Myanmar’s Military Struggles to Control the Virtual Battlefield

Asia Report N°314 | 18 May 2021

Headquarters
International Crisis Group
Avenue Louise 235 • 1050 Brussels, Belgium
Tel: +32 2 502 90 38 • brussels@crisisgroup.org

Preventing War. Shaping Peace.

Table of Contents

APPENDICES

Principal Findings

What's new? After first trying to restrict internet use by banning social media platforms, enacting legal changes and ordering night-time outages, the Myanmar military has shut down nearly all access to the web in the wake of the 1 February coup d'état and started establishing a countrywide intranet with limited services.

Why did it happen? The military was losing the online battle and felt it had few options. Activists have used social media platforms – particularly Facebook – highly effectively to organise protests, galvanise the public and document abuses, while the military has been banned from Facebook altogether, limiting its outreach abilities.

Why does it matter? The internet shutdown has undermined the opposition movement – particularly its ability to organise street protests – but at huge social and economic cost. The military faces a long-term strategic challenge in managing internet use as it seeks to consolidate power in the coup's wake.

What should be done? Technology companies should help keep Myanmar's online space as open and safe as possible, particularly by expanding free access to secure virtual private networks. Foreign governments should embargo "dual-use" items that can be used for repressive purposes, including software, and strengthen enforcement by better policing sales made through middlemen.

Executive Summary

Since the 1 February coup d'état in Myanmar, the online space has become a parallel battlefield on which the country's military and its opponents try to rally supporters, share information and control the narrative around events unfolding in the country. This virtual struggle has been vitally important to both sides. The scale of popular anger at the military, the regime's lack of technological capacity and the policies of social media companies have made it difficult for the military, known as the Tatmadaw, to gain the upper hand. At first, the junta resorted to temporary internet cuts and filtering websites, but when these had little impact, it moved to broader shutdowns, leaving the vast majority of people in Myanmar disconnected. It appears to have no viable long-term strategy for controlling online space, and prolonged internet outages are likely while it struggles to consolidate power. Foreign governments and technology companies should endeavour to keep what is left of Myanmar's internet as open and its users as safe as possible, while restricting sales of equipment and software that the military could use to oppress opponents.

The liberalisation of the telecommunications sector was a signature achievement of Myanmar's decade-long experiment with democracy. In the early 2010s, then President Thein Sein took the bold step of breaking the monopoly of the state telecoms firm by inviting foreign mobile operators to invest. His semi-civilian government lifted restrictions on websites, overhauled laws and allowed new international gateways connecting the country to the global internet. As a result, billions of dollars of investment flowed into the country and mobile phone penetration rose from just 10 per cent to more than 100 per cent (many users have more than one SIM card) in the space of a few years, with well over half the adult population online through mobile data. This digital revolution brought significant social and economic benefits but also new challenges, particularly in the form of disinformation and hate speech. The use of online platforms to whip up hatred of the Rohingya Muslim minority in Rakhine State during the Tatmadaw's campaign against them in 2017 is particularly notorious.

While the coup has brought an abrupt end to much of this online freedom, the openness of the internet in Myanmar was under threat even prior to 1 February. Since the National League for Democracy (NLD) took office in 2016, authorities have turned to vaguely worded defamation laws to lock up government opponents and ordinary social media users alike. At the Tatmadaw's request, the NLD government reintroduced filtering of websites and backed internet shutdowns in Rakhine State, where the military was waging war against a local insurgent group, the Arakan Army. Before it was deposed, the civilian government had also been drafting a Cyber Security Law requiring technology companies to keep user data onshore and hand it over to the authorities whenever requested. It was also taking steps to gain real-time access to user data from operators.

After taking power, the Tatmadaw drastically ramped up online repression. It enacted legal amendments to gain access to user data and prosecute prominent opponents. It also issued daily notices to mobile operators and internet service providers to restrict access to certain websites and virtual private networks (VPNs) that can skirt internet filtering. These responses reflect the military's keen awareness of the important role social media plays in spreading information and shaping public opinion; it has grappled with how best to manage the online sphere to support its strategic objectives since the very first hours of the coup.

In spite of the regime's censorship efforts, opposition forces have so far successfully used the internet to promote their political agenda, organise protests and share information about events inside the country with each other and the world. They have primarily relied on free tools that require little skill or knowledge, such as encrypted messaging services, free VPNs and censorship circumvention applications.

The military has responded by almost entirely shutting down internet access. Although the junta has not been technologically sophisticated in its actions, it has approached the challenge methodically, gradually ramping up internet shutdowns as it deemed necessary to achieve the desired effect. The mass outage it eventually opted for has already hurt the opposition movement, making it harder to organise protests and coordinate other activities.

But the junta has also come head to head with forces beyond its direct control, particularly the policies of major social media platforms. Having heeded lessons from the way its platform was used during the authorities' anti-Rohingya campaign of 2017, Facebook removed all military and some Myanmar government pages following the coup, dealing a major blow to the Tatmadaw's ability to spread pro-regime messaging and leaving it reliant on less widely used websites and platforms. Tatmadaw personnel, however, appear to have found an outlet in TikTok, which was initially slow to respond to content that violates its guidelines, such as videos of Myanmar soldiers wielding weapons and making threats against protesters. TikTok has since made efforts to clean up its platform but has stopped short of banning the Tatmadaw.

The Tatmadaw has faced significant online opposition before. In Rakhine State, the Arakan Army has harnessed the power of social media and other communications technologies with great effectiveness over the last few years, which partly explains its success in inflicting heavy losses on the Tatmadaw. There, the military eventually responded by pushing the civilian government to filter websites and shut down the internet on security grounds. The measures were somewhat effective in hindering Arakan Army operations, but also substantially hampered commerce and humanitarian efforts, turning the local population even more solidly against the Tatmadaw. The fact that the military is largely falling back on these same blunt methods of control following the February coup suggests it has not yet developed alternative strategies that could limit disruption and exact a lesser socio-economic toll.

Myanmar's military will face significant challenges shifting to a more sophisticated response to online dissent than wide-scale internet shutdowns. As it lacks the financial and human resources to develop a local version of China's "great firewall", in which access to the global internet is heavily restricted and local content actively censored, it has started developing what appears to be the first stage of an "intranet", where mobile users have access only to whitelisted applications. But this course will inevitably limit its ability to offer anything more than the most basic services, with a major impact on the economy. Even if the regime were to receive assistance from sympathetic outside actors to expand its capacities, domestic opposition would make it difficult to recruit the local expertise needed to maintain a more repressive system,

and the more tech-savvy users are likely to find ways to exploit the intranet to gain unfettered access to the wider web.

Nevertheless, technology companies and foreign governments should ensure that they are not directly or indirectly assisting the Tatmadaw's efforts to control the internet or digitally suppress the opposition. Before the coup, the military and civilian-controlled branches of government had acquired or sought to acquire a wide array of technologies from foreign companies – many of them based in the United States – to monitor social media, unlock devices, recover data and watch the public. These technologies are now all under military control and will likely be used to suppress dissent. To stop more from making their way into the generals' hands, foreign governments should introduce or broaden arms embargoes to cover "dual-use" equipment, software and technologies that could be employed to suppress political opposition. They should also enforce such bans properly by strictly policing sales through brokers.

More broadly, both technology companies and foreign governments have a role to play in supporting openness of the internet and user security. As the military increasingly targets social media users for content they post, companies and governments can help internet users in Myanmar gain access to the knowledge and tools to keep themselves safe while online. They should endeavour to make sure secure VPNs are freely available to activists and others likely to be at high risk of surveillance. Social media companies should also ensure they are adequately monitoring the Tatmadaw and its personnel on their platforms in light of both recent events and its past online behaviour.

Yangon/Brussels, 18 May 2021

International Crisis Group
Asia Report N°314 **18 May 2021**

Myanmar's Military Struggles to Control the Virtual Battlefield

I. Introduction

Telecommunications liberalisation was a signature reform of President Thein Sein's administration, which governed from 2011 to 2016, initiating Myanmar's transition to semi-civilian rule. Under military rule, internet access had been tightly controlled, expensive and slow: a mobile SIM card, without internet access, cost as much as $1,000 shortly before Thein Sein came to power. Reformers in the new government quickly identified the sector as an area in which they could attract investment and deliver tangible benefits to Myanmar's citizens, and announced plans for a tender of two mobile operator licences as soon as 2012.[1] Other important reforms included the lifting of all filtering on dissident websites and steps to encourage investment in international gateways to improve internet speeds.[2]

The pace of change was rapid: by the time Thein Sein left office, in 2016, the telecoms sector had attracted billions of dollars in new foreign investment, and tens of millions of people were enjoying fast, cheap and unfiltered internet for the first time. Because the web reached much of Myanmar so late, most users went straight to 3G or 4G mobile internet, leapfrogging slower connections and broadband.[3] Telenor of Norway and Ooredoo of Qatar launched their services in 2014, joining state-owned Myanmar Posts and Telecommunications (MPT), which partnered with a Japanese consortium to improve its services. The Myanmar military, or Tatmadaw, in partnership with Viettel of Vietnam and a consortium of Myanmar companies, launched a fourth operator, Mytel, in 2018.[4]

For many people getting online for the first time, the internet was limited almost exclusively to Facebook.[5] Helped along by the company's "free basics" package that allowed users to log on without incurring data charges, and later by promotions that made it more affordable to use Facebook than other parts of the web, estimated user numbers skyrocketed – from barely one million accounts in 2013 to ten million three years later, eventually reaching over 27 million, or around 50 per cent of the population, as of January 2021.[6] Facebook quickly became not just a place to keep in contact with family and friends, but also a major source of information, and an arena for political discussion, with little competition from other social media platforms.

[1] "The Political Road to Digital Revolution: How Myanmar's Telecoms Reform Happened", Developmental Leadership Programme, January 2017.
[2] "Burma lifts ban on international websites", *The Irrawaddy*, 16 September 2011.
[3] See "Foreign investment booms in Myanmar's telecoms", *Nikkei Asian Review*, 20 April 2017; and "The Facebook-loving farmers of Myanmar", *The Atlantic*, 21 January 2016.
[4] Mytel has been accused of influence operations targeting competitors on Facebook and providing the military with "off-budget revenue". See "Myanmar's connectivity curse", Medium, 12 February 2021; and "Nodes of Corruption, Lines of Abuse", Justice for Myanmar, 20 December 2020.
[5] Crisis Group is a partner of Facebook and in that capacity has occasionally been in contact with Facebook regarding misinformation on the platform that could provoke deadly violence.
[6] See "Facebook vows to tackle hate speech", *The Myanmar Times*, 12 July 2014; and "Digital 2021: Myanmar", We Are Social and Hootsuite, January 2021.

Although affordable internet access brought many positive changes to Myanmar, the dark side of this rapid liberalisation was illustrated starkly after the Arakan Rohingya Salvation Army (ARSA) attacked police outposts in northern Rakhine State in October 2016. The Tatmadaw responded with a brutal retaliatory campaign against both the group and the persecuted Rohingya Muslim minority that lives in the region. Violence escalated in August 2017, with the military again employing appalling levels of indiscriminate force and driving mass displacement, and UN experts subsequently called for Tatmadaw leaders to be investigated and prosecuted for genocide.[7] During this period, Facebook became a giant platform for hate speech directed at the Rohingya Muslim minority and, despite numerous warnings that such speech was appearing on its website dating back to at least 2013, the company had few mechanisms in place to counter Myanmar-language content; instead, it relied almost solely on local monitoring networks.[8]

Since then, Facebook has paid much closer attention to Myanmar, in particular by building its capacity to monitor vernacular content through human moderators and artificial intelligence.[9] This experience informed its approach to Myanmar's 2020 election, when the social network moved quickly to remove the relatively small amount of disinformation being posted to its platform.[10] Since the coup, it has banned the Tatmadaw entirely, and removed military-controlled media outlets, including state broadcasters.[11]

If Facebook and other social media platforms have changed the way in which they work in Myanmar, the Tatmadaw has struggled to use the insights it has gained in recent years to develop more sophisticated tactics. In seeking to squelch online opposition following the February 2021 coup, it continues to rely heavily on the crude measures it used in targeting the Arakan Army in 2019 and 2020, notwithstanding their costs and limitations.

This report examines how the military has sought to control internet access and use amid conflict in Myanmar since 2019. It is based on research conducted between October 2020 and April 2021 and builds on Crisis Group's years of fieldwork and analysis on conflict dynamics in Myanmar.[12] Given the constraints on travel due to COVID-19 and the military takeover during this period, the research was conducted

[7] "Report of the Independent International Fact-finding Mission on Myanmar", 12 September 2018.

