, it can help to coordinate a unified civil society action strategy and establish networks of allies among CSOs, businesses, and business people (for example chambers of commerce, industry unions, etc).

The forum could participate in industry events and discussions, as a way for CSOs to identify businesses willing to engage transparently with their operations and challenges, as well as those that may resist such cooperation. Furthermore, businesses participating in these forums may have connections within the SAC, enabling them to advocate for essential legal reforms.

Recommendation 6: Use international standards and industry-led initiatives to engage with companies operating in Myanmar

In light of the current regulatory landscape in Myanmar, which violates international human rights standards in numerous ways, it is imperative for tech companies to adopt best practices in data privacy to ensure responsible business conduct as part of their HRDD process.

Article 5 of the EU GDPR establishes that anyone processing data should to do so according to seven protection and accountability principles: (1) lawfulness, fairness, and transparency; (2) purpose limitation; (3) data minimisation; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality; and (7) accountability. Similarly, the International Association of Privacy Professionals explains that, 'there should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject'. The principle of data minimisation is particularly important for reducing privacy harms: tech companies should limit the collection of personal information to what is directly relevant and necessary

to accomplish a specified purpose, and should retain the data only for as long as is necessary to fulfil that purpose.

The GNI, an ICT industry-led initiative seeking to establish standards for responsible business decision-making regarding privacy and freedom of expression, calls for greater transparency and dialogue on mandatory, unmediated government access to data. It calls for all direct-access data collection legislation to 'provide sufficient authorization procedures, supervision, and remedy so as to ensure that surveillance conducted is proportional to the purpose for which it is authorized and provide effective guarantees against abuse', to 'allow companies to disclose information about interception and access to data on their networks', and to 'ensure that such access is disclosed to the subject in a timely manner if that data is used in any civil, administrative, or criminal proceeding'.

'Privacy by Design' is now a legal requirement under many privacy regulations across the world, including the EU GDPR. Article 25 of the GDPR, 'Data protection by design and by default', requires data controllers to implement 'appropriate technical and organizational measures' to uphold data security and privacy rights. In January 2023, the International Organization for Standardization (ISO) published a new standard, ISO 31700–1:2023, on privacy by design for consumer goods and services, which obligates ICT companies to implement it. This protects human rights across all stages of technology development.

The MCRB suggests that CSOs can also encourage companies to act in accordance with the concept of privacy by design – such as not asking for unnecessary personal data or using it for purposes other than those it was collected for, notifying if there is a risk, and communicating how they make data safe. Privacy by design means privacy is integrated into products, services, and system designs by default, through a holistic approach encompassing seven foundational principles: (1) proactive not reactive (preventive not remedial); (2) privacy as the default setting; (3) privacy embedded into design; (4) full functionality (positive-sum, not zero-sum); (5) end-to-end security (lifecycle protection); (6) visibility and transparency; and (7) respect for user privacy (keep it user-centric).

Recommendation 7: Develop a coordinated strategy for advocacy with companies

While it is understandable that CSOs fighting an oppressive regime resent businesses operating within that regime, there are few options available for advocacy. Responses to digital human rights challenges depend partly on businesses fulfilling their responsibility to respect human rights. The decision about what strategy to pursue is a difficult one that requires individuals and organisations to gather for open discussion, perhaps best facilitated by a Myanmar Digital Rights Forum as suggested earlier.

Some CSOs have adopted an adversarial approach to advocacy with ICT companies that continue to operate in post-coup Myanmar. They have rightly pointed out weaknesses in the HRDD conducted by these businesses, particularly in the post-coup sale of ICT systems to much worse providers such as those conducted by Telenor and Ooredoo. In interviews, CSOs have stated that they distrust ICT businesses and suggested that the private sector has not been transparent or open to discussion and has not consulted widely enough, focusing only on a few chosen CSO representatives. Many suggest that the very presence of business legitimises and facilitates the military regime and its violation of human rights.

Other CSOs disagree with this approach, arguing that ICT companies that do reference human rights considerations, such as Telenor, are the best in terms of transparency, openness, and engagement. They adopt a pragmatic approach of continued engagement with responsible businesses investing in the region, preferring that such businesses return to Myanmar in the future. These activists and organisations would take up Telenor's offer of continued engagement, believing that such international businesses can have at least some influence over policy and data protection in Myanmar in the future. While it is a difficult balance, both strategies can legitimately be defended.

