The Rise of Online Censorship and Surveillance in Myanmar: A Quantitative and Qualitative Study

Phyu Phyu Kyaw
Information Controls Fellow, Open Technology Fund

November 2020

Contents

Key Findings

- **Approximately 200 URLs are blocked in Myanmar.** The majority of these blocked sites are pornographic websites, however, 41 media websites were also found to be blocked between January 1 and July 27, 2020.
    - The blocking of media websites varies across different networks in Myanmar because different Internet Service Providers (ISPs) block different sites. Despite this variance in blocking across networks, most of the blocked media websites were blocked on at least three local networks in the country.

- **The government of Myanmar finances surveillance technologies.** The Ministry of Transport and Communications (MoTC) designated approximately 4 million USD (6,190 million kyats) to implement a Lawful Interception System for 2019-2020.
    - These funds came in addition to the approximately 4.6 million USD that was spent in 2017 on a Social Media Monitoring Team (SMMT).

- **79% of surveyed human rights defenders, journalists, activists, and researchers do not feel secure online.**
    - This level of insecurity is attributable to high levels of intimidation and physical surveillance by the authorities.

- **45% of those individuals surveyed that work in rights-related fields acknowledge they engage in online self-censorship to avoid harassment from authorities.**
    - This heightened level is attributable to fears related to, and experience with, social media monitoring and surveillance.

- **72% of those who self-censor are women.**
    - This includes those working on the peace process, human rights violations documentation, digital rights, and legal reforms.

Introduction

This research study seeks to identify the various surveillance and censorship technologies and strategies deployed by the government and military in Myanmar. In doing so, the study utilizes a diverse combination of analytical methods including technical network measurements, interviews, and key research analysis of newspaper archives, media reports, and government publications. Throughout the overall assessment process, the study focuses not only on technology, but also on offline spaces and legal loopholes which tend to obscure transparency and allow the authorities in Myanmar to implement surveillance and censorship practices in unchecked manners.

The goal of this project is to shine a light on these troublesome tactics, helping both the people of Myanmar as well as other internet freedom researchers around the world. In countries such as Myanmar, where information on existing surveillance practices is limited, this type of research is all the more difficult - and important - to conduct. It is therefore the hope of this study the information produced by this research serves as a seed that will ultimately sprout and grow into a tree of resistance, hope, and change.

The study begins with an overview of Myanmar's relevant political and internet-based background. Next, the study's methodologies and limitations are discussed. The core of the study is then devoted to findings from research and measurements, followed by findings from interviews. Finally, the study finishes with concluding thoughts and key acknowledgements.

Background

This section of the research study provides relevant background information regarding Myanmar's political context as well as the country's online connectivity, surveillance practices, and restrictions.

Political Turbulence

Myanmar operated under the rule of a military regime from 1962 until 2011. This period of rule was followed by the 2010 election, which was criticized for allowing only government-sanctioned political parties to participate and declaring the opposition party, the National League for Democracy (NLD), to be illegal. After the election, the country was led from 2011 to 2015 by a former leading member of the military who maintained close ties to the prior junta. In 2015, the NLD came to power with a landslide electoral victory. Today, despite the presence of the ruling NLD government, the military still maintains a strong influence over politics, with 25% of the seats in the parliament reserved for the military.

Civil war still continues since the country's political transition began nearly a decade ago. Although the NLD government has attempted to broker a ceasefire agreement (via a series of peace conferences known as the 21st Century Panglong Conference), civil strife continues to exist in Rakhine State, Kachin State, and the northern parts of Myanmar. August 2020 marked the third anniversary of the displacement of more than 730,000 Rohingya from Rakhine State to Bangladesh after a military crackdown was triggered by an attack on Myanmar security posts in August 2017 by the Arakan Rohingya Salvation Army.

Amidst COVID-19 outbreaks and civil war, another election is scheduled to occur on November 8, 2020. According to the Rakhine State Election Sub-commission, however, the government has not been able to publicly post preliminary voter lists in 15 village-tracts in northern Rakhine due to armed conflicts between the Myanmar military and the Arakan Army.

Unprotected Connectivity

After Myanmar transitioned to a civilian government in 2011, the country experienced a connectivity revolution. Operating licenses to provide internet service were issued to foreign telecommunication companies following the 2013 passage of the Telecommunications Law. Yet although the market's opening enabled millions of people in Myanmar to access the internet, it also created new concerns for online rights. Overly broad and rights-abusing laws jeopardize online freedom of expression and privacy, enabling government authorities to harass and oppress their critics.

Online Surveillance

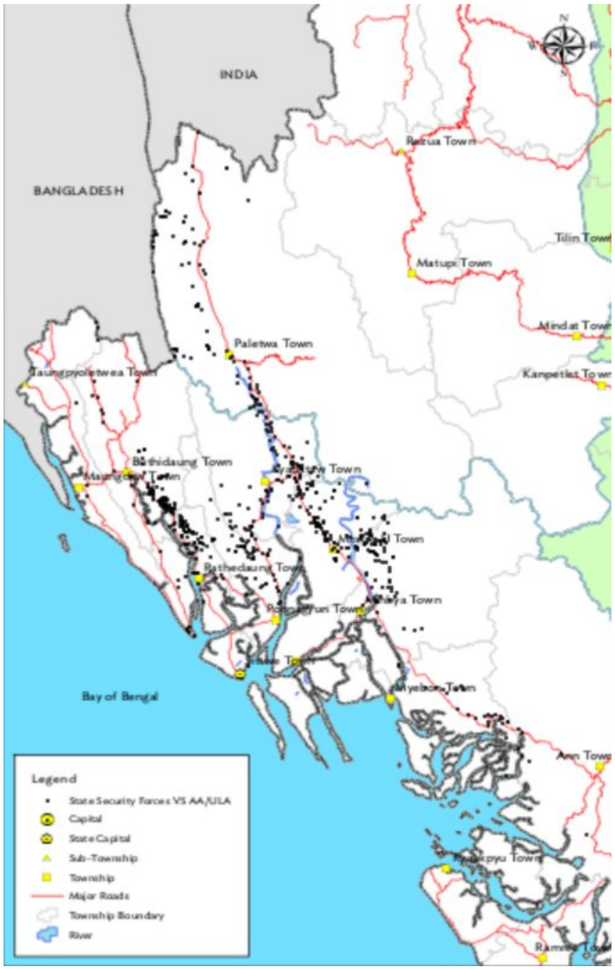
Phone surveillance, state-sponsored hacking attempts, and internet censorship and surveillance are common concerns for activists and journalists in Myanmar. For example, in 2017, the NLD government spent 6.42 billion kyats (approximately $4.6 million) to set up and purchase tools for the Social Media Monitoring Team (SMMT). According to an interview with the Minister of Transport and Communication (MoTC), the SMMT was established to track events that could potentially damage the stability of the state. Notably, however, the SMMT's mandate goes beyond monitoring social media and no information was made public regarding what devices or hardware were purchased.

