

Avoiding Pitfalls in Engaging with Digital Myanmar: A Post-coup Analysis of Risk Mitigation (Part 1)

- BY TEACIRCLEOXFORD
- POSTED ON MARCH 15, 2021

Benedict Mette-Starke analyses Myanmar digital communication considerations in Part 1 of a 2-part post on digital conduct concerning Myanmar.

The coup took many by surprise. So too did the first internet **shutdown** in the coup's early hours, the subsequent blocking of **Facebook** and later of **Twitter** and **Instagram** by the **Ministry of Transport and Communication**. On February 6, both landline and mobile internet access were **almost completely** shut down. They started **working** again on Sunday, February 7, 2 pm Myanmar Time when internet service providers (ISPs) received an **order** to turn internet access **back on**. Since **February 15**, **shutdowns** have occurred daily between 1-9 am.[1] As of February 10, a new draft „Cyber Security Law“ is circulating on **social media**. It has since been condemned in a **statement** by **over 250** civil society organizations. In parallel to the protests, laws including the **Law Protecting the Privacy and Security of Citizens**, the **Electronic Transactions Law**[2], the **Ward or Village-Tract Administration Law**, and sections of the **Penal Code** have been amended by the military. One of the first people to be shot at, Ma Mya Thwet Thwet Khine, on February 19, **succumbed** to wounds sustained ten days prior. The violence used by the armed forces has escalated, particularly since the **last weekend in February**. These many changes within a short timespan illustrate the situation's volatility.

Staying **connected**, something digital networks promise, is crucial for those inside and outside Myanmar for coordination, news, and support. Yet, some means of engagement bear risks. This post first elaborates the risks associated with digital communications laid out in a Myanmar language resource. The post then applies this resource to the communications strategies of those outside Myanmar.

Learning from those most experienced in avoiding digital pitfalls—those local to Myanmar—seems reasonable. Digital rights activists[3] and others have been adapting since at least 1994 (Houtman 1999: 2; see further Brooten, McElhone, and Venkiteswaran 2019b). Internet shutdowns and surveillance are nothing new, despite the current shutdowns' unprecedented scale, with shutdowns in

several townships in Rakhine and Chin State lasting from June 2019 to August 2020.[4]

To illustrate the experience gained by local activists and other digital media users, the post relies on a *Google Doc* named “Risk Mitigation and Management Guide.pdf” (RMMG; in Myanmar) posted on *Twitter* by @myanmarido, Myanmar ICT for Development’s (MIDO) account, on the first day of the coup. MIDO is a civil society organisation founded in 2012 that aims to make information and communication technology (ICT) a force for social and political change. The file itself, however, names no author. It is much broader than this blog post and is aimed at people currently in Myanmar. In this post, the RMMG will be a) analysed to tease out its underlying concerns in Part 1 and b) consulted for practical advice insofar as it is relevant for those outside of—but engaging with—Myanmar in Part 2. The latter will be supplemented, where needed, by resources on issues the RMMG does not cover. Taking the author of the RMMG as a primary holder of digital security skills and knowledge regarding Myanmar, this post argues that their concerns should also matter for those engaged with Myanmar from the outside.

ဆိုင်ဘာလုံခြုံရေးဥပဒေ (မူကြမ်း)

အိ:

ကုန်းရမှာလား?



Concerning Risks

Framed as a “[r]isk mitigation guide on communication strategies for the frontline journo and others in Myanmar in case of internet disruptions,” the RMMG places „risk“ very prominently. By posting it on Twitter, I understand @myanmarido to signal their concern that this might become relevant to many beyond “frontline journo” towards “others in Myanmar.”

At the outset, published immediately following the coup, the RMMG assumes a certain degree of risk. The author provides specific criteria against which a reader can evaluate their own risk level, „Code Green,” „Yellow” and „Red.” „Code Green”’s touchstones are that the internet is (still) accessible, that no arrests have been made (yet), and that there is (still) time to enact described measures. It thereby presents those events as everyday possibilities and articulates a distribution of risk (cf. Beck 1992; Lupton [1999] 2013) across time. In „Code Green,” the suggestion is to establish buddy groups to regularly check-in with if in immediate danger of arrest, as well as having a suitcase with everything you need in that case. Codes „Yellow” and „Red” escalate measures for times when arrests are imminent and time is of the essence. While „Code Yellow”, for instance, recommends device factory resets, „Code Red” recommends apps to keep up communication if there is no internet. However, as the RMMG states early on, no app will guarantee full security. Risk is ever-present and digital security an everyday practice.

Risks of Illegitimate Access

The first measures described in the RMMG address the risk of illegitimate access to one’s data. Several password security measures are suggested to safeguard an account, including a free, encrypted password manager and 2 Factor Authentication (2FA). 2FA relies on additional identifying factors inherent or in the possession of a user to grant account access. Advising that one should not share one’s passwords and devices with others contradicts common practice in Myanmar (compare, e.g., Zainudeen and Galpaya 2016; Thant Sin Oo 2019). Many people share phones, accounts, and passwords with loved ones and family. Keeping those „private” can be interpreted as secrecy „against” them. However, the RMMG’s measures emphasize illegitimate access by third parties, not secrecy against close relations or privacy from companies. It is more important to patch security loopholes through updates provided through app stores than to guard against surveillance by companies providing those app stores or than keeping features of old app versions. The need to secure all media and restrict illegitimate access by third parties is further corroborated by the RMMG recommending the encryption of entire devices and sensitive material. Images, e.g., taken as evidence, the author suggests, should be

encrypted using *Tella*. Recommending encryption shows that the aim is to guard access to accounts and stored data.