We suggest that CSOs in Myanmar prioritise the development of a cohesive and inclusive strategy for advocacy with tech companies. This is crucial for fostering unity and addressing the challenges that ICT businesses told us they have faced in the aftermath of the coup. Open dialogues should be established to achieve this to help foster nuanced understanding and effective collaboration.

Recommendation 8: Identify and engage with responsible companies which are human rights-centred

In Myanmar's current political and economic climate, business has more influence than CSOs. For example, in February 2021 the military faced some pushback from the private sector on its draft Cybersecurity Law, leading to a partially amended draft in 2022. To date, it is unclear whether the draft law will be adopted in its current form. The experience of encouraging business advocacy and collective action against concerning legal provisions shows that it is possible to find business support for the defence of the right to privacy, especially when it affects their operations. The MCRB suggests that it may be possible to have some impact on an authoritarian regime by focusing on economic impacts and amplifying the business voice.

Most international ICT businesses want a predictable legal framework that protects people's freedom of expression and privacy. In a 2018 assessment of the human rights impacts of Facebook (now Meta) in Myanmar, consultancy firm Business for Social Responsibility (BSR) recommended that Facebook play an active role in advocating for policy, legal, and regulatory reform in Myanmar. Investors and asset managers have engaged with telecom companies in Myanmar, including Telenor and Ericsson, and requested clarification about human rights concerns and commitments. Regional businesses too are concerned with Myanmar's legal ICT regime. The Asia Internet Coalition of 16 Asian internet companies criticised Myanmar's draft laws in 2022 for undermining user privacy, limiting freedom of expression, and creating undue burdens on domestic and foreign businesses.

It is our opinion that, ideally, CSOs should engage with responsible businesses through the heightened HRDD process as outlined below to prevent future abuses and harness the leverage of influential businesses. At the same time, we recommend that they also explore advocacy campaigns, strategic litigation, and the use of international complaints and human rights protection mechanisms against any business in Myanmar that fails to respect international human rights law.

Part of building a strategy to engage business is recognising the reality of ICT business in a state that is unwilling or unable to protect human rights, engaged in conflict, or authoritarian by nature. Regional trends are moving away from the protection of the rights

to privacy and freedom of expression, and international norms are not implemented evenly. Much still depends on national frameworks and how businesses operate within them.

Recommendation 9: Advocate for responsible investment and respect for human rights

It would be useful for CSOs to collaboratively define clear expectations for responsible investors in Myanmar's ICT sector. Advocating for 'responsible' ICT businesses to adhere strictly to human rights principles and implement rigorous HRDD is essential. CSOs could emphasise that businesses have the option of not engaging with other businesses or of withdrawing from the country rather than contributing to human rights violations. Through coordinated efforts, CSOs can guide ICT businesses in promoting ethical practices, ultimately fostering a responsible and sustainable ICT sector in Myanmar.

In the meantime, we recommend that CSOs demand that businesses operating in Myanmar at the very least adopt transparency provisions and safeguards that reflect international best practices. When businesses are obliged, through legislation or otherwise, to provide the military with private data, users should be informed. The public should also be made aware of actions they can take to help protect their data. Specifically, CSOs can ask companies to make human rights impact assessments' public, embed legal safeguards in their operations, engage in industry discussion and collective action – for example through the GNI – and establish operational-level grievance mechanisms.

The private sector cannot justify negative human rights impacts merely by the need to comply with domestic law. Instead, there may be times it needs to challenge the state. The OHCHR's interpretive guide on the corporate responsibility to respect human rights notes that if an ICT company automatically defers to every government request for information about users, regardless of the human rights implications, it runs the risk of contributing to abuse.

Many CSOs argue that their advocacy efforts should specifically target the reputations of those ICT businesses with direct or indirect military connections or who act in complicity with the military to violate human rights or commit atrocity crimes. This targeting can focus on reputational damage in the short run, while CSOs build cases against these companies

to pursue accountability and access to justice and to annul their contracts in a future, democratic Myanmar. Justice for Myanmar has done exemplary work identifying businesses, international agencies, and foreign governments supporting the military in Myanmar.