The surveillance capacity of Myanmar's military is also a major concern for individual and digital rights. For example, it has been documented that the military is using software such as Cellebrite (a forensics tool that can be used to surveil). Cellebrite was used in Myanmar when reporters Wa Lone and Kyaw Soe Oo were arrested for reporting on the Rohingya crisis. According to court documents and statements, Cellebrite pulled documents from the reporters' phones - including the itineraries for Pope Francis's visit to the country and the details of the military's campaign in Rakhine. The military also operates a specialized psychological warfare unit which produces and disseminates a systematic flow of disinformation and hate speech on Facebook.

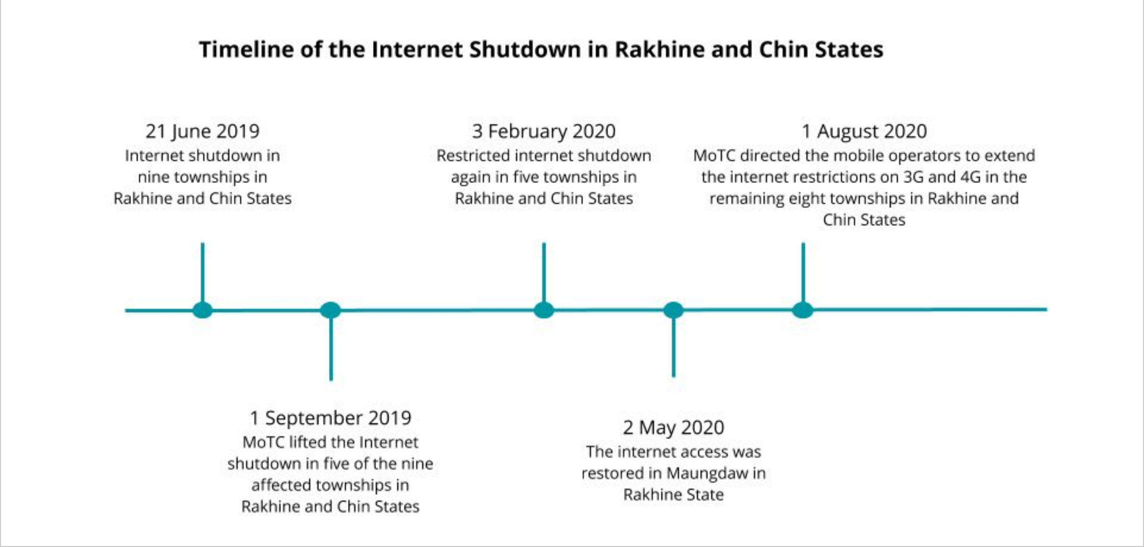
Additionally, in June 2019, Kaspersky reported having detected FinSpy being used to collect a variety of private user information on various platforms. According to their telemetry, several dozen unique mobile devices have been infected over the past year.

Internet Shutdowns and Restrictions

Restrictions on internet access and bandwidth also occur in Myanmar. Nine townships in Rakhine and Chin States have experienced an internet shutdown that lasted over one year. Eight of these townships were from Rakhine State (Maungdaw, Ponnagyun, Mrauk-U, Kyauktaw, Minbya, Buthidaung, Rathedaung, Myebon), along with Paletwa township from Chin State.



Notably, the conflict between Myanmar's military and the Arakan Army has been ongoing for nearly two years. The map above shows the clashes between state security forces and the Arakan Army in Rakhine and Chin states in 2019 (as reported by Myanmar Institute for Peace and Security). From this reporting, it appears as though the townships which experienced internet shutdowns and still do not have quality internet are all townships where clashes frequently occur.



Timeline of the Internet Shutdown in Rakhine and Chin States

21 June 2019
Internet shutdown in nine townships in Rakhine and Chin States

1 September 2019
MoTC lifted the Internet shutdown in five of the nine affected townships in Rakhine and Chin States

3 February 2020
Restricted internet shutdown again in five townships in Rakhine and Chin States

2 May 2020
The internet access was restored in Maungdaw in Rakhine State

1 August 2020
MoTC directed the mobile operators to extend the internet restrictions on 3G and 4G in the remaining eight townships in Rakhine and Chin States

Figure 1: *Timeline of the internet shutdown in Rakhine and Chin States*

As demonstrated in Figure 1, the MoTC's directive to shut down the internet in nine townships in Rakhine and Chin States went into effect on June 21, 2019. On September 1, 2019, the MoTC lifted the shutdowns in five of the nine affected townships. The restrictions were then reimplemented on February 3, 2020. Internet access was restored in Maungdaw in Rakhine State on May 2, 2020. On July 30, 2020, the MoTC directed mobile operators to extend the internet restrictions on 3G and 4G in the remaining eight townships in Rakhine and Chin States.

On April 10, 2020, the Ministry of Foreign Affairs, led by the State Counsellor Aung San Su Kyi, stated that the reason for the internet shutdowns in Rakhine and Chin States was to prevent the misuse of the internet by the Arakan Army for their political and military agenda.

As of August 25, 2020, people in those nine townships (except for Maungdaw) still do not have access to 3G or 4G. According to Telenor, the MoTC cited prevention of acts of terrorism as the reason to continue the internet restrictions until October 31, 2020.

Methodology

This research study utilized a three-step process to help identify the various surveillance technologies and strategies used by the Myanmar government and military. The first step involved gathering relevant publicly available information by continuously reviewing and monitoring reports and announcements by the government and media. The second step involved assessing the presence of government and military-backed surveillance technology by testing at-risk devices and testing levels of internet censorship by employing OONI network measurements. The third step involved conducting one-on-one interviews (either in person or over the phone) to obtain real-life insight into privacy, surveillance, and digital safety for those individuals who have high potential to be targeted and surveilled by the authorities. These three steps are discussed below.

Step One: Gathering Public Information

This first step of the research process involved gathering primary and secondary sources of information by monitoring government websites, independent media, and government and military activities. In doing so:

- Media and government websites were monitored to identify capacity-building training performed by external organizations for the government and military (or attending regional or international conferences/training).
- Government websites were monitored to gather information about conferences and call for tenders for software and hardware technologies from the relevant ministries such as the MoTC, as well as the Ministry of Information and the Ministry of Labour, Immigration, and Population.

Step Two: Device Testing and Network Measurements

The second step of the research process involved testing the devices of at-risk individuals (to determine the type of surveillance tools being utilized by the government and military) and taking network measurements (to determine levels of internet censorship and restrictions).

Identifying the targeted group for device testing

This approach was implemented by working with people who have been surveilled or hacked, or who have the potential for their communications and devices to be compromised by the authorities. The process of identifying members of the targeted group helps to uncover the various types of surveillance methods and tools that have been used by the authorities or other groups. Below, the individuals identified as part of the targeted group are referred to as “contact.” The individual who conducted the study is referred to as “the fellow.”

Selection Criteria

To be selected as a member of the targeted group, at least one of the following must be true:

- The contact’s device has been confiscated by the authorities,
- The contact’s online communications have been hacked,
- State-backed attackers have attempted to hack the contact’s communications,
- The contact has another potential risk or risks.