[8] "How Facebook's rise fueled chaos and confusion in Myanmar", *Wired*, 6 July 2018. Testifying before the U.S. Congress in April 2018, Facebook CEO Mark Zuckerberg acknowledged that the company needed to "do more" on Myanmar, outlining several steps it was taking to improve moderation of Myanmar-language content. For more, see "Transcript of Mark Zuckerberg's Senate hearing", *The Washington Post*, 11 April 2018.

[9] "Facebook turns to artificial intelligence to fight hate and misinformation in Myanmar", *The Washington Post*, 16 August 2018.

[10] Crisis Group interviews, social media researchers, November 2020 and March 2021.

[11] "Myanmar military banned from Facebook and Instagram with immediate effect", Facebook, 24 February 2021.

[12] On the coup and subsequent events, see Crisis Group Asia Briefing N°166, *Responding to the Myanmar Coup*, 16 February 2021; Richard Horsey, "A Close-up View of Myanmar's Leaderless Mass Protests", Crisis Group Commentary, 26 February 2021; and Crisis Group Asia Briefing N°167, *The Cost of the Coup: Myanmar Edges Toward State Collapse*, 1 April 2021. On earlier events, see the citations throughout this report as well as Appendix C.

remotely via telephone, using pre-existing networks of contacts. In Yangon, these included social media and conflict researchers, data privacy and digital rights advocates, lawyers, security officials, technology entrepreneurs and representatives of major technology firms, while in Rakhine State, interviewees included politicians, activists, civil society leaders and ordinary residents. Crisis Group also consulted social media platforms regarding their Myanmar policies and responses to the coup.

II. Rakhine: A Test Run for Repression

Many of the approaches that the military has employed to try to control the online world since the 1 February coup were tested during an earlier conflict, when it waged a bloody war against the insurgent Arakan Army in central and northern Rakhine State in 2019-2020. During that period, the Tatmadaw witnessed for the first time how its opponents could use social media to devastating effect if given the opportunity. After almost a decade of unfettered internet access across the country, it urged the National League for Democracy (NLD) government to order internet shutdowns and website filtering in order to undermine the insurgency's operations. The conflict gave the Tatmadaw insights into the impact of these restrictions, the technological challenges linked to controlling online content and the domestic and international response it could expect when resorting to such measures.

A. *The Arakan Army: Sowing the Seeds of an Insurgency*

Among Myanmar's many armed groups, the Arakan Army, which seeks greater rights and autonomy for the Rakhine Buddhist community, has harnessed the country's new online space to greatest effect since its founding in 2009. At first, the group employed traditional techniques, such as newsletters and word-of-mouth campaigns, to build support and recruit.[13] But as it grew in strength and began quietly shifting forces from its base in Kachin State to Rakhine State from 2014, its young leaders – particularly its charismatic chairman Twan Mrat Naing, a former tour guide – started pushing out relatively sophisticated posts and videos on social media. These outlined their vision for self-determination, which they called "The Way of Rakhita", labelled the Tatmadaw and Myanmar government "invaders", and promised to lift the yoke of Burman oppression from Rakhine State and restore it to its former glories. Deputy commander Nyo Twan Awng became a popular presence on Facebook from around 2016, attracting thousands of followers with posts about the group's activities and the political situation in Rakhine State.[14]

The Arakan Army's use of social media was not limited to propaganda. The group also used Facebook to solicit donations and recruits during these formative years (and has continued to do so). It selected the most effective platforms for reaching different audiences, whether that was WeChat to recruit young Rakhine near the Chinese border or WhatsApp to send statements to journalists.[15] While its leaders crafted engaging social media posts, the group issued formal statements in multiple languages, including Chinese, and created high-quality videos for YouTube. Later, its

[13] Crisis Group interview, conflict researcher, November 2020.

[14] Much of this content has disappeared and does not appear to have been preserved after Facebook banned the Arakan Army and several other ethnic armed groups from its platform in February 2019. Some of it, however, remains accessible on YouTube, including an English-language video from early 2018, "The Way of Rakhita", that has amassed more than two million views. For further discussion of the use of social media by the Arakan Army and other ethnic armed groups in Myanmar, see Stein Tønnesson, Min Zaw Oo and Ne Lynn Aung, "Pretending to be States: The Use of Facebook by Armed Groups in Myanmar", *Journal of Contemporary Asia*, 4 May 2021.

[15] Crisis Group interview, conflict researcher, November 2020.

reports on clashes with the Tatmadaw featured maps with precise details, enhancing its information's credibility in the eyes of users.[16]

Crucially, improvements in communications technology enabled the Arakan Army to bridge the distance between its leaders in northern Kachin State and Rakhine communities some 1,000km away. Earlier Rakhine insurgencies, such as the Arakan Independence Organisation and Arakan Liberation Party, had foundered when they attempted to move from their border bases near China and Thailand to gain a foothold in Rakhine State.[17] The combination of online access to Rakhine communities, combined with its more straightforward ethno-nationalist ideology, helped the Arakan Army to succeed where its predecessors had failed.

The group used technology in creative ways to bridge the physical distances and build support. One video that circulated widely on social media shows the group's leader, Twan Mrat Naing, speaking on a computer screen to villagers in Rakhine State, who are asking him questions about the Arakan Army and its activities. "Without Facebook, the Arakan Army would have found it very difficult to get a popular following", commented one social media researcher.[18] A Rakhine civil society leader confirms:

> At first, I noticed the Arakan Army theme songs spreading on Facebook – these songs were really penetrating Rakhine society, becoming popular. Only later did I find out that the Arakan Army was not actually here [in Rakhine State] and used the internet to spread their information. From 2018, many people – including my friends – talk about the Arakan Army whenever we meet.[19]

The Arakan Army's propaganda landed on fertile ground. Rakhine State is among Myanmar's poorest, and political liberalisation and outbreaks of communal violence since 2012 had heightened ethno-nationalism among its majority Rakhine population. Rakhine political parties had performed strongly in the 2010 and 2015 national elections, but Naypyitaw had blocked them from assuming any real power. Resulting frustrations were at times channelled at the Rohingya Muslim minority to horrific effect, but the Arakan Army used its online propaganda to portray the Burmans, who control the central government, the administrative apparatus and the armed forces, as the real enemy. In January 2018, government forces played into that narrative by opening fire on demonstrators at the town of Mrauk-U, the former capital of the once-flourishing Rakhine kingdom, killing seven people. Later that month, the state's leading politician, Aye Maung, was arrested for a speech in which he said the Burmans treated the Rakhine like slaves. He was later convicted of treason and sentenced to twenty years' imprisonment.[20]

[16] For detailed discussion of the Arakan Army's communications strategy, see David Scott Mathieson, "The Arakan Army in Myanmar: Deadly Conflict Rises in Rakhine State", U.S. Institute of Peace, November 2020, pp. 11-12.

[17] Martin Smith, "Arakan (Rakhine) State: A Land in Conflict on Myanmar's Western Frontier", Transnational Institute, December 2019, p. 39.

[18] Crisis Group interview, social media researcher, November 2020.

[19] Crisis Group interview, Rakhine civil society leader, November 2020.

[20] For more, see Crisis Group Asia Report N°307, *An Avoidable War: Politics and Armed Conflict in Myanmar's Rakhine State*, 9 June 2020.

Despite the longstanding grievances, emerging tensions and growing evidence of a strengthening Arakan Army presence in Rakhine State, the government and Tatmadaw were ill prepared when the group landed its first major blow. On 4 January 2019 – Myanmar's Independence Day – Arakan Army forces staged coordinated attacks on Border Guard Police posts, killing thirteen officers and injuring nine others. Naypyitaw responded swiftly, with the civilian administration ordering the military to undertake "clearance operations" to "crush" the insurgent group, which now controlled somewhere from 5,000 to 10,000 troops.[21] Over the next two years, the fighting in Rakhine and southern Chin States was the fiercest Myanmar had experienced in decades, with thousands of combatants and civilians killed, and hundreds of thousands displaced.[22]

Mobile internet and social media continued to be important tools for the Arakan Army once conflict escalated in January 2019. It used them for operational purposes, for command and control, and to gather intelligence, as well as to solicit donations and to recruit. In the early stages of the conflict, the group relied on mobile internet and common messaging applications to stage mass offensives, as well as highly effective ambushes of Tatmadaw units. The armed group used these tools to receive intelligence from civilians – principally, the location of government forces – and to coordinate its combatants.

The Arakan Army also relied on the internet and social media to help it reach its objective of dismantling the government administration across much of central and northern Rakhine State. To this end, the group used social media to publicly threaten "traitors" and issue warnings to local government officials, including police officers, backing up these threats with targeted killings. Fear of the Arakan Army – or alternatively of being detained by the Tatmadaw as an insurgency collaborator – prompted many local officials to resign, directly leading to the administrative breakdown.[23] In an attempt to build up its legitimacy, the Arakan Army then used official statements and social media posts to position itself as the de facto governing authority in these areas.[24]

The Arakan Army continued to use social media throughout the conflict but Facebook's decision, in February 2019, to ban it from its platform for being a "dangerous organisation" has had a significant impact on its capacity to communicate online.[25]

[21] Crisis Group Asia Briefing N°154, *A New Dimension of Violence in Myanmar's Rakhine State*, 24 January 2019.

[22] Total casualties are not known but are thought to number in the thousands; the Myanmar Institute for Peace and Security estimates that between 934 and 1,711 combatants were killed in 2019 alone. See "Annual Peace and Security Review 2020", Myanmar Institute for Peace and Security, p. 12. Civil society groups estimate that more than 220,000 people were displaced and almost 300 civilians killed. See "Five Rohingya killed in shooting incidents in Myanmar's Rakhine State", Radio Free Asia, 6 October 2020.

[23] Crisis Group interview, social media researcher, November 2020.

[24] Ibid.

[25] On 5 February 2019, Facebook announced that it was banning the Arakan Army and three other armed groups, collectively known as the Northern Alliance, from its platform in "an effort to prevent and disrupt offline harm", stating there was "clear evidence that these organizations have been responsible for attacks against civilians and have engaged in violence in Myanmar". See "Banning More Dangerous Organizations from Facebook in Myanmar", Facebook, 5 February 2019.

In the eyes of many, Facebook's move in effect tilted the online battlefield in Rakhine State in favour of Myanmar's military, which continued to use Facebook, while the insurgency fell back on less popular platforms, such as Twitter, YouTube, WeChat, VK and, more recently, TikTok. Indeed, although Facebook had banned Commander-in-Chief Min Aung Hlaing and removed some military pages due to hate speech in 2018, after the Rohingya crisis the previous year, it did not block the Tatmadaw itself from its platform until after the 1 February coup.

Facebook told Crisis Group that the Arakan Army's acts of violence had prompted it to begin a review in December 2018 that found the group met the criteria for being designated a "terrorist organisation", and therefore banned as a "dangerous organisation" under Facebook rules. The company made this finding due not only to the group's violent acts targeting civilians, but also to its alleged involvement in the illicit economy and recruitment of minors.[26] Other sources, however, told Crisis Group that the decision to ban the Arakan Army was rushed in the wake of the 4 January attacks because the company was concerned about its reputation in the wake of the Rohingya crisis.[27] In response to criticism of the ban, particularly from Myanmar civil society, Facebook moderated its policy slightly to allow "praise" for the Arakan Army.[28]

Facebook users following the conflict in Rakhine State have felt the effects of this policy in several ways. Posts with content related to the Arakan Army are subject to removal for violating community standards as expressions of "praise, support or representation" for a dangerous organisation. Repeated violations result in a person or page being banned or unpublished (ie, removed from public view). Violations can include posts containing the group's name, the names of its leaders, its logo or its announcements, but also seemingly legitimate political comment about the conflict.

Nevertheless, Facebook has not been able to completely remove support for the Rakhine insurgency from its platform. Even a cursory search reveals dozens of accounts containing the words "Arakan Army", with some of the English characters replaced with accented characters from foreign languages.[29] Some of the group's senior members were able to re-establish a presence on the platform under other names. Since other platforms have not banned it, the Arakan Army uses them (and its own website) as a platform for publishing its statements and propaganda, while seemingly fake accounts are used to redistribute the content on Facebook, in what appears to be a coordinated operation. "When the Arakan Army releases a statement on VK or their website, it pops up on Facebook in minutes", said one Rakhine activist.[30]

[26] Crisis Group interview, Facebook representative, November 2020.

[27] Crisis Group interviews, social media researcher, November 2020; industry source with knowledge of the issue, March 2021.