Myanmar's current investment law, for example, allows for screening investors based on human rights performance. The Investment Rules instruct the Myanmar Investment Commission (MIC) to consider whether investors have demonstrated a commitment to responsible investment – for example, whether they have previously broken the law in Myanmar or any other jurisdiction. The rules explicitly mention environmental, labour, tax, anti-bribery, and corruption or human rights law. If an investor is determined to have committed a crime, violated environmental protection standards, or been involved with human rights abuses, the MIC can refuse it a permit. If such a company applies for an investment permit, CSOs can play a part in ensuring that the MIC – or any future screening body – is aware of the company's record and advocating for the refusal of a permit.

Recommendation 10: Ask business to carry out a heightened human rights due diligence process

Businesses investing or operating in conflict-affected areas have a heightened responsibility to assess the human rights impact of their operations and to adopt mitigation measures where any human rights risks or negative impacts on conflict dynamics are identified.

Sufficient information on the heightened HRDD must be made public to allow for the evaluation of its adequacy by CSOs. Business should also demonstrate their attempts to use their leverage in dealing with the military, even if these are unsuccessful. Advocacy and dialogue with ICT businesses that do not have staff employed in Myanmar is also an important strategy, given that those with employees in the country face challenges using influence with the SAC for fear of staff security.

While there is extensive guidance on HRDD for companies, such as on how they should engage with stakeholders and on provisions of remedy for affected people, there are few resources for CSOs on how they can best call for a heightened HRDD process to protect

human rights in conflict-affected areas. One relevant resource is GNI's how-to guide for civil society, but it does not deal specifically with conflict-affected areas and heightened HRDD processes.

First, CSOs should call upon businesses to focus on three main steps that expand on normal HRDD: (1) identify the root causes of tensions and potential triggers, which include the local context and background of conflict; (2) map the main actors in the conflict – this includes learning the motives and capacities of all actors; and (3) identify and anticipate the impacts of the business's operations, products, or services on existing social tensions and relationships among the various groups, and the potential to create new tensions or conflicts.

The guide on heightened HRDD for business in conflict-affected contexts by the UN Development Programme and the UN Working Group on Business and Human Rights includes a useful set of risks and indicators relevant to recognising when heightened HRDD is required. This applies to all of Myanmar, whether there is an active armed conflict or not.

We recommend that CSOs advocate for business to fulfil the heightened responsibilities outlined in Part 2 of this framework.

Principle 17 of the UNGPs indicates that due diligence 'should be ongoing, recognising that the human rights risks may change over time as the business enterprise's operations and operating context evolve'. CSOs should use consultation to ensure that both HRDD and conflict assessments are ongoing and undertaken before a new business activity or relationship is established, prior to major operational decisions, and in response to changes on the ground, as well as periodically throughout operations.

We believe it is crucial for CSOs to insist that the heightened HRDD process be linked to business decision-making, reported to senior management, and not limited to public relations. A human rights lawyer employed by a company with investments in Myanmar explained that, despite HRDD processes, there was no clear link to upper management. HRDD was undertaken by the public relations department and did not inform key business decisions taken by regional and international company CEOs. The UNGPs call for a company-wide commitment to respect human rights and for a joined-up strategy on

HRDD. It is important for CSOs to try to ensure this happens in practice, and not be limited to the business's website and promotional materials.

As highlighted by the OHCHR's B-Tech project, the key responsibility is for ICT companies to 'know and show' how they address adverse impacts resulting from the use of the products, services, and solutions they provide. Users and investors also have a responsibility to respect rights, but this does not diminish the critical responsibility of ICT providers to implement and act upon HRDD.

The UNGPs require meaningful consultation with affected stakeholders and business partners. Heightened HRDD requires additional local and international expertise on human rights and humanitarian law, conflict analysis, development cooperation, local cultures, power inequities, and vulnerable groups. Given the obvious security concerns and restrictions on the freedom of CSOs, meaningful consultation is not always feasible today in Myanmar, and fulfilling the business responsibility to respect human rights in the post-coup environment is nearly impossible. Given these difficulties, any ICT investment based on heightened HRDD will require public mitigation, leverage, and responsible exit plans.

Recommendation 11: Stress the importance of conflict analysis and local expertise

A heightened HRDD process should focus on impact on specific human rights and consider the wider context of the conflict itself. Conflict always creates negative human rights impacts, and businesses that contribute to the conflict capabilities of the SAC are also causing or contributing to human rights abuses, but even a responsible business that tries to be neutral will influence conflict dynamics. It would be useful for CSOs to be ready to demonstrate to businesses how their presence impacts the conflict and therefore human rights, and how business activities will be perceived in the light of the absence of the rule of law in Myanmar or independent oversight of the SAC.