Analysis Process

Once a contact was identified, the fellow conducted the following analytical process:

- After an explanation of Emergency VPN by the Civilsphere Project (EVPN) was provided, and with the contact's consent, EVPN was utilized to generate a VPN profile for the contact to run.
    - EVPN is a service that provides a free security analysis of the mobile device network traffic to determine if the phone is infected, under attack, or compromised. Once the user connects to the Emergency VPN, CivilSphere captures the network traffic generated from the device for a few days. The data is then analyzed to determine if the phone is infected, or if there are any threats that the user should be aware of.
- After EVPN sends the analysis to the contact, the fellow explains the risks and information included in the report. The contact receives the digital safety steps they can take to make themselves more secure, as well as recommendations from EVPN and the fellow depending on the particular analysis received.
- If the analysis determines additional steps should be taken, with the consent of the contact, the fellow recommends the next steps such as sharing the analysis with organizations like Access Now.

Test list review

Test lists (machine-readable CSV files that include URLs to be tested for censorship) were utilized as part of Step Two. Censorship measurement projects like OONI rely on a global community of volunteers who run censorship detection tests from local vantage points. In light of bandwidth constraints, testing most websites available on the internet is not practical (nor possible in many cases). Instead, their measurements focus on a sample of websites provided in "test lists" - machine-readable CSV files with a set of curated, interesting domains. There are two types of test lists:

- Global test list: Includes a wide range of internationally relevant websites (e.g., facebook.com), most of which are in English.
- Country-specific test lists: Include websites that are only relevant to a specific country (e.g., Brazilian media websites), many of which are in local languages.

To maximize the breadth of coverage while reducing research bias, test list URLs are broken down into 30 diverse categories. The categories range from news media, culture, and human rights issues to more provocative or objectionable categories, like pornography (the latter are included because they are more likely to be blocked, enabling the detection of censorship techniques adopted by ISPs).

Creating test lists requires local knowledge, an understanding of which sites are commonly accessed and more likely to be blocked in light of a country's social and political environment. The Citizen Lab (which manages the test list project) has, therefore, made the lists publicly available on GitHub and encourages community contributions.

For this research study, the Myanmar test list was reviewed and updated prior to performing network measurements. In doing so, Netalitica's methodology was used.

Network measurement

Once the test lists were reviewed and updated, network measurements were conducted using OONI Probe (a free and open source software designed to measure various forms of internet censorship, such as the blocking of websites, instant messaging apps, and circumvention tools). OONI Probe has been run in Myanmar since 2012, and more than 263,000 network measurements have been collected from 34 local networks.

OONI Probe

The OONI Probe tool can be run to measure:

- Blocking of websites,
- Blocking of instant messaging apps (WhatsApp, Facebook Messenger and Telegram),
- Blocking of censorship circumvention tools (Tor and Psiphon),
- Presence of systems (middleboxes) in a network that might be responsible for censorship and/or surveillance, and
- Network speed and performance.

By running OONI Probe, the collected data can potentially serve as evidence of internet censorship since it shows how, when, where, and by whom the restriction was implemented. As soon as an OONI Probe user runs a test, the network measurement data from that test is instantly sent to OONI servers where it is automatically processed and published in near real-time.

As part of this project, OONI Probe tests were run in Myanmar between January 1 and July 31, 2020. Through the use of OONI Probe, this study worked to address the following questions:

- Which websites are blocked in Myanmar?
- How do ISPs block access to websites in Myanmar?
- Does the blocking of websites vary across networks in Myanmar? If so, how?
- Are popular instant messaging apps (WhatsApp, Facebook Messenger, Telegram) consistently accessible in Myanmar throughout the testing period of this study? If not, which ISPs in Myanmar block access to these apps and how do they block access?
- Are Tor and Psiphon accessible in Myanmar throughout the testing period of this study? If not, which ISPs block access to Tor and/or Psiphon and how do they block access?
- What is the speed and performance of local networks in Myanmar?
- Are middleboxes present on tested networks in Myanmar?

The above questions were examined by running the following OONI Probe tests:

- Web Connectivity test: Measures the DNS, TCP/IP, and HTTP blocking of websites.
- WhatsApp test: Measures the blocking of WhatsApp's mobile app and web version.
- Facebook Messenger test: Measures the blocking of Facebook Messenger.
- Telegram test: Measures the blocking of Telegram's mobile app and web version.
- Tor test: Measures the blocking of Tor.
- Psiphon test: Measures the blocking of the Psiphon app.
- HTTP Header Field Manipulation test: Measures networks to detect the presence of middleboxes.
- HTTP Invalid Request Line test: Measures networks to detect the presence of middleboxes.
- Network Diagnostic Test (NDT): Measures the speed and performance of networks.
- Dynamic Adaptive Streaming over HTTP (DASH) test: Measures video-streaming performance.

Step Three: Interviews

As the final step of the research process, interviews were used to better understand the overall surveillance experience, sense of safety, and privacy for individuals working on sensitive issues in Myanmar (such as human or digital rights).

A mix of in-person and Signal interviews were carried out with 24 people, of whom 50% were women. These individuals were selected based on the nature of their work, as well as via snowball recommendations from initial interviewees. The work of the interviewees included freedom of expression, human rights, digital rights, federalism, peace, conflict, anti-corruption, countering hate speech, civic tech, open data and open parliament, data and design, data driven storytelling, press freedom, and legal reform. All of the interviewees identified themselves either as solely activists, journalists, or human rights defenders, or as multiple identities.

For security reasons, the interview data has been anonymized, and information about the identities of the interview participants will not be disclosed.

The interview questionnaire can be found attached to this report as Annex A.

Limitations

There are three potential limitations to this study.

The first and foremost limitation was the difficulty in determining the true use of the equipment and strategies employed by the government and military. At times it was challenging to determine through a review of the tenders, which themselves are put out by the authorities, whether these technologies are used for surveillance or censorship purposes.

The second limitation was the ongoing pandemic. Due to COVID-19, travel was limited. The ability to perform network measurement tests on many different networks in Myanmar was therefore limited as well. In addition, the interviews scheduled to be carried out with journalists working to uncover the third-party companies purchasing the surveillance and censorship equipment were not able to be implemented due to travel restrictions and identity security reasons.

Third and final limitation was the test list. The list of blocked websites does not reflect all the blocked websites in Myanmar since the test list does not include all of the websites that have been created in Myanmar. Since Facebook is the tool that the majority of the people in Myanmar use to access, communicate, and coordinate, it was harder to curate a list of the websites for different categories. Furthermore, any potential content censorship implemented by Facebook on its platform was not included within the scope of this study's research.

Research and Measurement Findings

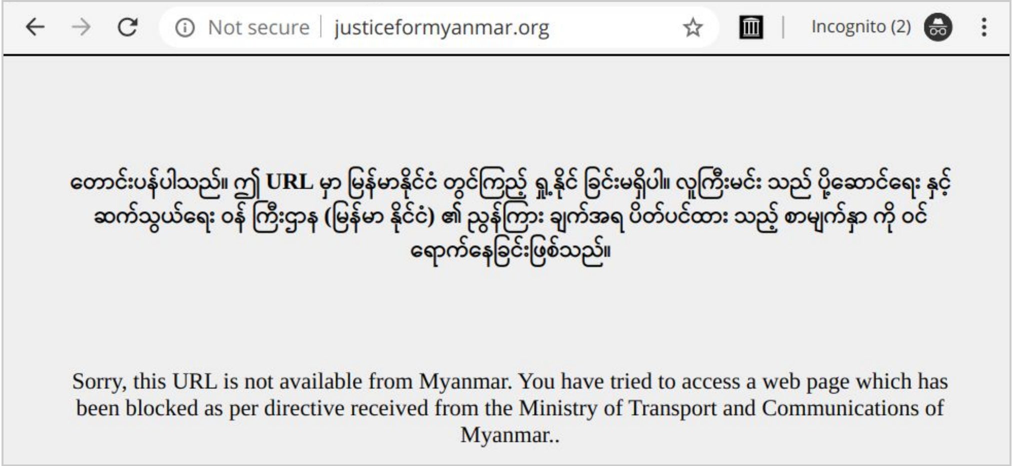
This section of the research study provides an overview of the project's research and measurement findings, detailing the existence of censorship in Myanmar as well as the surveillance capacity and capabilities of the authorities.