[28] In September 2020, Facebook placed the four Northern Alliance groups in a newly created category called "violent non-state actor", which still bans them from the platform but allows users to post "praise" of the groups without violating community standards. Crisis Group interview, Facebook representative, November 2020.

[29] "Facebook keeps failing in Myanmar", *Foreign Policy*, 21 June 2019.

[30] Crisis Group interview, Rakhine activist, October 2020.

B. *The State Fights Back*

In other circumstances, the Arakan Army's reliance on civilian communication channels could have been a major weakness and provided the Tatmadaw with a significant amount of intelligence. But the Myanmar military had seemingly very limited capacity to harvest information from telephone calls, social media and unencrypted communications. Indeed, Arakan Army members and supporters often used unencrypted applications, even with the government-owned operator MPT.[31] To disrupt enemy communication channels, the government and military were instead compelled to restrict access to the internet.[32]

The internet restrictions in Rakhine were among the longest-running anywhere in the world. In June 2019, the government's ministry of transport and communications, at the Tatmadaw's request, ordered mobile operators to stop internet access in eight townships in Rakhine State as well as Paletwa township in neighbouring Chin State. Access was restored in five townships in August 2019, before being interrupted again the following February, and then lifted in one township, Maungdaw, in May 2020. At the start of August 2020, the government permitted a resumption of 2G internet access in all areas, but in practice little changed, as it is difficult to perform even the most basic web-based functions on such low-speed connections.[33] Full internet access was restored on 3 February 2021, two days after the coup, but restricted again on 15 March all over the country (see Section IV.B below).[34]

The primary purpose of the mobile internet ban was to disrupt Arakan Army operations, including command and control and intelligence gathering. Undermining the insurgency's ability to spread propaganda, and minimising the flow of information about events on the ground – including the Tatmadaw's alleged human rights abuses – were likely secondary goals.[35] The strategy proved mostly effective in achieving Naypyitaw's key goal: the Arakan Army could no longer rely on common internet applications for command and control in most areas in which it operates, which was likely one of the reasons the group gradually staged fewer large-scale offensives from the second half of 2019.[36] The ban also made it more difficult for its supporters to provide the group with intelligence, particularly GPS locations of government forces,

[31] Myanmar has four mobile operators: MPT, Telenor, Ooredoo and Mytel. Many Rakhine users eschew Mytel because it is a military-owned joint venture, and Ooredoo because it is owned by a firm from Qatar, a majority-Muslim country. Crisis Group interviews, October and November 2020.

[32] Crisis Group interview, conflict researcher, November 2020. Had the Arakan Army been relying on encrypted communications only, the government could have asked mobile operators to switch off those particular applications.

[33] "Rakhine, Chin internet restored, but only 2G", *Myanmar Times*, 7 August 2020; and "Continued network restrictions in Myanmar from 1 August 2020 (updated 31 October 2020)", Telenor.

[34] The restoration of internet in Rakhine came following months of negotiations between the Tatmadaw and the Arakan Army, and the decision of the Arakan National Party, the state's leading political party, to work with the military regime. See Crisis Group Asia Briefing N°164, *From Elections to Ceasefire in Myanmar's Rakhine State*, 23 December 2020; and "Network restored in eight townships in Myanmar", Telenor, 3 February 2021.

[35] Crisis Group interviews, Rakhine State resident and political analyst, October 2020; conflict researcher, November 2020.

[36] Crisis Group interview, conflict researcher, November 2020.

reducing the risk that the troops would be ambushed. Finally, the internet ban diminished the amount of user-generated Facebook content about the conflict.

But a range of factors also limited the impact of the internet restrictions. On an operational level, the Arakan Army increased its use of satellite phones for command and control.[37] Because voice calls and SMS were not restricted, these services could still be used by the group's network of members and supporters on the ground to both send intelligence about Tatmadaw troop movements and disseminate information to communities.[38] Internet access was also not completely severed. Fibre-based connections remained available in several towns in the blackout zone, such as Mrauk-U, and it was often still possible to get a 3G signal in elevated areas.[39] After 2G was restored, those living in areas with unrestricted internet would copy and paste the text of news reports and share them on Facebook groups so that they could be read even with a slow connection.[40] Journalists and civil society groups were able to send information by telephone to contacts who could post online, or travel to areas with internet access to upload it directly.[41] Human rights violations were also still widely documented in mainstream and social media.

Later, at the military's request, Aung San Suu Kyi's government also re-introduced nationwide website filtering, almost a decade after such censorship had been lifted. In March 2020, the ministry of transport and communications ordered mobile operators and internet service providers to block access to 2,147 websites. Although the vast majority of these were either pornographic or part of an Interpol blacklist related to child sexual abuse, the list also included 67 sites that the government claimed were spreading "fake news".[42] Among the sites blocked were the Arakan Army's page and two Rakhine-based media organisations, Development Media Group and Narinjara. This measure was not particularly effective, either: both of these organisations' output could still be read on Facebook, which is where most people in Myanmar go for news, while information from the Arakan Army website is shared on social media by users outside Myanmar or who view the group's website inside the country using a virtual private network (VPN).

The consequences of the mobile internet ban for the Rakhine population in blacked-out communities have been significant, however. The blackout has had a negative social and economic impact on those communities, making it difficult to conduct

[37] Crisis Group interviews, Rakhine political analyst, October 2020; conflict researcher, November 2020. In September 2019, a few months after the internet ban was introduced, authorities in Mandalay arrested five alleged Arakan Army members with 40 satellite phones, high-powered binoculars and suspected bomb-making equipment. See "Mandalay on alert against Arakan Army operatives", *Myanmar Times*, 18 September 2019.

[38] Crisis Group interview, Rakhine politician close to the Arakan Army, November 2020.

[39] "Annual Peace and Security Review 2020", op. cit., p. 96.

[40] Crisis Group interview, Rakhine politician close to Arakan Army, October 2020.

[41] Although the quantity of information emerging from Rakhine State likely declined, a Myanmar Institute for Peace and Security study found only a slight effect on the speed with which civilian fatalities and injuries were publicly reported. See "Annual Peace and Security Review 2020", op. cit., p. 95.

[42] "Myanmar orders dozens of news websites blocked in crackdown on 'fake news'", Committee to Protect Journalists, 2 April 2020; and "Myanmar blocks 'fake news' websites amid COVID-19 pandemic", Ooni, 6 May 2020.

business, receive remittances, contact friends and relatives abroad, and provide aid to displaced people.[43] Arguably, it has put residents' lives at risk, by depriving them of information about the fighting and the COVID-19 pandemic. As one resident of rural Kyauktaw township observed:

> Before the shutdown, news [about the fighting] would pop up in a minute on the internet [Facebook]. That meant we had time to prepare to run or to hide or to store more essential items. … The internet ban has also affected our livelihoods. Many people were earning income from running internet shopping businesses [on Facebook] but now those are all gone.[44]

For the Tatmadaw, the trade-off for the drastic measures it applied to control the internet in Rakhine was also steep: the restrictions fuelled resentment of the government and armed forces, increased popular support for the Arakan Army among ethnic Rakhine, and further damaged the country's international image in the wake of the Rohingya crisis. The mobile internet blackout, in particular, has created so much anger that many sources argue it has been largely counterproductive. "It's like the Arakan Army doesn't need to send out propaganda anymore about how bad the government and military are – the internet ban is doing its job ," said a Rakhine activist, in comments echoed by other Rakhine-based sources.[45] After the ban, residents relied more on word of mouth for information, enabling the Arakan Army to control the narrative through its network of members and supporters.[46] Rakhine people living in areas where internet was not restricted became more engaged with the conflict, sharing information from Facebook with friends and relatives in northern Rakhine.[47]

[43] Crisis Group Report, *An Avoidable War: Politics and Armed Conflict in Myanmar's Rakhine State*, op. cit.

[44] Crisis Group interview, Kyauktaw resident, November 2020.

[45] Crisis Group interviews, Rakhine activist, Rakhine politician close to Arakan Army and senior official from a Rakhine political party, October 2020.

[46] Crisis Group interviews, Rakhine politician close to Arakan Army and Kyauktaw resident, November 2020.

[47] Crisis Group interviews, Rakhine activist and Rakhine politician close to Arakan Army, October 2020.

III. The Erosion of Data Privacy and Online Freedoms under the NLD

Alongside the responses to the Arakan Army insurgency, the NLD government oversaw a range of digital and security initiatives that began to undermine data privacy and digital rights for users across the country. In most cases, the government was responding to requests from the military or bureaucrats within the ministry of transport and communications, many of whom are ex-military officers trained in Russia, rather than driving the changes.[48] Although these initiatives – such as SIM card registration or cybersecurity laws – are common in other jurisdictions, in Myanmar they were poorly executed, without privacy or human rights safeguards. Nevertheless, the NLD was reluctant to oppose the military for political reasons. The ousted civilian government thus made the task of the post-coup military regime easier by setting in motion policies and laws that the latter could use for repressive purposes.

Online freedom of expression declined significantly under the NLD. Broadly worded defamation clauses in several laws were regularly used to jail activists and ordinary internet users alike for online comments, usually on Facebook. Although some of these, such as the 2013 Telecommunications Law, were enacted before it took office, the NLD oversaw the introduction of new legislation that was similarly open to abuse, such as the 2017 Law Protecting the Privacy and Security of Citizens, and made only minor amendments to address issues with older laws.[49] One survey by freedom of expression group Athan found that during the first four years of the NLD's term, more than 1,000 people had been prosecuted for social media posts under a range of laws. [50] More than half of the cases were initiated by the government itself, while others were based on complaints filed by the military, the NLD party and lawmakers.

During the NLD's tenure, many of the ministry of transport and communications' activities were cloaked in secrecy. In February 2018, the government allocated an emergency budget of almost $5 million to a mysterious Social Media Monitoring Team. An official later said its purpose was to prevent foreign interference rather than to monitor local users, but very little information on the team's activities has been released since then.[51] Similarly, it began work – largely behind closed doors – on a Cyber Security Law, aspects of which would eventually be included in amendments to the Electronic Transactions Law following the 1 February coup (see Section IV.A below).[52]

[48] Crisis Group interviews, digital rights advocate, March 2021.

[49] Amendments to the Telecommunications Law enacted in 2017 reduced the penalty for defamation from three to two years' imprisonment and made it more difficult for a third party to file a complaint. The full text of both laws in Myanmar and English is available on the Free Expression Myanmar website.

[50] "Analysis on Freedom of Expression Situation in Four Years under the Current Regime", Athan, 2 May 2020.

[51] "Social media team will not spy on netizens, official says", *Myanmar Times*, 23 May 2018.

[52] An initial version, written under a World Bank-supported program, was provided to stakeholders in early 2019 but later discarded after the World Bank ended the cooperation. In 2020, the ministry then began working on a new "zero draft" that formed the basis of the version released by the mili-

At the same time, the NLD government began to push for stronger lawful interception powers that would enable it to gain direct access to user data from mobile operators and internet service providers. In December 2020, mobile operator Telenor warned at a briefing in Yangon that without sufficient safeguards, the plan would create "an opportunity for misuse and breach of customers' human rights". The telecoms giant said it had so far been reviewing government requests for user data on a case-by-case basis, and had rejected some, but under the proposed regime the government would be able to collect the information directly.[53] Budget documents show that a lawful interception program was already well under way by the time of Telenor's disclosure, with the ministry of transport and communications receiving the equivalent of $4.6 million in early 2019 to carry out the initiative.[54]

The government also launched a SIM card registration program in 2020, enabling it to better track individuals' online conduct, despite warnings from some in the industry and digital rights proponents of the potential for abuse. The program required all users to re-register their SIM cards by uploading their national ID or passport, and limited users to a maximum of two cards. Although SIM registration was previously a requirement, it was common practice to purchase a card that had already been registered under another person's name. Mobile operators and digital rights advocacy groups warned there was a lack of clarity over how the information gathered from users would be stored and used, highlighted that many people in the country (such as the Rohingya) lack any ID, and questioned whether it was wise to chill access to information amid the COVID-19 pandemic and given the restrictions already created by the Rakhine internet shutdown.[55] The government ignored these reservations, and more than 34 million SIM cards were reportedly deactivated. "This was a massive surveillance operation, essentially, with no safeguards", said one source.[56]

Prior to being removed from office, the NLD government was also in the process of creating a biometrics database for telephone users, which would have included their fingerprints and a scan of their ID.[57] Another initiative would have created "e-IDs" – a system that is not controversial in principle, but under Myanmar's laws implied that the authorities, including the military, could have had access to personal data with few checks and balances.[58]

tary regime in February 2021. See "Myanmar's Legal Framework for Cybersecurity Needs to Be Built to International Standards", Myanmar Centre for Responsible Business, 12 February 2021.