More than anything else, CSOs' local knowledge and expertise can help businesses engaged in heightened HRDD to understand the context in which they are investing and the nature of their business relationships.

According to Principle 12 of the UNGPs and Commentary, businesses must consider international humanitarian law, which applies in situations of armed conflict alongside human rights, whose application does not cease in times of armed conflict.

We recommend that CSOs try to ensure that businesses consider humanitarian law in HRDD processes in Myanmar. This may include explaining the challenges of operating in areas where armed non-state actors are present. CSOs can provide businesses with a clear understanding of the structure, territory, objectives, and political agenda of armed groups as well as the support of local populations. In addition, while the rights to privacy and freedom of expression are poorly protected in Myanmar and the region, violations of these rights remain relevant for businesses operating in conflict-affected areas.

Recommendation 12: Participate in meaningful consultation with responsible businesses

Companies are expected to start consultations before signing contracts and continue them through project implementation to closure. The OECD Due Diligence Guidance for Responsible Business Conduct expects heightened due diligence before investment. UNGPs' Principle 18 calls for meaningful and timely consultation with relevant stakeholders whose human rights are affected by a company's operations, products, or services. To comply with international standards, businesses should 'consult externally with credible, independent experts, including … governments, civil society, national human rights institutions, and relevant multi-stakeholder initiatives'.

We recommend that CSOs use any consultation and HRDD process before ICT businesses set up operations in Myanmar to press for a public commitment to human rights across all operations, signalling a break from the past and an awareness of international standards. This commitment should be communicated widely and directly to affected stakeholders, whether they be individuals whose rights are potentially impacted or wider communities affected by the conflict. Some ICT businesses in Myanmar have made such commitments, but few have examined conflict impact in detail, so CSOs could push future investors to do so.

We also recommend that CSOs advocate that businesses consult with all legitimate stakeholders. This must include those identified as most impacted by or vulnerable to the

conflict, as well as any other actors that the conflict may affect. CSOs could stress that an ICT business's responsibility extends not only to its own operations and people but to the states in which it operates and the individuals and communities of these states.

Further, we suggest that CSOs emphasise the security risks for stakeholders in the consultation process. Guaranteeing safety may not be possible. The government may oppose consultation with certain groups or may outlaw contact with its opposition. The unpredictable and risky nature of conflict-affected areas may prevent ongoing consultation.

In practice, stakeholder mapping must identify all stakeholders' economic and social agendas and interests, leverage, representation of vulnerable groups, and roles in the legal and policy framework. Building local connections requires resources, but it is crucial for respecting human rights and avoiding negative impact. CSOs can help to foster extensive, reliable local connections but must ensure that the business understands that this takes time and patience. If this is impossible due to conflict or opposition from the government, the business must consider whether it can fulfil its responsibility to respect human rights and not negatively impact the conflict.

CSOs can highlight the experience of Telenor Myanmar as an example of what happens without heightened HRDD in a conflict-affected country. Telenor operated in Myanmar from 2014. This was informed by a thorough human rights impact assessment as part of the pre-investment due diligence commissioned by Telenor from consultancy firm BSR, based on BSR's human rights impact assessment framework but also covering labour rights, bribery and corruption, and environmental sustainability. However, from the documents disclosed by Telenor or BSR, the company does not seem to have carried out a conflict analysis or consulted with conflict experts before investing.

CSOs can show ICT businesses how their business operations might contribute to or be linked to actions by the SAC or business partners that violate human rights, cause instability, or exacerbate conflict. The links between business, government, and the military in Myanmar are extensive, and this should go beyond ensuring that business partners are not on the US or other sanctions list.

Recommendations for businesses

Recommendation 13: Harness leverage to influence government and business relationships

The UNGPs recognise the 'the ability of a business enterprise to effect change in the wrongful practices of another party that is causing or contributing to an adverse human rights impact'. Leverage should be used to improve risky relationships and a business, the UNGPs explain, 'should be able to demonstrate its own ongoing efforts to mitigate the impact and be prepared to accept any consequences – reputational, financial, or legal – of the continuing connection'. International organisations encourage businesses in conflict-affected areas to advocate for reform of domestic legislation that conflicts with international human rights standards, while appealing to the government's self-interest in making conditions easier for responsible foreign investors.