Censorship

In March 2020, ISPs in Myanmar received a directive from the MoTC ordering them to block 230 websites, most of which contained adult or explicit content. Media websites, however, also appeared on the list (such as Narinjara News and Development Media Group). Both of these organizations were covering the ongoing conflict in Rakhine State at the time.

Telenor Myanmar (a telecommunications subsidiary of the Norwegian Telenor Group) published a press release disclosing the government's March 2020 request, noting that the company had blocked access to the requested 230 websites by serving a block page. Although a list of the blocked websites was not published, an OONI report confirmed the DNS-based blocking of 174 domains by Telenor Myanmar (AS133385). Most of these domains contain adult content, but as mentioned, many of them include news outlets as well.

On August 29, 2020, Telenor disclosed that the Myanmar government had issued another directive to block the website Justice for Myanmar and three related IP addresses based on Section 77 of the Telecommunications Law. The government's directive justified the blocking by asserting that the website in question was circulating fake news and rumors. According to international reports, the blocked website is for a campaign seeking to collect evidence to expose the vast business network that helps fund oppression in Myanmar.



တောင်းပန်ပါသည်။ ဤ URL မှာ မြန်မာနိုင်ငံ တွင်ကြည့် ရှု့နိုင် ခြင်းမရှိပါ။ လူကြီးမင်း သည် ပို့ဆောင်ရေး နှင့် ဆက်သွယ်ရေး ဝန် ကြီးဌာန (မြန်မာ နိုင်ငံ) ၏ ညွှန်ကြား ချက်အရ ပိတ်ပင်ထား သည့် စာမျက်နှာ ကို ဝင် ရောက်နေခြင်းဖြစ်သည်။

Sorry, this URL is not available from Myanmar. You have tried to access a web page which has been blocked as per directive received from the Ministry of Transport and Communications of Myanmar..

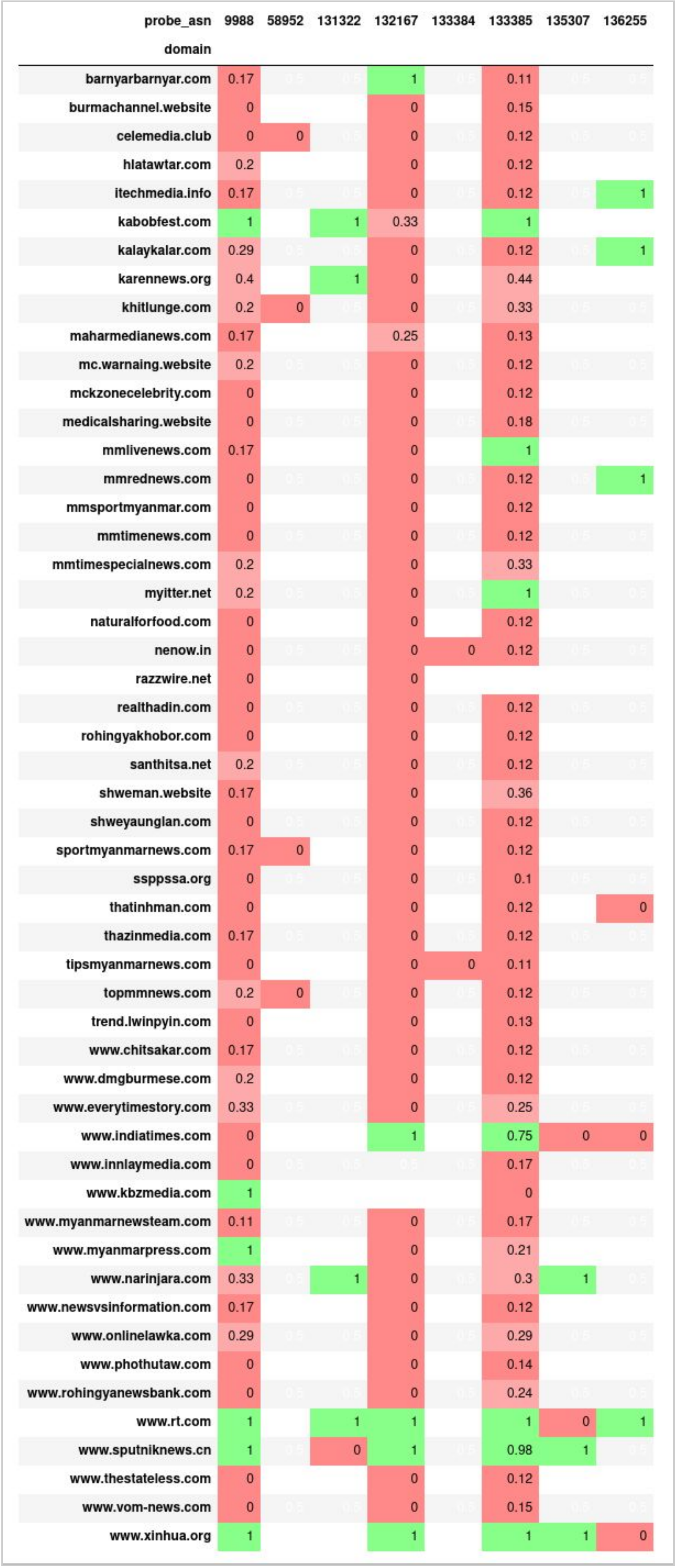
Image 1: *The landing page of a blocked website*

An OONI analysis conducted between January 1 and July 27, 2020, found approximately 200 URLs were blocked in Myanmar. Although the majority of these are pornographic websites, 41 media websites were also found to be blocked. The table below shows the network measurement data for blocked websites that are legitimate and trusted media sources, including Mandalay In-Depth News, KarenNews, Narinjara News, Development Media Group, and Voice of Myanmar. As reported by Qurium Media Foundation, these sites remained blocked for five additional months. OONI measurements conducted as part of this research study also show that Rohingya blogs such as RohingyaKhobor, Rohingya News Banks, and The Stateless Rohingya were blocked.