[53] "Telenor Myanmar 7th Sustainability Briefing", Telenor Myanmar, 3 December 2020. For further discussion, see "Telenor says government is seeking direct access to customers' personal data", Myanmar Now, 12 December 2020.

[54] "The Rise of Online Censorship and Surveillance in Myanmar: A Quantitative and Qualitative Study", Open Technology Fund, November 2020.

[55] See, for example, "Millions in Myanmar risk having mobile phones cut off after SIM registration deadline", *Myanmar Times*, 29 April 2020.

[56] Crisis Group interview, digital rights advocate, March 2021. See also "Telenor Myanmar 7th Sustainability Briefing", op. cit.; and "Telecoms ministry says it has deactivated more than 34 million SIM cards", Myanmar Now, 27 October 2020.

[57] "Myanmar diverts special telecoms fund to biometrics database", *Myanmar Times*, 11 June 2020.

[58] "e-ID System Working Committee discusses finishing touches to contract with Austrian company", *Global New Light of Myanmar*, 2 November 2019; "Myanmar to receive Austrian loan for national e-ID system", *Myanmar Times*, 28 May 2020.

Further surveillance initiatives with potentially troubling repercussions were also planned or implemented through what were called "Safe City" projects. In the capital, Naypyitaw, a system of 335 Huawei surveillance cameras with facial recognition and licence plate identification technology went live in December 2020.[59] A similar project in Mandalay Region covering three townships was due to come online in mid-2021, with Yangon expected to follow later. The system is designed to automatically alert authorities when it detects individuals who are on a wanted list, among other applications.[60] In principle, these initiatives could have been of great benefit to Myanmar, harnessing technology to improve governance, administrative efficiency and security. But in the absence of legal safeguards protecting individual privacy and digital rights, they also risked providing the authorities – whether civilian or military – with the tools to monitor, censor and prosecute members of the public, including political opponents, at will.

Those who tried to raise concerns about data privacy and digital rights issues with the NLD government or party lawmakers saw their concerns brushed aside. Although many NLD officials had personally experienced abuses at the hands of the military during junta rule, they seemed indifferent to the possibility that their initiatives could be misused by civil servants or the security forces, including against themselves. Few if any foresaw a scenario in which the military came back to power through force. "When the coup happened, the NLD was a sitting duck because of these programs", said one digital rights advocate. "We had tried to draw their attention to the red flags, but it was like talking to a brick wall".[61] NLD lawmakers and government officials also failed to push back against the military's proposals to equip the police force with advanced surveillance and monitoring equipment that it is now likely to use against the opposition movement, if it is not already doing so (see Section IV.A below).[62]

[59] "Hundreds of Huawei CCTV cameras with facial recognition go live in Naypyitaw", Myanmar Now, 15 December 2020.
[60] "Myanmar: Facial Recognition System Threatens Rights", Human Rights Watch, 12 March 2021.
[61] Crisis Group interviews, January and March 2021.
[62] Crisis Group interviews, social media researchers and digital rights advocates, March 2021. See also "Myanmar's military deploys digital arsenal of repression in crackdown", *The New York Times*, 1 March 2021.

IV. The Post-coup Technology War

Since the first hours of the coup on 1 February, the Tatmadaw's actions have reflected a keen awareness of the importance of the internet, social media and communications technology for consolidating control. In an effort to gain the upper hand over its opponents, it has grappled with a range of approaches – from legal amendments and filtering websites to complete internet shutdowns. But given how connected Myanmar citizens have become, and how united they are in opposing military rule, the internet is a battlefield on which the Tatmadaw will struggle to win. It poses significant risks for the regime, for example by enabling the public to organise rallies and document abuses. As a result, the generals have turned to the bluntest of censorship instruments to stifle opposition – an approach it initially avoided due to the economic consequences, but also because it sought to project an image of business as usual to domestic and international audiences. At the time of writing, the country was in a near-total internet blackout, with online access limited to fibre optic connections where available.

A. *Targeted Measures Fail*

The difficulties the military would face in controlling online activity were apparent from the first hours of the coup. One of the junta's first actions after detaining members of the civilian government in the early hours of 1 February was to send soldiers into the offices of the mobile operators and internet service providers to force them to switch off all phone and internet connections, plunging the country into a communications blackout.[63] The blackout had the desired effect of stopping the flow of information about fast-unfolding events, but it also immediately highlighted constraints that the Tatmadaw had never faced in the past, including when it shut down the internet for weeks after the 2007 protests.[64] This time, the internet outage triggered chaos for businesses, forcing manufacturers to close their factories and shutting down the banking system entirely. By the early afternoon of 1 February, the military had no choice but to restore all internet access.

With the internet back on but people initially hesitant to venture into the streets, social media was the natural place for opposition to the coup to germinate. On 2 February, medical workers used Facebook to launch a civil disobedience movement, refusing to work for the regime and calling for the reinstatement of the democratically elected government.[65] The ministry of transport and communications – one of the few ministries in the military regime led by a serving officer, Admiral Tin Aung San – responded by ordering mobile operators and service providers to block access to social media platforms, beginning with Facebook on 3 February and followed by Twitter and Instagram two days later. As the first street protests against the regime gath-

[63] "A digital firewall in Myanmar, built with guns and wire cutters", *The New York Times*, 23 February 2021.

[64] "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma", OpenNet Initiative, 29 September 2007.

[65] "After coup, medical workers spearhead civil disobedience campaign", *Frontier Myanmar*, 2 February 2021.

ered steam on 6 February, the ministry shut down the internet for more than 24 hours to thwart online coordination, before reinstating access on the afternoon of Sunday 7 February, prior to the start of the working week.[66]

The availability of free VPNs in Myanmar meant the regime's orders to filter websites and block access to social media platforms only had limited effect.[67] The ministry has since been ordering mobile operators and service providers to restrict access to thousands of internet protocol (IP) addresses used by VPNs, as well as sites from where VPNs can be downloaded, but this task has proven impossible: although it provides them with long lists of IP addresses for filtering almost every day, the sheer number of VPNs available means that free versions are easily accessible and widely used.[68] Social media monitoring continues to show elevated levels of engagement with content from news organisations, suggesting that most users are having little trouble circumventing the controls in order to view Facebook.[69] (At the same time, free VPNs and censorship circumvention apps often come at the cost of speed and/ or security, and are usually not suitable for those at high risk of surveillance.)

The military's next tactic was to enact legal changes to restrict freedom of expression and gain access to user data. Its very first public act of law-making after taking power was to distribute a draft Cyber Security Law – based on the NLD government's version – to mobile operators and internet service providers on 9 February. The law would have required tech companies to onshore their data and provide it to the government at any time on vague national security grounds; it also introduced new categories of offence for spreading "misinformation" or "disinformation" that could result in a three-year prison sentence.[70] The draft provoked strong public opposition from activists and businesses, and behind the scenes even some bureaucrats within

[66] See "Directive to temporarily block social media service Facebook", 4 February 2021; "Directive to block social media services Twitter and Instagram, until further notice", 5 February 2021; and "Directive to temporarily shut down data network", 6 February 2021. All are available at "Directives from authorities in Myanmar – February-April 2021" on the Telenor website.

[67] Data from one source showed a massive 7,200 per cent increase in VPN demand in Myanmar on 4 February, the day that restrictions on Facebook access were put into effect. Similarly, the censorship-bypassing application Psiphon experienced a huge rise in users after the coup and has been among the most downloaded applications since then. See "VPN demand surges around the world", Top10VPN, 4 February 2021; "The battle for Myanmar plays out on Twitter, TikTok and Telegram", Deutsche Welle, 20 April 2021.

[68] The Telenor website referenced in fn 65 contains a list of directives from the ministry of transport and communications to mobile operators and internet service providers up to 14 February, when Telenor said it could no longer publicise the directives, apparently due to threats from the authorities. Those identified as "Directive to temporarily (but open ended) block IP addresses" reflect efforts to stop VPN use. The ministry has continued to issue directives to block VPN IP addresses since 14 February. Crisis Group interviews, March 2021.

[69] Social media monitoring shows the top news story each day on Facebook in January 2021 typically had from 50,000 to 80,000 interactions. In February, this total reached around 300,000 to 400,000 interactions.

[70] Onshoring data refers to keeping it in locally based data centres. This change would be significant in Myanmar because it would mean the authorities could gain access to data more easily than if it is kept abroad. "Civil society, businesses condemn junta's draft Cyber Security Law", *Frontier Myanmar*, 11 February 2021. See also "Telenor Group's response to proposed Myanmar Cyber Security Bill", Telenor, 15 February 2021.

the ministry of transport and communications urged a more moderate approach.[71] The regime quietly shelved the draft and instead enacted amendments to the Electronic Transactions Law on 15 February. These included some sections of the draft Cyber Security Law but minus the requirement to store data inside the country.[72]

Around the same time, the regime also pursued legal changes that seemed designed to deter online criticism. On 14 February, it announced amendments to the colonial-era Penal Code and Code of Criminal Procedure, including the addition of a new charge, commonly known as Article 505-A, that carries a three-year prison term for "causing fear", "spreading false news" or "agitating directly or indirectly" to commit a criminal offence against a government employee.[73] The regime has since used this law extensively against a wide range of opponents, including journalists, politicians, activists, striking doctors and social media users (see Section IV.B below).

Additionally, from the early hours of 15 February, the military began instituting a nightly internet shutdown that has continued ever since. Initially enforced from 1am to 9am, the blackout was later relaxed to 1am to 6:30am on weekdays, following lobbying by businesspeople.[74] There has been significant speculation as to why the military chose to cut the internet at night, when most internet users are asleep. It seems to have been driven by two factors. The first is that shutting down the internet at night has less impact on the economy and government operations. The second is that it stopped livestreams of night-time raids by security forces, which had caused public outrage and even hindered police operations as in some cases members of the public had rallied to the support of those being arrested, forcing the outnumbered police to back off.[75]

B. *Falling Back on Blunt Tools*

In spite of these somewhat flailing efforts to curtail online activity, social media continued to play an important role in building opposition to the regime. It helped sustain the civil disobedience movement by enabling it to foster solidarity and mobilise public support for striking workers, while activists used Facebook and other platforms to organise themed protests, such as the "22222 uprising" on 22 February that saw millions march across the country. As security forces began to employ lethal force more readily from late February, social media platforms also became important for documenting violence against protesters. Soon, livestreams, videos and photos of the dead and wounded began to flood social media, along with footage of security forces

[71] Crisis Group interview, digital rights advocate, March 2021.

[72] Crisis Group interviews, Yangon-based businesspeople, February and March 2021. This requirement would have been unworkable for companies and, most likely, unenforceable for the regime. It may, however, have resulted in some technology companies – such as cloud storage providers – no longer offering services in Myanmar. For analysis and a translation of the amendments, see the Free Expression Myanmar website.

[73] "State Administration Council Law No (5/2021), Law Amending the Penal Code" and "State Administration Council Law No (6/2021), Law Amending the Code of Criminal Procedure". English versions are available in the 15 February 2021 issue of the *Global New Light of Myanmar*.

[74] For full details, see the NetBlocks website or Twitter feed. After more than 70 nights, these restrictions were lifted from 28 April.

[75] Crisis Group interviews, March 2021. See also Crisis Group Briefing, *The Cost of the Coup: Myanmar Edges Toward State Collapse*, op. cit.

committing a range of abuses against unarmed civilians. Not only did this footage provide evidence of what was happening on the ground, but it also strengthened domestic and international opinion against the military regime.[76]

Recognising it was losing the online battle, the military on 15 March ordered the total shutdown of mobile internet services, which constitute the main source of access to the web for the vast majority of users in Myanmar. Two days later it shut down public wi-fi services, and from 2 April instructed mobile operators and internet service providers to also halt fixed wireless services, which many urban households use for home connections. Only the much less common fibre-to-the-home connections remained operational, leaving rural areas completely disconnected.[77] In urban areas, service providers have been inundated with applications for fibre connections, and are unable to meet demand. In the meantime, many residents are sharing connections with neighbours who have fibre to get around the blackout. But by one estimate, there are likely just 600,000 active internet connections left in the country – barely one for every 100 people – down from close to 25 million prior to the mobile data shutdown.[78]

A factor that may have influenced the military's thinking in taking this draconian step is its forces' morale. The majority of military personnel and their families live in cantonments, and anecdotal evidence suggests that many have not been allowed off base since the last week of January. Some sources indicate that a desire to stop information about events unfolding across the country from reaching rank-and-file soldiers played a role in the Tatmadaw's decision to shut down mobile internet.[79] They now have little choice but to rely on state media for information, with the 8pm nightly news often compulsory viewing.[80]

The mobile, public wi-fi and fixed wireless internet shutdowns have had a discernible impact on the opposition movement. The organisational networks of the civil disobedience and protest movements have been significantly affected. "The impact of losing most communication channels has been very noticeable. Two weeks after losing fixed wireless access, there are some people who are still completely offline", commented one civil society leader.[81] The volume of user-generated content on social media about what is happening inside the country has also diminished significantly. In some regional cities, protests stopped almost immediately because activists were unable to organise; coordination in rural areas, which have been almost entirely cut off, has been even more affected. Underscoring how limited con-

[76] The Independent Investigative Mechanism for Myanmar, which was established by the UN Human Rights Council to gather and store evidence of Tatmadaw abuses against minorities, has been looking into possible crimes against humanity by the military since the coup. See "Human Rights Council reiterates urgent need to ensure accountability in Myanmar", Independent Investigative Mechanism for Myanmar, 24 March 2021.