It is important for CSOs to understand that businesses are experts at leverage. They use it all the time in commercial relationships and in lobbying government for beneficial conditions. This power should be harnessed to lessen impacts on human rights and conflict. In pursuing this, however, both CSOs and business need to consider the challenges posed by the Myanmar regulatory framework, detailed earlier in this report.

We suggest that CSOs help responsible businesses to identify points of leverage, strategies, and activities that can promote change, as well as evaluate mitigation strategies and identify barriers to success. They can work with responsible businesses, again using the Digital Rights Forum, on multi-stakeholder capacity-building programmes for users, businesses, and government officials. They could encourage ICT businesses to undertake collective action as an industry and through engagement with relevant international organisations such as GNI.

Adopting preventive safeguards is complicated in Myanmar. Some tech companies have adopted preventive and mitigating actions, establishing protocols to ensure the immediate deletion of data, and training staff in situational awareness and digital security. Telenor had identified the issues of lawful interception and surveillance as risks to human rights in the regulatory framework during their HRDD process prior to market entry. Telenor was informed shortly after the 1 February coup that further disclosures of authority directives

could have serious security consequences. Telenor decided to stop the disclosures, balancing the principle of transparency against the safety of employees in Myanmar.

There are better leverage opportunities before investment decisions are made. In high-risk countries, the OECD Due Diligence Guidance for Responsible Business Conduct expects heightened due diligence 'prior to forming new first-tier high-risk business relationships'. Businesses should use leverage to set out conflict-related human rights expectations from the start of their engagement, referring to relevant laws and international standards. Clear rights and conflict-related benchmarks can be formally captured in contracts, MoUs, or licensing agreements.

Nevertheless, the credible prospect of disengagement can be a powerful leverage tool for incentivising business partners – including host states – to improve their human rights performance. Companies should emphasise disengagement at the beginning of a business relationship, when screening possible trading patterns and drafting specific contractual clauses, and should agree on a process for triggering it.

Recommendation 14: Discuss divestment options and responsible exits

Heightened HRDD increases the need for a responsible exit strategy, because it considers the additional impacts of the business on conflict. CSOs recommend disengagement where a business partner has committed a deliberate and irremediable violation of a human right. Both the UNGPs and the OECD Guidelines outline the decision-making process for responsible exit, citing factors such as severity of human rights impacts, previous attempts at mitigation, whether it is a crucial relationship, and how much leverage the business exerts, but they do not provide a universally applicable answer as to whether a company should stay or leave a certain country. In practice, however, the costs and logistics of responsible exit mean that it is rarely considered unless there is no other choice.

The UN Working Group explains that the road map for responsible exit is based on mitigating risks to stakeholders, not profit and reputation. Responsible exit requires business to anticipate and plan a clear exit strategy in advance, to identify and assess the impacts of disengagement on all stakeholders, and to develop mitigation strategies. This should include providing reasonable notice to stakeholders, protecting staff salaries and

capacity-building to mitigate the loss of employment, and ensuring the security of remaining staff who cannot be evacuated.

The question is never as simple as staying or going: it is a matter of how you stay and how you go. When deciding on a responsible exit, businesses often consider their influence and leverage over the human rights and conflict impacts of both their operations and their relationships. In practice, it may be beneficial for a responsible business to remain in a conflict-affected area despite the risk of conflict or human rights impacts.

The exiting business must also remediate the adverse impacts its exit may cause or contribute to, including those caused by business relationships from which it has disengaged. It is crucial to have a publicly available, clearly benchmarked, rights-based, and conflict-sensitive divestment and disengagement plan.

Myanmar CSOs have experienced and have made it clear through advocacy and access to justice initiatives that an unplanned, hasty exit by ICT investors can negatively impact human rights and the conflict. If a business decides to exit, it needs a proper exit strategy. We recommend that CSOs push for proactive, comprehensive risk assessments that include conflict risks. The various trade-offs, like whether to stay or go, should be assessed ahead of time. Interviewees from CSOs stressed that most exits from Myanmar have been irresponsible in that they were reactive to the coup. Instead, a responsible exit requires a clear, public, human rights benchmarked plan. This plan must consider whether exiting could exacerbate tensions and whether these impacts outweigh the benefits.


ARTICLE 19