Domain	OONI measurements showing blocking
karennews.org	https://explorer.ooni.org/measurement/20200707T075819Z_AS132167_KU728VAR6AGfgGpp3nnfLAWUzUobajgrw8bitm8J4oboUjWO4p?input=http%3A%2F%2Fkarennews.org%2F
www.dmgburmese.com	https://explorer.ooni.org/measurement/20200716T100226Z_AS133385_aNTUv79L4c0dZmX7FEoECFCV6mUipCkDq5oDPcsznB6QQ4vhGV?input=https%3A%2F%2Fwww.dmgburmese.com%2F
www.narinjara.com	https://explorer.ooni.org/measurement/20200716T100226Z_AS133385_aNTUv79L4c0dZmX7FEoECFCV6mUipCkDq5oDPcsznB6QQ4vhGV?input=https%3A%2F%2Fwww.narinjara.com%2F
www.vom-news.com	https://explorer.ooni.org/measurement/20200716T100226Z_AS133385_aNTUv79L4c0dZmX7FEoECFCV6mUipCkDq5oDPcsznB6QQ4vhGV?input=https%3A%2F%2Fwww.vom-news.com%2F
rohingyakhobor.com	https://explorer.ooni.org/measurement/20200326T121415Z_AS9988_ECLvshPEDDxY2ytBrZJCTXy4uJDa16RclYiVq0mmN1jCXSKLrV?input=https%3A%2F%2Frohingyakhobor.com%2F
www.rohingyanewsbank.com	https://explorer.ooni.org/measurement/20200329T120520Z_AS9988_SMeWOedI5Y2ALXkUH0rdC6Fg2v4rVOEpRlauqGiho7UbVTBDge?input=https%3A%2F%2Fwww.rohingyanewsbank.com%2F
www.thestateless.com	https://explorer.ooni.org/measurement/20200326T121415Z_AS9988_ECLvshPEDDxY2ytBrZJCTXy4uJDa16RclYiVq0mmN1jCXSKLrV?input=https%3A%2F%2Fwww.thestateless.com%2F

Chart 1: *Blocked media websites (based on OONI data)*

Notably, the blocking of media websites varies across different networks in Myanmar based on how different ISPs choose to block different media sites. This variance is illustrated in the following chart.



probe_asn	9988	58952	131322	132167	133384	133385	135307	136255
domain								
barnyarbarnyar.com	0.17			1		0.11		
burmachannel.website	0			0		0.15		
celemedia.club	0	0		0		0.12		
hlatawtar.com	0.2			0		0.12		
itechmedia.info	0.17			0		0.12		1
kabobfest.com	1		1	0.33		1		
kalaykalar.com	0.29			0		0.12		1
karennews.org	0.4		1	0		0.44		
khitlunge.com	0.2	0		0		0.33		
maharmedianews.com	0.17			0.25		0.13		
mc.warnaing.website	0.2			0		0.12		
mckzonecelebrity.com	0			0		0.12		
medicalsharing.website	0			0		0.18		
mmlivenews.com	0.17			0		1		
mmrednews.com	0			0		0.12		1
mmsportmyanmar.com	0			0		0.12		
mmtimenews.com	0			0		0.12		
mmtimespecialnews.com	0.2			0		0.33		
myitter.net	0.2			0		1		
naturalforfood.com	0			0		0.12		
nenow.in	0			0	0	0.12		
razzwire.net	0			0				
realthadin.com	0			0		0.12		
rohingyakhobor.com	0			0		0.12		
santhitsa.net	0.2			0		0.12		
shweman.website	0.17			0		0.36		
shweyaunglan.com	0			0		0.12		
sportmyanmarnews.com	0.17	0		0		0.12		
ssppssa.org	0			0		0.1		
thatinhman.com	0			0		0.12		0
thazinmedia.com	0.17			0		0.12		
tipsmyanmarnews.com	0			0	0	0.11		
topmmnews.com	0.2	0		0		0.12		
trend.lwinpyin.com	0			0		0.13		
www.chitsakar.com	0.17			0		0.12		
www.dmgburmese.com	0.2			0		0.12		
www.everytimestory.com	0.33			0		0.25		
www.indiatimes.com	0			1		0.75	0	0
www.innlaymedia.com	0					0.17		
www.kbzmedia.com	1					0		
www.myanmarnewsteam.com	0.11			0		0.17		
www.myanmarpress.com	1			0		0.21		
www.narinjara.com	0.33		1	0		0.3	1	
www.newsvsinformation.com	0.17			0		0.12		
www.onlinelawka.com	0.29			0		0.29		
www.phothutaw.com	0			0		0.14		
www.rohingyanewsbank.com	0			0		0.24		
www.rt.com	1		1	1		1	0	1
www.sputniknews.cn	1		0	1		0.98	1	
www.thestateless.com	0			0		0.12		
www.vom-news.com	0			0		0.15		
www.xinhua.org	1			1		1	1	0

Chart 2: Blocking of media websites across ASNs in Myanmar between January 2020 and July 2020 (based on OONI data)

The chart above presents relevant measurement results for the domain of each blocked media website across eight local networks. Most of the measurements, however, were collected from the three networks: AS9988, AS132167, and AS133385.

The AS numbers included in the above chart correspond to the following Internet Service Providers (ISPs):

- AS9988 - Myanmar Posts and Telecommunications
- AS58952 - Frontiir Co. Ltd
- AS 131322 - Yatanarpon Teleport Company Limited
- AS132167 - Ooredoo Myanmar
- AS133384 - RedLink Communications Co., Ltd
- AS133385 - Telenor Myanmar
- AS135307 - Golden TMH Telecom Co. Ltd
- AS136255 - Telecom International Myanmar Company Limited

The red fields illustrate whether the tested domains were found to be blocked on the tested networks, while the green fields show whether the tested domains were accessible on those networks. The white/gray fields are used when there is absence of relevant data. The number 0 is used to signal cases where the tested domain was *always blocked*, while the number 1 is used for cases where the domain was *never blocked*.

A cursory review of the above chart demonstrates that most of the media websites were blocked on at least three local networks (although there is some variance in their specific blocking across networks). From a transparency standpoint, there is little clarity as to how many directives have been issued by the government, or how many specific sites are included in the directives. No list of blocked URLs has been officially published. As of August 2020, no report has been issued by the government or any ISP (other than Telenor Myanmar) regarding the blocked websites or related internet restrictions.

The complete list of the blocked news websites can be accessed here.

Notably, instant messaging and circumvention tools such as Tor, Psiphon, WhatsApp, Facebook Messenger, and Telegram were all found to be accessible in Myanmar throughout the testing period. The relevant measurements can be accessed by filtering the results here based by name.

Surveillance Capacity and Capabilities

The Telecommunications Law of 2013 allowed foreign telecommunication companies to enter the Myanmar market for the first time, resulting in a connectivity revolution. Unfortunately, however, no legal framework was in place at the time to protect individual privacy rights on the internet. The absence of such legal protections in the country enabled the government and military to decide whether or not to surveil or censor without true legal limitations or impediments on their behavior.

In turn, as discussed above, the NLD government formed the SMMT and the military employed tools such as Cellebrite. It also appears as though the Myanmar government has involved telecommunications companies in its surveillance activities. Telenor, which entered the Myanmar market pursuant to the passage of the Telecommunications Law of 2013, has published Annual Sustainability Briefings since 2014. These briefings cover issues related to anti-corruption, human rights, customer privacy, cybersecurity, climate impact and environmental management, and digital inclusion. According to the human rights-related Authority Request Disclosure Report - 2020, Telenor received 70 requests - of which 86% were received from the Post and Telecommunication Department of the MoTC. Telenor's briefings indicate that the law enforcement authorities were the ones requesting the data. Unfortunately, however, there is little additional transparency into this issue as no other ISPs provided reports on these types of requests.