[77] See, for example, "'Any news from the internet?': Fear and rumour in villages forced offline", *Frontier Myanmar*, 10 April 2021.

[78] "Myanmar shutdown of wireless internet fuels fears of news blackout", *Nikkei Asia*, 2 April 2021; and "Digital 2021: Myanmar", op. cit.

[79] "Inside Myanmar's army: 'They see protesters as criminals'", *The New York Times*, 28 March 2021.

[80] Crisis Group interviews, social media and digital security researchers, March 2021.

[81] Crisis Group interview, civil society leader, April 2021.

nectivity is, large protests took place in several towns in Mandalay and Sagaing regions on 24 March, with demonstrators apparently unaware that activists had declared a "silent strike" urging the public to stay indoors that day.[82]

The regime's phased shutdown of the internet has been complemented by some even cruder methods to restrict information flows, internet access and social media use. Since late February, numerous reports have emerged of security forces stopping and searching civilians' mobile devices, looking for social media content or VPNs, in what seems to be an attempt to scare people off the platforms.[83] When security forces enter an area, they now routinely disable or destroy privately owned CCTV cameras, which have been a source of evidence of regime abuses, often shared on social media. Before launching a violent crackdown in Yangon's South Dagon in late March, security forces even disabled all internet services in the township.[84] More recently, in rural areas, local administrators have ordered residents to take down satellite dishes from a Thai company, PSI, that broadcasts banned media outlets Mizzima and DVB.[85]

Since early March, the military has also ramped up arrests of regime opponents with a high-profile social media presence for spreading "fake news" and "threaten[ing] the public on the social media". The new Penal Code provision, Article 505-A, has been used widely to charge high-profile opponents of the coup, as well as at least ten journalists detained while covering street protests. For most of April, the military announced charges under this article against twenty people each day on national television. The link between the charge and their online activity was made explicit in the televised public announcements, which included their name, home address and Facebook URL.[86] The list includes not only celebrities, activists and journalists, but also seemingly ordinary social media users. This tactic seemed designed to instil fear, so that people would not criticise the military or support the opposition movement on social media. Many of those listed have since been arrested and are facing three years in prison.

Since the coup, the regime has used the police force's social media monitoring team to track celebrities and social influencers who were posting anti-military statements on social media. At the end of March, shortly before the 505-A charges were announced, the team received instructions to begin finding the addresses of targeted social media users. One officer said the team had no technology to match Facebook users with physical addresses and relied instead on informants (known as *dalan* in Burmese) and data from the General Administration Department. Regarding the charges against ordinary users, the team member explained that some of those fac-

[82] Crisis Group interviews, journalist and social media researcher, March 2021. See, for example, Facebook posts on protests in the towns of Kume, Wuntho and Katha on 24 March 2021.

[83] See, for example, "Police search phone records of detainees in Myitkyina", Radio Free Asia, 9 March 2021 (Burmese); and "In Mandalay city, security forces inspect motorcycles and cars", Mizzima, 5 April 2021 (Burmese).

[84] Crisis Group interview, journalist who covered the crackdown, April 2021. The same tactic was reportedly used in the town of Kalay in Sagaing Region in early April.

[85] The Myanmar military banned five media outlets on 8 March: 7Day, Myanmar Now, Khit Thit Media, Mizzima and DVB. See also "Myanmar junta limits internet, seized satellite dishes", The Associated Press, 9 April 2021.

[86] The nightly announcements commenced on 2 April and stopped from 24 April.

ing charges had been active in private Facebook groups, unaware that informers had infiltrated them and were reporting back to the police.[87]

These blunt tactics reflect the lack of other options that the military has to respond to such widespread opposition. Although it has acquired a range of tools to disrupt communications, monitor individuals and unlock devices (discussed in further detail in Section V.A), these are largely ineffective in the face of a mass uprising, particularly given the lack of capacity in the security forces to deploy them at scale.

Although the internet shutdown has also had a significant impact on businesses and government operations, these are no longer major considerations for the Tatmadaw. The escalating protests and the existential threat they pose to military rule mean that security imperatives – the need to consolidate power and crush all opposition – are now the dominating factor in decision-making in Naypyitaw. Asked about the internet shutdown at a 23 March press conference, Deputy Information Minister Brigadier-General Zaw Min Tun replied that the military had "no plan" to restore internet services:

> The most fundamental and important task in a country is maintaining the rule of law and stability. Without the rule of law and stability, other activities cannot function. We have found that most of the incitement for the ongoing riots comes from the internet and social media. We will continue to put the restrictions in place for a certain period of time.

Driven by this logic, the military will likely prolong the mobile internet outage if opposition to its rule continues – as was the case in Rakhine – or even go further and shut down the last remaining fibre connections. "The reason we're winning is because we're still online", confided a civil society source active on digital rights issues. "But the Tatmadaw controls the kill switch and might use it – even though the collateral damage, economically, will be huge".[88]

C. *Propaganda Fail on Social Media*

The Tatmadaw's difficulties have not been limited to controlling the online space and undermining the ability of its opponents to organise and challenge its authority. It has also lost control of the narrative about what is happening in Myanmar, to the point that it has struggled to even disseminate messages to its own supporters through major social media platforms. In contrast, anti-military activists have used social media highly effectively to reach domestic and international audiences with key messages and campaigns, as well as to raise funds for striking workers and the Committee Representing Pyidaungsu Hluttaw (CRPH), a group of parliamentarians elected in November 2020 who have formed a shadow government in the absence of the deposed NLD leadership.

Facebook's decision to completely remove the Tatmadaw from its platform shortly after the coup was a major blow to the military leadership. Following the brutal campaign against the Rohingya in 2017, the company had banned Myanmar's commander-in-chief, Senior General Min Aung Hlaing, and removed twenty military-

[87] Crisis Group interview, social media monitoring team member, April 2021.
[88] Crisis Group interview, civil society member, March 2021.

linked pages, but it had refrained from banning the Tatmadaw entirely. Over the following two years, it also removed at least six military-run networks that had been engaging in "coordinated inauthentic behaviour".[89] The military responded by setting up a page for its "True News Information Team", which gradually rebuilt the following that had been lost when Min Aung Hlaing's page was removed in 2018.[90] On 24 February, however, Facebook announced it was officially banning the Tatmadaw from Facebook and Instagram, and removing military-controlled media accounts such as Myawady and MRTV, with immediate effect.[91] On 14 April, it announced that it would also remove "praise, support and advocacy" of violence by either the security forces or protesters in the future.[92]

This decision to ban the Tatmadaw has had implications for pro-military accounts, known in Myanmar as "lobby" pages, that often propagate pro-military disinformation. Civil society groups monitoring such content report that since the coup, Facebook has been very responsive in taking action, in part because the new policy makes decisions on removal much more straightforward.[93] Facebook's efforts over the past several years to identify and remove military proxies pushing disinformation or engaging in coordinated inauthentic behaviour have also significantly diminished the Tatmadaw's ability to reach mass audiences.[94] Although Facebook's ability to detect recidivism could be improved, these accounts now struggle to build a following when they try to re-establish themselves; pages that once had millions of followers now often attract a maximum of 1,000 before they are removed.[95]

Despite the restricted operating space, the military has still been able to propagate disinformation campaigns, using a combination of social and state-controlled media. One prominent example was a campaign in early March that aimed to shift the blame for protester deaths away from security forces. Social media accounts posted the more extreme claims, such as assertions of the involvement of a non-state armed group, while concurrent articles in state media exonerated the security forces and said further investigation was ongoing.[96] Amid the internet blackout and the Facebook ban, the military has also resorted to distributing pamphlets laying out its justification for seizing power.[97]

[89] Facebook defines coordinated inauthentic behaviour as "when groups of pages or people work together to mislead others about who they are or what they are doing".

[90] "Tatmadaw returns to Facebook after two-year absence", *Myanmar Times*, 9 June 2020.

[91] The ban applies to accounts that are representing the Tatmadaw – either institutional pages, or individual users who are using their accounts to post information about the Tatmadaw. Individual soldiers using Facebook for personal purposes are not automatically removed. See also "Myanmar military banned from Facebook and Instagram with immediate effect", op. cit.

[92] Ibid.

[93] Crisis Group interview, social media researcher, March 2021.

[94] Although networks engaging in coordinated inauthentic behaviour often spread disinformation, Facebook removes them because of their behaviour – for example, misleading users on their identity or location – rather than the content they are posting.

[95] Crisis Group interview, civil society member, March 2021.

[96] "Disinformation campaign tries – and fails – to shift blame for protester deaths", *Frontier Myanmar*, 7 March 2021.

[97] See tweet by Athens Zaw Zaw, Deutsche Presse-Agentur journalist, @zawathens, 6:43pm, 14 April 2021.

It is not entirely clear who the military is trying to reach with such propaganda campaigns. Some sources suggested the main target may be its own base – military personnel and their families, supporters of the military-affiliated Union Solidarity and Development Party, nationalist groups and civil servants – rather than the broader public, particularly as attitudes harden against the military and opportunities to convince a wider audience diminish.[98] Growing concerns over troop morale may make it imperative that pro-military messaging continue to reach the rank and file.

Regardless, the Facebook account removals appear to be a major source of frustration for the Tatmadaw, which seems eager to reach an audience beyond its – relatively small – base. When Deputy Minister for Information Brigadier-General Zaw Min Tun hosted the military regime's second press conference since the coup on 11 March, numerous new Facebook pages were set up in order to livestream the event. Anti-military internet users were, however, prepared for this possibility, and coordinated in order to detect and report these pages to Facebook as the press conference was taking place so they could be removed immediately.[99] "The military keeps trying to set up new accounts and new pages – it hasn't given up on Facebook. It just goes to show how significant it is to their communications operation", commented one civil society source.[100] The military and pro-military groups often refer conspiratorially to the "Myanmar Facebook Team". This term reflects an apparent misconception that a large number of Facebook employees is in-country working to undermine the Tatmadaw's activities in collaboration with the NLD.[101]

The coup has undoubtedly forced Facebook to take a clear political position and choose between the military and its opponents. This progression began with the Rohingya crisis in 2017, after which Facebook received a barrage of criticism for its failure to police hate speech against the Muslim minority.[102] It has since made significant changes in the way it monitors and addresses risks relating to the use of its platform, not only removing military accounts but also developing closer relationships with civil society groups and vastly increasing its capacity to monitor Myanmar-language content. Since the coup, the company has not only further limited the Tatmadaw's ability to use its platform, but it has also verified the pages of the civil dis-

[98] Crisis Group interviews, civil society member and social media researcher, March 2021.

[99] Crisis Group interview, civil society member, March 2021. URLs of some of the removed pages are on file with Crisis Group.

[100] Crisis Group interview, civil society member, March 2021.

[101] At the 23 March press conference, a journalist from a pro-military media organisation, the Myanmar National Post, asked Zaw Min Tun about the "Myanmar Facebook Team", complaining that it was "supporting media that are publishing content inciting the riots, but at the same time our pages and government pages are at risk of being removed". Zaw Min Tun replied that the regime was "conducting a detailed examination", and that it plans to take unspecified legal action to address the issue. Also see, for example, "Facebook's been obviously interfering in Myanmar's election", Radio Free Myanmar, 24 October 2020. Radio Free Myanmar is a Wordpress blog that spreads pro-military and anti-NLD disinformation by encouraging supporters in its network to screenshot and share articles on Facebook in order to get around moderation efforts. See "Radio Free Myanmar: Disinformation network spread false news and hate speech", *Frontier Myanmar*, 9 October 2020, for more background.

[102] "How Facebook's rise fueled chaos and confusion in Myanmar", op. cit.

obedience movement and the CRPH. Interestingly, it even quickly gave the CRPH a blue tick to verify its identity and described it as a "government organisation".