The RMMG author's fear, as I interpret it, is that illegitimate access could be used to impersonate someone online, to get contact details of their friends and colleagues, or access material to incriminate or extort someone, potentially wrongfully. Parties that could take those actions could include the military. Device locking and encryption reduces these possibilities.

Risk of Surveillance

Surveillance of communication is another significant concern in the RMMG. It explicitly calls phone calls and text messages (SMS) insecure. This seems to suggest that conversations, like data and access, can be used to increment, extort and expose those under surveillance. To mitigate this risk, the author suggests using end-to-end encrypted (e2ee) methods of communication, such as *Signal*, *Wire*, *Silence SMS*, *Briar* and others. Thereby, only communicating users (or devices) can decrypt and read the messages sent. E2ee means that, as the messages are transmitted, they get scrambled so that it becomes unfeasible to decrypt them. In addition to this strategy, the author suggests several other ways to make conversations safer, by carving out spaces where communication is possible away from watchful eyes and ears.

The risk of surveillance may be compounded by Article 40 of the [Telecommunication Law \(Pyidaungsu Hluttaw Law No. 31/2013, amended 2017\)](#), which grants regulators access to unspecified information held by telecommunications companies, including ISPs. Legally sanctified surveillance is expanded upon by many of the amendments and the drafted Cyber Security Law mentioned above. The draft's Articles 30 and 31 raise anxieties over increased surveillance, requiring those who offer online services for use in Myanmar to keep users' details as specified by the ministry for three years and hand these over at the ministry's request. So, while there have been calls to [boycott individual companies](#), it seems that the RMMG implies that all non-encrypted communication through telecommunication operators' services, be

they mobile service operators such as MPT, Telenor, Ooredoo or Mytel or fixed line and other operators such as 5BB Broadband, WeLink, or Myanmarnet, to name a few, are generally insecure.

YOU ARE UNDER SURVEILLANCE



Risk of Arrest

Concern over surveillance is coupled with the risk of arrest and prosecution. Arrests have been very visible since the coup. In addition to the laws already mentioned, several others can easily lead to incarceration. There are defamation laws like the famous Article 66(d) of the Telecommunication Law and the Computer Science Development Law issued on September 27, 1996. The latter requires government registration of any connection-capable device (personal communication, February 2019; see further Hudson-Rodd 2008: 89; Brooten, McElhone, and Venkiteswaran 2019a: 27; Emad and McAuliffe 2019: 142), but this is rarely observed. Therefore, practically anyone with a smartphone can be prosecuted if they attract someone's negative attention with the means to charge them. Even under civilian governments, conviction rates for some of the above laws were exceptionally high.

Since negative attention can spell conviction, particularly for those residing in Myanmar, it is vital to know how those you work with want to be portrayed. While there are some who might want their message to be spread, some might also want to keep their names out of the spotlight. Communicate with them to establish their terms. As people engaging with Myanmar, we need to acknowledge and use our privileges without unnecessarily endangering our interlocutors.^[5]

Risk of Restrictions to Access to Information and Communication

The RMMG suggests managing the risk of losing touch digitally through both measures to circumvent internet blockages as well as through non-internet-based ways of connecting. While it aims against illegitimate access to data, the RMMG tackles communication impediments. Staying in touch is vital for sharing news and to coordinate protests. To allow for this, the RMMG recommends using a Virtual Private Network (VPN). VPNs redirect all or part of these devices' internet traffic, depending on the setup, through a server network. It, therefore, looks as if the network, not the device itself, is communicating with the internet at large. Only traffic between the server network and the device can be seen. If a VPN server is not affected by website blocking, these websites can be accessed through the VPN. Some VPN providers further cloak traffic by encrypting it so that information cannot be intercepted by themselves or any other party. Some also refrain from logging connection details so that these cannot be examined later.

While the RMMG document speaks of risk mitigation, it also highlights the potential benefits of keeping in touch through digital means, e.g., the „buddy“ groups mentioned above, as long as communication is secured through e2ee.

Hence, the RMMG recommends several ways of staying in touch without depending on cell towers and the companies which run them. While the RMMG does not endorse only one app, all those it recommends, like *Bridgefy*, *Briar*, and *Talkie*, work through lower-scale connections, e.g., mesh-networks over Wi-Fi or Bluetooth. Those networks use devices as nodes relaying information ideally. They do not depend on more extensive telecommunication infrastructures, although they can use them, and are therefore more challenging to shut down, keeping networks of trusted parties intact.

Read [Part 2](#) here.

(All images used permission of owners)

***Benedict Mette-Starke** is a PhD candidate in social and cultural anthropology at the University of Konstanz, Germany. He has conducted ten months of research on digital rights activism in Myanmar in 2019 and 2020.*