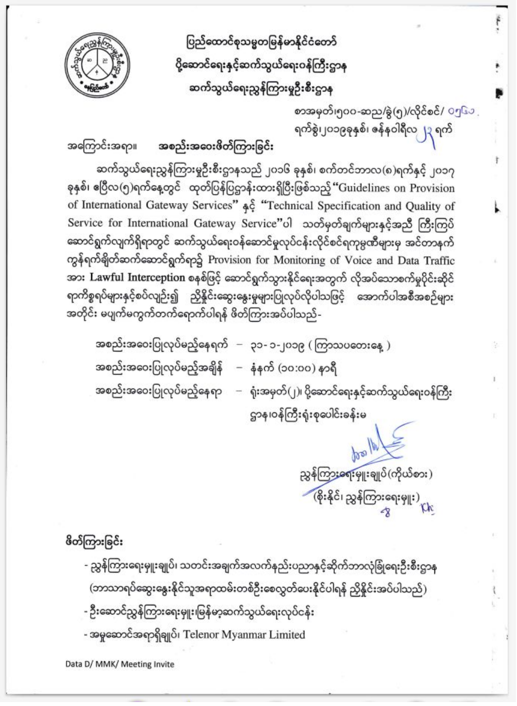
Given these troubling developments, advocates have been urging the government to adopt a rights-respecting Lawful Interception model to help maintain open access to the internet and ensure Myanmar does not become a surveillance state.

Government documents

In an effort to uncover surveillance practices within Myanmar, this research study sought out official government documents related to the issue. Two key documents were discovered.

Meeting to monitor voice and traffic data

The first leaked document (provided below) shows the MoTC called for a meeting on January 31, 2019, to discuss the necessary technical aspects of the Provision for Monitoring of Voice and Data Traffic as part of the Lawful Interception System according to the Guidelines on Provision of International Gateway Services and Technical Specification and Quality of Service for International Gateway Service. Companies invited to the meeting included Telenor, Ooredoo, MPT (a state-owned company), MyTel (a military-owned company), all companies licensed to provide network support services, all companies that are licensed to operate international gateways and the applicants, and all companies licensed for network services. The meeting generally discussed the monitoring of voice and traffic data in the country.



ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်
ပို့ဆောင်ရေးနှင့်ဆက်သွယ်ရေးဝန်ကြီးဌာန
ဆက်သွယ်ရေးညွှန်ကြားမှုဦးစီးဌာန

စာအမှတ်၊ ၅၀၀-ဆည/ခွဲ(၅)/လိုင်စင်/ ၀၅၆၁.
ရက်စွဲ၊ ၂၀၁၉ခုနှစ်၊ ဇန်နဝါရီလ ၂၃ ရက်

အကြောင်းအရာ။ **အစည်းအဝေးဖိတ်ကြားခြင်း**

ဆက်သွယ်ရေးညွှန်ကြားမှုဦးစီးဌာနသည် ၂၀၁၆ ခုနှစ်၊ စက်တင်ဘာလ(၈)ရက်နှင့် ၂၀၁၇ ခုနှစ်၊ ဧပြီလ(၅)ရက်နေ့တွင် ထုတ်ပြန်ပြဌာန်းထားရှိပြီးဖြစ်သည့် "Guidelines on Provision of International Gateway Services" နှင့် "Technical Specification and Quality of Service for International Gateway Service"ပါ သတ်မှတ်ချက်များနှင့်အညီ ကြီးကြပ်ဆောင်ရွက်လျက်ရှိရာတွင် ဆက်သွယ်ရေးဝန်ဆောင်မှုလုပ်ငန်းလိုင်စင်ရကုမ္ပဏီများမှ အင်တာနက်ကွန်ရက်ချိတ်ဆက်ဆောင်ရွက်ရာ၌ Provision for Monitoring of Voice and Data Traffic အား **Lawful Interception** စနစ်ဖြင့် ဆောင်ရွက်သွားနိုင်ရေးအတွက် လိုအပ်သောစက်မှုပိုင်းဆိုင်ရာကိစ္စရပ်များနှင့်စပ်လျဉ်း၍ ညှိနှိုင်းဆွေးနွေးမှုများပြုလုပ်လိုပါသဖြင့် အောက်ပါအစီအစဉ်များအတိုင်း မပျက်မကွက်တက်ရောက်ပါရန် ဖိတ်ကြားအပ်ပါသည်-

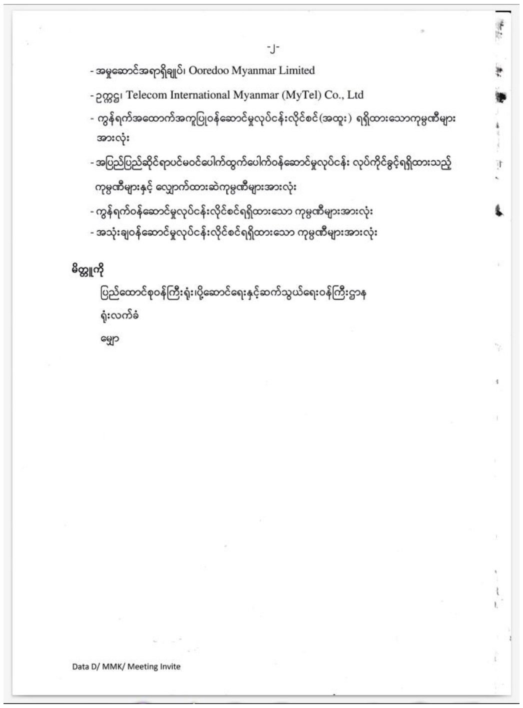
အစည်းအဝေးပြုလုပ်မည့်နေရက် – ၃၁-၁-၂၀၁၉ (ကြာသပတေးနေ့)
အစည်းအဝေးပြုလုပ်မည့်အချိန် – နံနက် (၁၀:၀၀) နာရီ
အစည်းအဝေးပြုလုပ်မည့်နေရာ – ရုံးအမှတ်(၂)၊ ပို့ဆောင်ရေးနှင့်ဆက်သွယ်ရေးဝန်ကြီးဌာန၊ဝန်ကြီးရုံးစုပေါင်းခန်းမ

ညွှန်ကြားရေးမှူးချုပ်(ကိုယ်စား)
(စိုးနိုင်၊ ညွှန်ကြားရေးမှူး)

ဖိတ်ကြားခြင်း

- ညွှန်ကြားရေးမှူးချုပ်၊ သတင်းအချက်အလက်နည်းပညာနှင့်ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာန (ဘာသာရပ်ဆွေးနွေးနိုင်သူအရာထမ်းတစ်ဦးစေလွှတ်ပေးနိုင်ပါရန် ညှိနှိုင်းအပ်ပါသည်)
- ဦးဆောင်ညွှန်ကြားရေးမှူး၊မြန်မာ့ဆက်သွယ်ရေးလုပ်ငန်း
- အမှုဆောင်အရာရှိချုပ်၊ Telenor Myanmar Limited