The Tatmadaw's experience across other social media platforms has been mixed. As it became harder for the military and their proxies to maintain a presence on Facebook, they increasingly began using YouTube to host videos that could then be shared by users on the more popular platform.[103] The video hosting platform has far less capacity to monitor Myanmar-language content than Facebook, and in the past has been slower to act on dangerous content, such as disinformation.[104] But it is increasingly mirroring Facebook's policies in terms of account removal, and since 1 February has banned five accounts linked to the military, including those of TV channels MRTV and Myawady, as well as some accounts that push pro-military propaganda.[105] YouTube's parent company, Google, has also disabled some military accounts on Gmail, the Play Store and Blogger, including a mirror site for the Tatmadaw Information Team.[106]

TikTok was initially slower to act, with some warning that Tatmadaw soldiers' use of the service, and the platform's inadequate response, had echoes of Facebook's missteps prior to the wake-up call created by the Rohingya crisis. Of particular concern were videos from ordinary soldiers brandishing their weapons and threatening protesters, some of which had been viewed millions of times.[107] Misinformation and military propaganda were also prevalent; as with YouTube, the increased use of the video clip sharing platform by military personnel and supporters seems to have been partly driven by stricter moderation on Facebook. But in contrast to the Russian platform VK, which also has a heavy Tatmadaw presence but is otherwise not popular in Myanmar, TikTok has millions of ordinary Myanmar users. Many of them took to TikTok in the wake of the coup to express their support for protests and their anger at the military, and like Facebook and other platforms it saw a significant spike in engagement until the mobile data shutdown.[108]

After the videos of soldiers threatening protesters came to light, TikTok took steps to clean up its platform, issuing new guidance to its content moderators. It has also expanded partnerships with local organisations to improve its understanding of Myanmar. It has, however, stopped short of banning the Tatmadaw; company representatives say they instead review content on a case-by-case basis, and point out the Tatmadaw does not have an official presence on TikTok.[109] Some social media researchers have expressed concern at this policy on the basis that individual soldiers posting videos may be doing so with the endorsement of superiors or even as part of a coordinated campaign. Since the Rohingya crisis, the Tatmadaw has in-

[103] One prominent example was a video from an account named MMLeak that accused the NLD government of being beholden to foreign interests. The video surfaced shortly before the 2020 election and continues to reappear periodically on YouTube.

[104] Crisis Group interviews, social media researchers, November 2020 and March 2021.

[105] "YouTube bans Myanmar military channels as violence rises", *The New York Times*, 5 March 2021. In mid-April, YouTube removed Myanmar-American News, a pro-military disinformation account that had tens of thousands of followers.

[106] The page is no longer accessible.

[107] "TikTok on alert after it becomes outlet for Myanmar soldiers", *Financial Times*, 4 March 2021.

[108] Crisis Group interview, TikTok representative, May 2021.

[109] Crisis Group interview, TikTok representative, May 2021.

troduced stricter controls on what its personnel can say and do on social media; soldiers are unlikely to post videos of themselves with their weapons without permission.[110] TikTok says it has been "aggressively" looking for signs of coordination but has thus far detected it on only a limited scale.[111]

As with other platforms, TikTok has seen user behaviour adapt in response to stricter enforcement. Threats of violence and misinformation have become subtler; instead of threatening a protester with a gun, a user might make a shooting motion with their fingers or, for example, a veiled threat in the form of a warning.[112] For all platforms, this adaptive behaviour underscores the importance of constant monitoring, hiring adequate numbers of native speakers as moderators and building partnerships with local organisations.

At the same time as social media platforms have diminished the military's ability to communicate, its opponents have ramped up campaigns against the regime. While Facebook remains popular, particularly for sharing information in Myanmar language with other users inside the country and with the large diaspora, many political figures and ordinary social media users have adopted new platforms in order to reach new audiences. Twitter, in particular, has witnessed an explosion of users from Myanmar since 1 February, in part because it is widely perceived as the most effective platform for sharing information – particularly military abuses – with the outside world.[113]

D. *A Strategic Dilemma*

Although the military's immediate focus is on consolidating control over the country, and it appears willing to take whatever steps are necessary to do so, the online space does present it with a longer-term problem. Maintaining an internet blackout for an extended period of time will not only impede a well-functioning economy and society, and isolate Myanmar from the rest of the world, but also impair government operations, and prevent the military from communicating with its supporters through social media. It will also damage its standing domestically and internationally, undermining further its narrative that opposition to military rule is less significant than it appears. Yet any relaxation of internet restrictions is likely to reinvigorate protests, enabling activists to once again mobilise more readily.

Controlling the internet at a national scale was a challenge for which the Tatmadaw was largely unprepared. It did not expect to face such wide-scale or sustained opposition to its power grab. It has quickly realised that it is not set up to win the fight

[110] Crisis Group interviews, social media and conflict researchers, March 2021.

[111] Crisis Group interview, TikTok representative, May 2021.

[112] Another subtle example of misinformation is the use of the gold emoji to push the narrative that the NLD leadership is corrupt, as the Tatmadaw has alleged that Aung San Suu Kyi received gold as a bribe. Crisis Group interview, TikTok representative, May 2021.

[113] Analysis of popular coup-related hashtags in early February found almost half of users had set up their accounts in 2021, while Statista recorded a six-fold increase in Twitter users in Myanmar from December 2020 to March 2021. Many Myanmar Twitter users new to the platform simply retweet posts with long lists of hashtags in an effort to bring it to the attention of international organisations, journalists and high-profile individuals. For further discussion on Twitter uptake, see "Twitter and SMS: Myanmar's new frontiers of fear", *Frontier Myanmar*, 24 February 2021; and "The battle for Myanmar plays out on Twitter, TikTok and Telegram", op. cit.

for control of the online space, given that it faces overwhelming domestic and international opposition and has essentially been banned from the most influential social media platforms. It has neither the financial nor the human resources to replicate the model of China's "great firewall", which requires not only restricting access to the global internet but also developing an ecosystem of local applications and actively censoring local content.[114] Although on paper the military has many officers with degrees or other training in information technology, few have much proficiency. "In terms of technical skill, the military is behind the protesters and general public. Civilians have more technical know-how. … As a result, the military's response has been reactive rather than proactive", commented a social media researcher.[115]

There are few avenues to rectify this capacity shortfall in the short to medium term. Even if the military could get foreign assistance to pursue a more sophisticated approach, finding the staff to make it work would be a major challenge. Given the widespread anger at the military and the social pressure not to collaborate with the regime, recruiting from the private sector would be extremely difficult. A lack of centralised databases for even basic information, such as identity card details, mean possibilities for applying artificial intelligence will also be limited.[116]

Instead, the regime appears to have settled on an old solution: an intranet.[117] From mid-April, at the military's direction, mobile operators began "whitelisting" certain applications so they could be opened using mobile data despite the shutdown. This practice started with account services for mobile users and mobile banking applications, but it went on to include productivity services such as Microsoft's Office 365. Big businesses are expecting that they will soon be able to secure dedicated internet connections, known as dedicated internet access (DIA), on the condition that these connections are not used for political activities that undermine the regime.[118] Multiple sources said whitelisting was not likely to be a short-term measure, after which regular mobile internet would be switched back on; instead, the regime considers it a potential long-term solution. Some sources anticipate that, once it has completed its plan, the military may even limit fibre-based connections to whitelisted applications only.[119]

This whitelisting approach might seem to offer control over the internet without disrupting (at least entirely) essential business services, but it is unlikely to be the panacea the Tatmadaw is hoping for. Technically it will present challenges, particularly as many applications use dynamic IP addresses that by nature change frequently.[120] Myanmar's tech-savvy youth are also likely to find loopholes through whitelist-

[114] One source has estimated that the Chinese government spends at least $6.6 billion per year on internet censorship, employing huge numbers of human moderators. "Buying Silence: The Price of Internet Censorship in China", The Jamestown Foundation, 12 January 2021.

[115] Crisis Group interview, social media researcher, March 2021.

[116] Crisis Group interviews, industry sources and social media researchers, March 2021.

[117] Shortly after the former military regime permitted the country's first internet connections in the late 1990s, it began work on an intranet that was pejoratively called the "Myanmar Wide Web". The initiative was relatively unsuccessful, hosting just a small number of sites mainly for administrative purposes.

[118] Crisis Group interviews, businesspeople from the banking and technology sectors, April 2021.

[119] Ibid.

[120] Telenor has already pointed to some of the technical challenges to whitelisting, including that to function properly, a whitelisted service will often require multiple other services that will need to be

ed applications, particularly cloud services, that will give them access to the wider internet, and restrictions on how DIA is used can easily be circumvented through VPNs. Already, instructional videos are widely available online explaining how to regain mobile internet access using certain applications and VPNs.[121] One local information technology expert said: "Burmese people are very good at bypassing a lot of controls. We're born in a system where everything has been blocked. Give us an inch of freedom, we'll take ten inches".[122]

In the long term, the economic cost of such a "walled garden" would be massive. Restricting the online sphere to a locally managed intranet would stifle innovation and entrepreneurship, decimating Myanmar's growing e-commerce sector and promising start-up scene. The effects will be felt far beyond the technology sector, however, because many ordinary businesses, particularly small and medium-sized enterprises, are unlikely to have access to a DIA service. They will be reliant on a small number of whitelisted applications, and not the full suite of services they have come to use in their economic activity. If Myanmar develops an intranet, it will not resemble the internet, because it will not have social media or popular instant messaging services, for example – unlike in China, which had the resources to develop homegrown versions.[123] The plan might also wipe out billions of dollars in investment, including in operator licences, cell towers and international gateways.[124]

Experience from elsewhere suggests the regime is likely to face significant challenges implementing its intranet model. Countries like Iran and Russia have spent years trying to retrofit an intranet onto existing architecture without success, in part because users have resisted and found workarounds.[125] North Korea and Cuba have been more successful, partly because the population has never experienced political freedom. China's model, while effective, carries a financial burden that Myanmar simply cannot afford, and has developed in a similarly closed political culture. The military is likely to encounter significant pushback in Myanmar, given the telecommunications liberalisation of the past decade. "The internet is part of our lifestyle now. … This is trying to take us back to the Stone Age. It might have worked twenty years ago, or even ten years ago, but I don't think people will accept these restrictions", said one information technology expert.[126]

whitelisted, too. It also warned that whitelisting could increase the risk of cyberattacks. See "The case for open internet in Myanmar", Telenor Myanmar, 11 May 2021.

[121] To prevent these loopholes from being closed, Crisis Group has decided not to disclose further details about how the restrictions are being circumvented.

[122] Crisis Group interview, Myanmar-based IT expert, April 2021.

[123] Crisis Group interviews, IT expert and businesspeople, April 2021.

[124] In its first-quarter earnings for 2021, Telenor announced a 6.5 billion krone ($780 million) write-down of its Myanmar business, valuing it at zero. The business is heavily reliant on revenue from mobile data, and the write-down suggests the company sees little prospect of the restrictions being lifted in the near future. See "Telenor Group's results for the 1st quarter 2021", Telenor, 4 May 2021.

[125] See, for example, "How Russia is stepping up its campaign to control the internet", *Time*, 1 April 2021; "How the Iranian government shut off the internet", *Wired*, 17 November 2019; and "Oracle: China's internet is designed more like an intranet", ZDNet, 23 July 2019.

[126] Crisis Group interview, IT expert, April 2021.

V. What Role for International Actors?

The trajectory of the technological battle inside Myanmar will largely be determined by the decisions of the military regime. Influencing its policies is difficult, particularly as for now its sole focus is accomplishing near-term security objectives. Yet there are a number of steps international actors can take to minimise the risk of harm to internet users in Myanmar, and to limit the ability of the regime to use technology against its opponents or to build its capacity to control the online space.

A. *Restricting the Military's "Digital Toolkit for Repression"*

Budget documents show that under the NLD government, the civilian-led ministry of transport and communications and military-controlled ministry of home affairs acquired or attempted to acquire various equipment and software from companies from a range of countries, including the U.S., Canada, Sweden and Israel. In some cases, such as sales to the police force, these transactions may have violated existing arms embargoes.[127] The equipment and software in question have a range of uses, including retrieving data from phones and computers, tracking users and listening in on telephone conversations.[128] Since 1 February, these are now all in the hands of the military.

Such tools can easily be deployed against activists, political opponents and journalists – and already have been. In the most prominent example, technology from the Israeli firm Cellebrite was used to retrieve data from the phones of two Reuters reporters who were arrested in December 2017 in what many observers believe was a setup, after they uncovered evidence of a military massacre of Rohingya in Rakhine State.[129] It is unclear whether police are continuing to use Cellebrite.[130] They have, however, acquired other, similar tools since 2017.[131] As the trials of the thousands who have been arrested since the coup proceed, the use of such software to retrieve data from encrypted devices is likely to increase. One human rights lawyer representing several detainees said it was now routine for police to confiscate devices from

[127] "Myanmar's military deploys digital arsenal of repression in crackdown", op. cit.

[128] For a full list of technologies, see "Tools of Digital Repression", Justice for Myanmar, 2 March 2021.

[129] "Security-tech companies once flocked to Myanmar. One firm's tools were used against two journalists", *The Washington Post*, 4 May 2019. Both journalists were eventually released, after spending more than 500 days in prison.

[130] Cellebrite has declined to comment on whether its products are still being used in Myanmar, but its local distributor has said the company halted new sales in 2020 and stopped servicing equipment it had already sold. See "Myanmar's military deploys digital arsenal of repression in crackdown", op. cit.

[131] See "Tools of Digital Repression", op. cit. A company named Oxygen Forensics that produces similar software to Cellebrite has confirmed licencing its product for use in Myanmar in January 2019, likely to the ministry of home affairs. It has declined to identify whether the end user of its product is from the government or private sector. It insists that when it is made aware that its products are being used "in a way that does not conform to [its end user license agreement], international law or Oxygen Forensics ideals, these licenses are noted, as are the end users, and they cannot be renewed". The company declined to comment on whether it had done so in Myanmar. See "Filling a gap", Mike Lewis Research (blog), 25 April 2021.

prisoners and search their social media profiles in order to identify other activists and issue warrants for their arrest. As this lawyer noted: "In some cases, detainees' messaging applications have been active after they've been arrested because the police are carrying out investigations on their phone".[132]

The most effective means of restricting further access to such tools is to include them in an arms embargo covering all branches of the Myanmar government while it is under military control. Given that a UN arms embargo is unlikely due to a lack of consensus in the Security Council, like-minded countries should introduce or broaden bilateral embargoes to cover such sales, and agree on a common list of prohibited items. Beyond military equipment, they should ensure that such embargoes cover "dual-use" items – those that can have civilian or military applications, including for law enforcement – particularly digital tools that could be used for surveillance, data retrieval and other acts of repression targeting the opposition. They should also strengthen enforcement by better policing the sale of such technologies through middlemen, a modus operandi which is often used to avoid sanctions, scrutiny or due diligence requirements, and has been common practice in Myanmar in the past.[133]

Considering some of the technologies that the military has already acquired require regular licensing and software updates or maintenance, the relevant companies should cease providing this support in order to undermine the effectiveness of their products at the hands of the military regime. Meanwhile, outside actors should immediately suspend any technical cooperation with nominally civilian branches of the government on cybersecurity or related issues.

B. *Keeping Myanmar's Internet Open and Its Users Safe*

Foreign governments and technology companies have a responsibility to do what they can to ensure the internet is as widely available as possible, information is accessible and users are safe. To begin with, they should consistently prioritise the issue in their public statements about the situation in Myanmar, condemning the regime for its digital repression, emphasising that internet access is an economic and humanitarian necessity, and calling for full restoration of connectivity.

As long as the Tatmadaw keeps the internet on to some degree, there are also several other steps governments and companies can take. Filtering restrictions put in place by the regime mean VPNs are an essential tool for finding and sharing information on events inside the country. The military is taking steps to restrict access to free VPNs, which are also less secure than paid options. For most internet users in Myanmar, however, paid VPNs are unaffordable or simply inaccessible because they need to be purchased online, and credit cards are uncommon. Making secure VPNs available to all users is not feasible, but VPN providers should follow the lead of companies like NordVPN, which have set up programs to provide emergency access to high-risk individuals.[134] Governments and civil society outside Myanmar should push to get as many users as possible in Myanmar access to secure VPNs through

[132] Crisis Group interview, human rights lawyer, April 2021.
[133] See "Myanmar's military deploys digital arsenal of repression in crackdown", op. cit., for further discussions of the use of resellers and apparent violations of sanctions.
[134] See, for example, "Emergency VPN and the situation in Myanmar", NordVPN, n.d.

these programs, by drawing attention to them, helping those eligible apply, and suggesting potential candidates to VPN providers.

Several tech companies are already taking steps to better protect users against potential reprisals for their online activities. Facebook has launched a safety feature enabling users to quickly and easily lock their profiles, which applies additional security settings that restricts visibility to non-friends.[135] Such measures are welcome, and other social media, messaging and email providers – particularly those that are widely used by activists – should consider following suit with similar precautions. Systems to remotely delete applications and data – for example, after a device is seized – would be particularly useful.

At the same time, use of these tools requires a level of knowledge and security awareness that many Myanmar internet users simply do not have. Although digital security habits have improved significantly since 1 February, including through the uptake of VPNs and encrypted messaging applications such as Signal, it is largely younger and better educated users who have tightened up their practices. There is still a significant knowledge deficit in some demographics, which is particularly concerning given the array of tools the Tatmadaw has to target users. Digital rights and digital literacy have been much neglected amid Myanmar's telecoms liberalisation; donors and technology companies need to start taking it much more seriously by providing the necessary financial and technical support to local actors involved in these issues.[136]

Finally, the CRPH and the National Unity Government it recently formed should take steps, if only symbolic ones given their limited power, to rectify some of the damage that the NLD inflicted on digital rights and privacy during its time in office. They could announce policies that enshrine privacy. They could also affirm their commitment to a free and open internet and to protecting the rights of internet users, including their right to freedom of expression. Even though the unity government is not now in the position to enforce such policies, such steps would send an important signal that the NLD and its partners recognise the importance of the issue. The CRPH could also use its high-profile platform to promote digital literacy and good security habits among Myanmar internet users.

C. *Investing and Operating Responsibly*

Technology companies in Myanmar, most of which entered the country during the term of the Thein Sein government, have been forced to navigate an increasingly difficult operating environment in recent years. The NLD government had already taking steps to erode data privacy, freedom of expression and access to a free and open internet, and Myanmar's regulatory framework often left investors with few options but to comply. This trend has accelerated dramatically since the 1 February coup, and orders to technology companies are now backed up, if necessary, by soldiers with guns. Refusing to follow the junta's instructions is not an option if they are to con-

[135] See "Facebook Introduces a New Safety Feature in Myanmar", Facebook, 31 March 2021.
[136] One example of a local initiative to draw attention to digital rights issues is the Myanmar Digital Rights Forum, which has been held annually since 2016.

tinue to operate in Myanmar. Leaving the country, however, would mean both abandoning their investment and depriving users of their services.

Nevertheless, companies operating in Myanmar should, to the extent possible, push back against the military regime's diktat, both publicly and privately. The military is increasingly difficult to influence because it is so focused on survival, but a combination of direct, behind-the-scenes lobbying and public collective action is the approach most likely to have any positive effect. Joint statements, including through foreign chambers of commerce, also offer the chance to publicly raise concerns, which reduces (though does not eliminate) the risk of being singled out for retribution by Naypyitaw.[137] For their part, civil society organisations working on digital rights should appreciate the challenges that technology businesses, particularly mobile operators and service providers, are facing, and try to build alliances with those that are committed to improving digital rights and protecting their users, such as Telenor.[138]

The regime's push to establish an intranet creates a further ethical dilemma for businesses already operating in Myanmar, particularly mobile operators and internet service providers. Agreeing to whitelist applications might benefit users, for example by giving them access to mobile banking applications, but also contributes to perpetuating internet restrictions that serve the regime's political needs. Although playing along will benefit these businesses in the short term, it comes with long-term costs because the whitelisting system will restrict the growth of the digital economy. Although it would involve some risk, ideally, operators and service providers should adopt a common position on the type of applications they will whitelist – for example, essential services – but at the same time continue to push back against the intranet plan, and publicly and privately call for the lifting of all restrictions.

Meanwhile, technology companies from around the world – whether equipment suppliers or software providers – should exercise heightened due diligence when conducting business with entities in Myanmar, to make sure they are not directly or indirectly assisting or supporting the military regime.

D. *Improving Social Media Moderation and Policies*

Social media companies have a particularly important role to play in post-coup Myanmar. The military regime has a long history of coordinated disinformation on social media. It is likely to continue to pursue such campaigns if given the opportunity, especially at a time when it seeks to project legitimacy in the face of overwhelming domestic and international condemnation.

Social media platforms need to be prepared for these activities. In response to its earlier mistakes during the 2017 Rohingya crisis, Facebook has made major progress in detecting and removing dangerous content linked to the military. Since the coup it

[137] Some foreign business chambers have already used statements on the crisis to call for internet access to be restored. See "Statement on Myanmar by AustCham Myanmar, British Chamber of Commerce Myanmar, CCI France Myanmar, New Zealand Myanmar Chamber of Commerce", 30 March 2021.

[138] Among mobile operators and internet service providers, Telenor has been the most consistent in pushing for internet restrictions to be lifted and in disclosing government orders. See, for example, "The case for open internet in Myanmar", op. cit.; and "Myanmar needs connectivity", Telenor Myanmar, 13 April 2021.

has also taken a clear position by banning the Tatmadaw from its platform. As the military shifts to other social networks in an effort to keep its propaganda online, these platforms should carefully consider whether to follow Facebook's lead and ban the military as well, taking into account not just recent events, but also the fact that it has a history of coordinated dangerous behaviour that has resulted in real-world harm. Given that the lack of Myanmar-language capacity at most social media platforms leaves them vulnerable to misuse, they certainly need to be vigilant about the possibility of the Tatmadaw and its proxies misusing them.

TikTok, in particular, needs to consider carefully how it responds to the use of its platform by military personnel. While worrying content appears to emanate from individual accounts, their behaviour is different from what is observed on other platforms, where in recent times soldiers have rarely worn their uniforms or shown their weapons. It is possible the military has coordinated a campaign designed to take advantage of TikTok's relative lack of moderation capacity and less-developed policies to influence younger internet users, as well as the military's political base.[139] The company has taken steps to eliminate a large part of the intimidating content flooding its platform by better enforcing its existing policy on the display of firearms.[140] But given its rising popularity in Myanmar, it needs to continue to invest in technology, personnel and partnerships to better tackle the threat moving forward.

[139] Crisis Group interviews, social media researchers, March 2021.

[140] Although TikTok bans displays of firearms outside a "controlled environment", this policy has been loosely enforced across the platform, not just in relation to Myanmar content. See, for example, "TikTok has a gun problem, and it's doing nothing to fix it", Digital Trends, 8 March 2021; and "TikTok is teaching teens how to build fully automatic rifles and make 'hollow point' ammunition", Media Matters for America, 10 February 2021.