Data D/ MMK/ Meeting Invite



-၂-

- အမှုဆောင်အရာရှိချုပ်၊ Ooredoo Myanmar Limited
- ဥက္ကဌ၊ Telecom International Myanmar (MyTel) Co., Ltd
- ကွန်ရက်အထောက်အကူပြုဝန်ဆောင်မှုလုပ်ငန်းလိုင်စင်(အထူး) ရရှိထားသောကုမ္ပဏီများအားလုံး
- အပြည်ပြည်ဆိုင်ရာပင်မဝင်ပေါက်ထွက်ပေါက်ဝန်ဆောင်မှုလုပ်ငန်း လုပ်ကိုင်ခွင့်ရရှိထားသည့်ကုမ္ပဏီများနှင့် လျှောက်ထားဆဲကုမ္ပဏီများအားလုံး
- ကွန်ရက်ဝန်ဆောင်မှုလုပ်ငန်းလိုင်စင်ရရှိထားသော ကုမ္ပဏီများအားလုံး
- အသုံးချဝန်ဆောင်မှုလုပ်ငန်းလိုင်စင်ရရှိထားသော ကုမ္ပဏီများအားလုံး

မိတ္တူကို

ပြည်ထောင်စုဝန်ကြီးရုံး၊ပို့ဆောင်ရေးနှင့်ဆက်သွယ်ရေးဝန်ကြီးဌာန
ရုံးလက်ခံ
မျှော

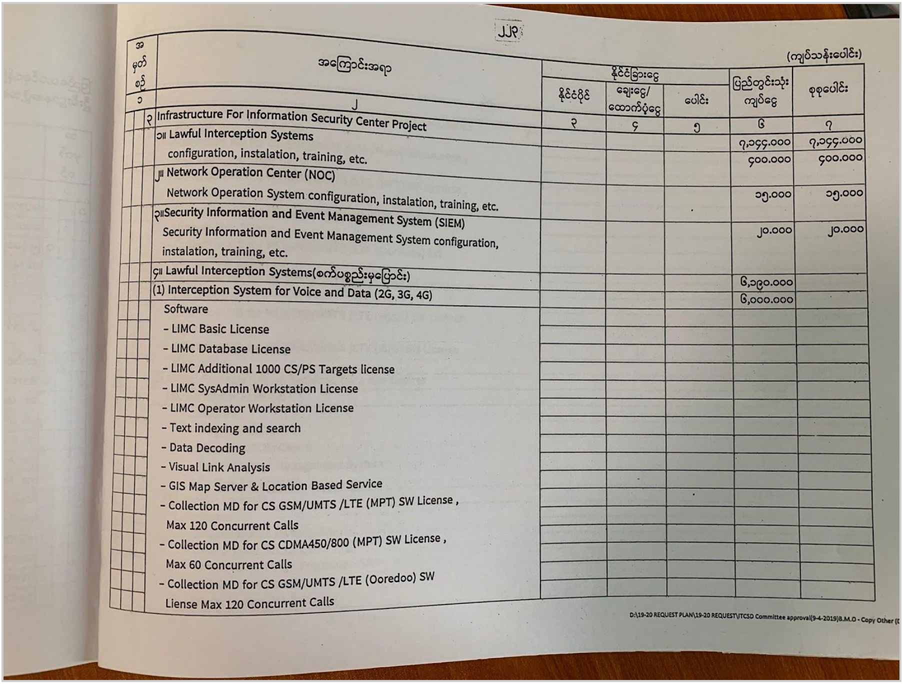
Data D/ MMK/ Meeting Invite

Image 2: *Order calling for a meeting to discuss the Provision of Monitoring of Voice and Data Traffic*

Civil society organizations in Myanmar, such as the Myanmar Centre for Responsible Business (MCRB), had previously welcomed that ETSI standards will be used for internet gateway facilities, and had recommended drafting Lawful Interception Regulations with rights-respecting characteristics. As of the timing of this study, however, Myanmar still lacks a rights-respecting Lawful Interception framework and the government continues to monitor the voice and traffic data of the people in Myanmar.

Creation of a Lawful Interception System

The second document uncovered by this research study indicates that, following the meeting discussed above, the MoTC allocated 6,190 million kyats (approximately 4 million USD) to implement a Lawful Interception System for 2019-2020 Financial Year. This figure came in addition to the approximately 4.6 million USD spent on the SMMT. Notably, even though the Lawful Interception System was proposed, as outlined above, Myanmar does not have a lawful intercept framework with the characteristics protecting human rights.

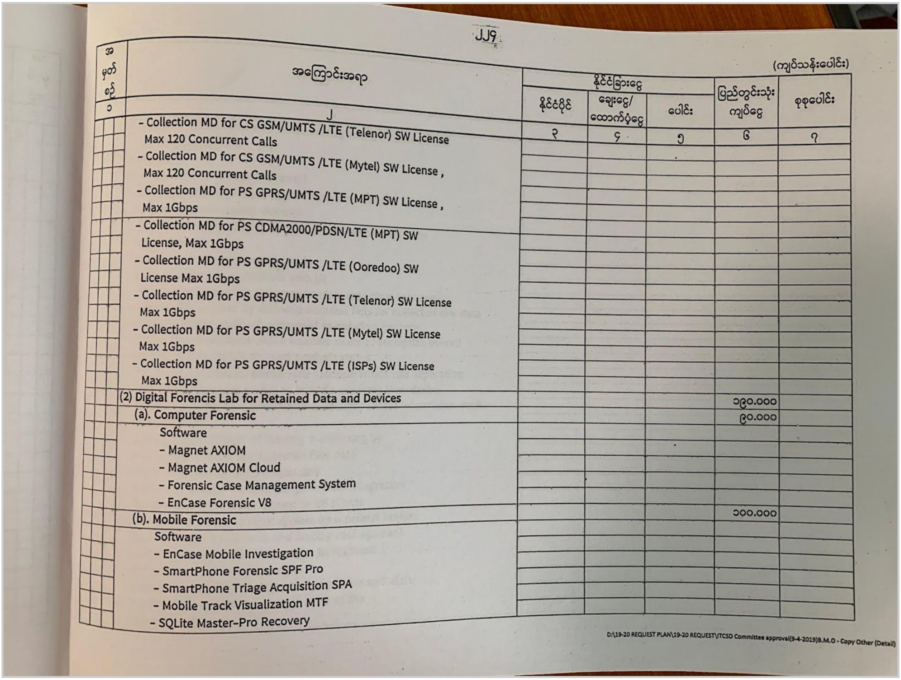


၂၂၃

(ကျပ်သန်းပေါင်း)