VI. Conclusion

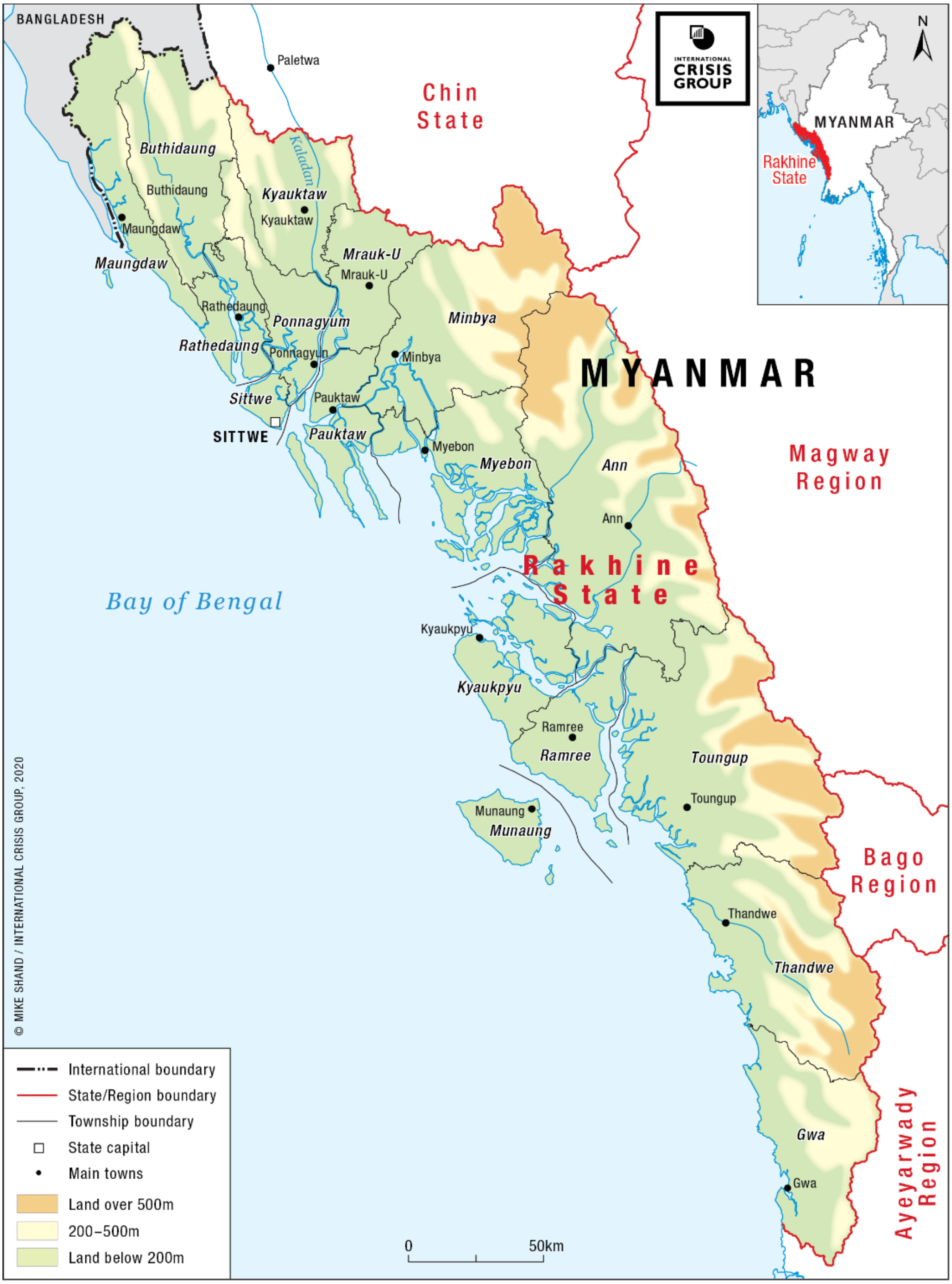
The 1 February coup has turned Myanmar's online sphere into a key battleground for both the military regime and its opponents. Although the Tatmadaw has sought to build its digital capabilities over the years, it was not prepared to tackle such strong and widespread opposition to military rule. Protest organisers, NLD politicians and leaders of the civil disobedience movement have used social media and other applications highly effectively to organise demonstrations and undertake activities to undermine the regime. Meanwhile, Facebook's decision to ban the military from the country's most popular social media platform has significantly disrupted its ability to communicate with the public or even its own soldiers.

Reflecting the difficulty it faces in controlling Myanmar's population after a decade of liberalisation, the only way the military has found to wage this online fight is to shut down the internet. The economic and social cost of such a decision is enormous, crippling businesses and nurturing even stronger resentment toward the military. Lack of internet access also impairs the regime's ability to govern, as well as communicate with its own base. Yet any relaxation of internet restrictions is likely to re-energise the protest movement by enabling activists to once again coordinate and share information. To overcome this contradiction, the junta appears to be taking the first steps toward developing a national intranet, in which most users will have access to just a handful of vetted applications. While an intranet may appear to be a short-term solution, it will stifle innovation, access to information and economic growth, and tech-savvy users are likely to find loopholes and gain access to the worldwide web.

Foreign governments, technology firms and businesses operating within the country should push back strongly against internet restrictions, which are a violation of the fundamental rights of the people of Myanmar. Foreign technology companies can and should take steps to help keep the internet as open as possible and protect users from the regime, particularly by making VPNs more widely available, and improving digital security knowledge. Foreign governments should, for their part, strengthen arms embargoes to include "dual-use" equipment and software that can be used by the regime to target opponents and enforce such embargoes properly.

Yangon/Brussels, 18 May 2021

Appendix A: Map of Rakhine State



© MIKE SHAND / INTERNATIONAL CRISIS GROUP, 2020

Appendix B: About the International Crisis Group

The International Crisis Group (Crisis Group) is an independent, non-profit, non-governmental organisation, with some 120 staff members on five continents, working through field-based analysis and high-level advocacy to prevent and resolve deadly conflict.

Crisis Group's approach is grounded in field research. Teams of political analysts are located within or close by countries or regions at risk of outbreak, escalation or recurrence of violent conflict. Based on information and assessments from the field, it produces analytical reports containing practical recommendations targeted at key international, regional and national decision-takers. Crisis Group also publishes *CrisisWatch*, a monthly early-warning bulletin, providing a succinct regular update on the state of play in up to 80 situations of conflict or potential conflict around the world.

Crisis Group's reports are distributed widely by email and made available simultaneously on its website, www.crisisgroup.org. Crisis Group works closely with governments and those who influence them, including the media, to highlight its crisis analyses and to generate support for its policy prescriptions.

The Crisis Group Board of Trustees – which includes prominent figures from the fields of politics, diplomacy, business and the media – is directly involved in helping to bring the reports and recommendations to the attention of senior policymakers around the world. Crisis Group is co-chaired by President & CEO of the Fiore Group and Founder of the Radcliffe Foundation, Frank Giustra, as well as by former Foreign Minister of Argentina and Chef de Cabinet to the United Nations Secretary-General, Susana Malcorra.

After President & CEO Robert Malley stood down in January 2021 to become the U.S. Iran envoy, two long-serving Crisis Group staff members assumed interim leadership until the recruitment of his replacement. Richard Atwood, Crisis Group's Chief of Policy, is serving as interim President and Comfort Ero, Africa Program Director, as interim Vice President.

Crisis Group's international headquarters is in Brussels, and the organisation has offices in seven other locations: Bogotá, Dakar, Istanbul, Nairobi, London, New York, and Washington, DC. It has presences in the following locations: Abuja, Addis Ababa, Bahrain, Baku, Bangkok, Beirut, Caracas, Gaza City, Guatemala City, Jerusalem, Johannesburg, Juba, Kabul, Kiev, Manila, Mexico City, Moscow, Seoul, Tbilisi, Toronto, Tripoli, Tunis, and Yangon.

Crisis Group receives financial support from a wide range of governments, foundations, and private sources. Currently Crisis Group holds relationships with the following governmental departments and agencies: Australian Department of Foreign Affairs and Trade, Austrian Development Agency, Danish Ministry of Foreign Affairs, Dutch Ministry of Foreign Affairs, European Union Emergency Trust Fund for Africa, European Union Instrument contributing to Stability and Peace, Finnish Ministry of Foreign Affairs, French Development Agency, French Ministry of Europe and Foreign Affairs, Global Affairs Canada, Iceland Ministry for Foreign Affairs, Department of Foreign Affairs and Trade of Ireland, Japan International Cooperation Agency, the Principality of Liechtenstein Ministry of Foreign Affairs, Luxembourg Ministry of Foreign and European Affairs, Norwegian Ministry of Foreign Affairs, Qatar Ministry of Foreign Affairs, Swedish Ministry of Foreign Affairs, Swiss Federal Department of Foreign Affairs, United Nations Development Programme, UK Foreign, Commonwealth and Development Office, and the World Bank.

Crisis Group also holds relationships with the following foundations and organizations: Adelphi Research, Carnegie Corporation of New York, Facebook, Ford Foundation, Friedrich-Ebert-Stiftung, Global Challenges Foundation, Henry Luce Foundation, John D. and Catherine T. MacArthur Foundation, Open Society Foundations, Ploughshares Fund, Robert Bosch Stiftung, Rockefeller Brothers Fund, and Stiftung Mercator.

May 2021

Appendix C: Reports and Briefings on Asia since 2018

Special Reports and Briefings

Council of Despair? The Fragmentation of UN Diplomacy, Special Briefing N°1, 30 April 2019.

Seven Opportunities for the UN in 2019-2020, Special Briefing N°2, 12 September 2019.

Seven Priorities for the New EU High Representative, Special Briefing N°3, 12 December 2019.

COVID-19 and Conflict: Seven Trends to Watch, Special Briefing N°4, 24 March 2020 (also available in French and Spanish).

A Course Correction for the Women, Peace and Security Agenda, Special Briefing N°5, 9 December 2020.

North East Asia

The Korean Peninsula Crisis (I): In the Line of Fire and Fury, Asia Report N°293, 23 January 2018 (also available in Chinese).

The Korean Peninsula Crisis (II): From Fire and Fury to Freeze-for-Freeze, Asia Report N°294, 23 January 2018 (also available in Chinese).

The Case for Kaesong: Fostering Korean Peace through Economic Ties, Asia Report N°300, 24 June 2019.

South Asia

Countering Jihadist Militancy in Bangladesh, Asia Report N°295, 28 February 2018.

China-Pakistan Economic Corridor: Opportunities and Risks, Asia Report N°297, 29 June 2018 (also available in Chinese).

Building on Afghanistan's Fleeting Ceasefire, Asia Report N°298, 19 July 2018 (also available in Dari and Pashto).

Shaping a New Peace in Pakistan's Tribal Areas, Asia Briefing N°150, 20 August 2018.

Sri Lanka: Stepping Back from a Constitutional Crisis, Asia Briefing N°152, 31 October 2018.

After Sri Lanka's Easter Bombings: Reducing Risks of Future Violence, Asia Report N°302, 27 September 2019.

Getting the Afghanistan Peace Process Back on Track, Asia Briefing N°159, 2 October 2019.

Twelve Ideas to Make Intra-Afghan Negotiations Work, Asia Briefing N°160, 2 March 2020.

Raising the Stakes in Jammu and Kashmir, Asia Report N°310, 5 August 2020.

Pakistan's COVID-19 Crisis, Asia Briefing N°162, 7 August 2020.

Taking Stock of the Taliban's Perspectives on Peace, Asia Report N°311, 11 August 2020.

What Future for Afghan Peace Talks under a Biden Administration?, Asia Briefing N°165, 13 January 2021.

South East Asia

The Long Haul Ahead for Myanmar's Rohingya Refugee Crisis, Asia Report N°296, 16 May 2018 (also available in Burmese).

Myanmar's Stalled Transition, Asia Briefing N°151, 28 August 2018 (also available in Burmese).

Bangladesh-Myanmar: The Danger of Forced Rohingya Repatriation, Asia Briefing N°153, 12 November 2018.

Fire and Ice: Conflict and Drugs in Myanmar's Shan State, Asia Report N°299, 8 January 2019 (also available in Burmese).

A New Dimension of Violence in Myanmar's Rakhine State, Asia Briefing N°154, 24 January 2019 (also available in Burmese).

Building a Better Future for Rohingya Refugees in Bangladesh, Asia Briefing N°155, 25 April 2019.

An Opening for Internally Displaced Person Returns in Northern Myanmar, Asia Briefing N°156, 28 May 2019 (also available in Burmese).

The Philippines: Militancy and the New Bangsamoro, Asia Report N°301, 27 June 2019.

Peace and Electoral Democracy in Myanmar, Asia Briefing N°157, 6 August 2019.

Myanmar: A Violent Push to Shake Up Ceasefire Negotiations, Asia Briefing N°158, 24 September 2019.

A Sustainable Policy for Rohingya Refugees in Bangladesh, Asia Report N°303, 27 December 2019.

Southern Thailand's Peace Dialogue: Giving Substance to Form, Asia Report N°304, 21 January 2020 (also available in Malay and Thai).

Commerce and Conflict: Navigating Myanmar's China Relationship, Asia Report N°305, 30 March 2020.

Southern Philippines: Tackling Clan Politics in the Bangsamoro, Asia Report N°306, 14 April 2020.

Conflict, Health Cooperation and COVID-19 in Myanmar, Asia Briefing N°161, 19 May 2020.

An Avoidable War: Politics and Armed Conflict in Myanmar's Rakhine State, Asia Report N°307, 9 June 2020.

Rebooting Myanmar's Stalled Peace Process, Asia Report N°308, 19 June 2020.

COVID-19 and a Possible Political Reckoning in Thailand, Asia Report N°309, 4 August 2020.

Identity Crisis: Ethnicity and Conflict in Myanmar, Asia Report N°312, 28 August 2020.

Majority Rules in Myanmar's Second Democratic Election, Asia Briefing N°163, 22 October 2020 (also available in Burmese).

From Elections to Ceasefire in Myanmar's Rakhine State, Asia Briefing N°164, 23 December 2020.

Responding to the Myanmar Coup, Asia Briefing N°166, 16 February 2021.

The Cost of the Coup: Myanmar Edges Toward State Collapse, Asia Briefing N°167, 1 April 2021.

Southern Philippines: Keeping Normalisation on Track in the Bangsamoro, Asia Report N°313, 15 April 2021.

Appendix D: International Crisis Group Board of Trustees