အမှတ်စဉ်	အကြောင်းအရာ	နိုင်ငံခြားငွေ			ပြည်တွင်းသုံးကျပ်ငွေ	စုစုပေါင်း
		နိုင်ငံပိုင်	ချေးငွေ/ထောက်ပံ့ငွေ	ပေါင်း		
၁	၂	၃	၄	၅	၆	၇
၃	Infrastructure For Information Security Center Project					
	၁။ Lawful Interception Systems				၇,၁၄၄.၀၀၀	၇,၁၄၄.၀၀၀
	configuration, instalation, training, etc.				၄၀၀.၀၀၀	၄၀၀.၀၀၀
	၂။ Network Operation Center (NOC) Network Operation System configuration, instalation, training, etc.				၁၅.၀၀၀	၁၅.၀၀၀
	၃။Security Information and Event Management System (SIEM) Security Information and Event Management System configuration, instalation, training, etc.				၂၀.၀၀၀	၂၀.၀၀၀
	၄။ Lawful Interception Systems(စက်ပစ္စည်းမှပြောင်း)				၆,၁၉၀.၀၀၀	
	(1) Interception System for Voice and Data (2G, 3G, 4G)				၆,၀၀၀.၀၀၀	
	Software					
	- LIMC Basic License					
	- LIMC Database License					
	- LIMC Additional 1000 CS/PS Targets license					
	- LIMC SysAdmin Workstation License					
	- LIMC Operator Workstation License					
	- Text indexing and search					
	- Data Decoding					
	- Visual Link Analysis					
	- GIS Map Server & Location Based Service					
	- Collection MD for CS GSM/UMTS /LTE (MPT) SW License , Max 120 Concurrent Calls					
	- Collection MD for CS CDMA450/800 (MPT) SW License , Max 60 Concurrent Calls					
	- Collection MD for CS GSM/UMTS /LTE (Ooredoo) SW Liense Max 120 Concurrent Calls					

D:\19-20 REQUEST PLAN\19-20 REQUEST\ITCSD Committee approval(9-4-2019)B.M.O - Copy Other (



၂၂၄

(ကျပ်သန်းပေါင်း)

အမှတ်စဉ်	အကြောင်းအရာ	နိုင်ငံခြားငွေ			ပြည်တွင်းသုံးကျပ်ငွေ	စုစုပေါင်း
		နိုင်ငံပိုင်	ဈေးငွေ/ထောက်ပံ့ငွေ	ပေါင်း		
၁	၂	၃	၄	၅	၆	၇
	- Collection MD for CS GSM/UMTS /LTE (Telenor) SW License Max 120 Concurrent Calls					
	- Collection MD for CS GSM/UMTS /LTE (Mytel) SW License , Max 120 Concurrent Calls					
	- Collection MD for PS GPRS/UMTS /LTE (MPT) SW License , Max 1Gbps					
	- Collection MD for PS CDMA2000/PDSN/LTE (MPT) SW License, Max 1Gbps					
	- Collection MD for PS GPRS/UMTS /LTE (Ooredoo) SW License Max 1Gbps					
	- Collection MD for PS GPRS/UMTS /LTE (Telenor) SW License Max 1Gbps					
	- Collection MD for PS GPRS/UMTS /LTE (Mytel) SW License Max 1Gbps					
	- Collection MD for PS GPRS/UMTS /LTE (ISPs) SW License Max 1Gbps					
	(2) Digital Forencis Lab for Retained Data and Devices				၁၉၀.၀၀၀	
	(a). Computer Forensic				၉၀.၀၀၀	
	Software					
	- Magnet AXIOM					
	- Magnet AXIOM Cloud					
	- Forensic Case Management System					
	- EnCase Forensic V8					
	(b). Mobile Forensic				၁၀၀.၀၀၀	
	Software					
	- EnCase Mobile Investigation					
	- SmartPhone Forensic SPF Pro					
	- SmartPhone Triage Acquisition SPA					
	- Mobile Track Visualization MTF					
	- SQLite Master-Pro Recovery					

D:\19-20 REQUEST PLAN\19-20 REQUEST\ITCSD Committee approval(9-4-2019)B.M.O - Copy Other (Detail)

Image 3: *The 2019-2020 budget for the MoTC*

It is possible that the "Lawful Interception System" referenced in the MoTC's budget might be referring to the system similar to CISCO's Lawful Interception System. According to the budget document and the CISCO's system, the possible capabilities are:

- Operation of Lawful Intercept Monitoring Centers.
- Text indexing and search: indexing the content of intercepted communications to make it easily searchable, e.g. a Google for the intercepted SMS, calls, metadata.
- Visual link analysis: monitoring the graphical depiction of the notes and links between them.
- GIS Map Server and Location Based Service: showing the physical location of the targets when various communications were made, likely using cell tower data/ triangulation.
- Intercepting 120 concurrent calls of the cellular service, GSM/ UMTS/ LTE and 60 concurrent calls for CDMA 450/ 800.
- Intercepting 1Gbps of the phone service, GPRS/ UMTS, CDMA2000/ PDSN, GPRS/ UMTS.

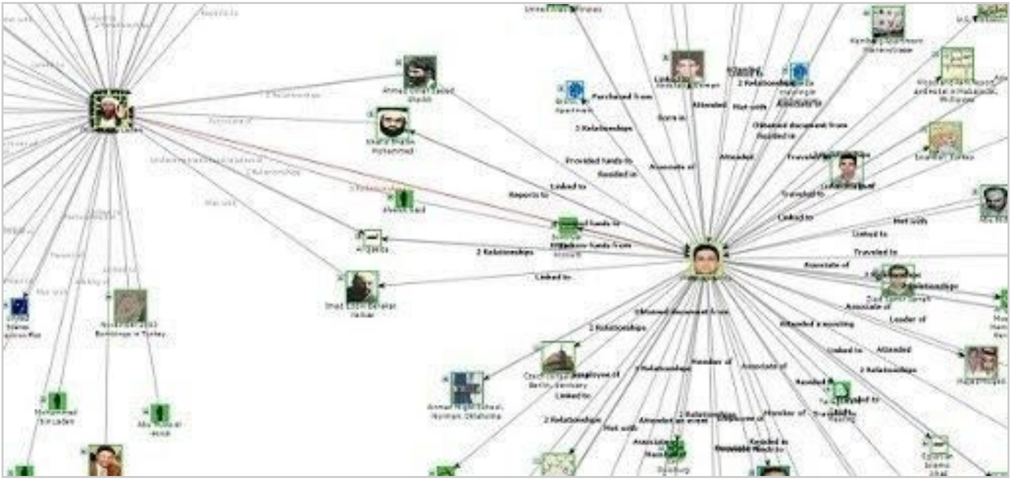


Image 4: *An example of the visual link analysis*

If Myanmar is to truly implement a proper Lawful Interception System, a key point of reference would be the ICT Sector-Wide Impact Assessment Executive Summary (SWIA), which is published by MCRB, the Institute of Human Rights and Business (IHRB), and the Danish Institute of Human Rights (DIHR). The SWIA includes recommendations on the characteristics of a rights-respecting model for Lawful Interception, including:

1. Prerequisites
2. Authorisation Processes
3. Oversight
4. The notification of individuals
5. Remedy
6. Transparency
7. Provision for Framework Review

The SWIA recommends that companies providing services to users should not be compelled to modify their infrastructure to enable direct surveillance that eliminates the opportunity for judicial oversight. The impact assessment also recommends that service providers should have the right to seek clarification or modification to a request which does not seem to follow domestic legal procedures (which, in turn, should incorporate internationally accepted human rights protections). Such recommendations should be accepted and followed by any Lawful Interception System in Myanmar.

Undisclosed documents

As part of the study, relevant calls for tender that were published on the authorities' websites were monitored and documented from September 2016 to July 2020. The goal of the monitoring was to document what types of equipment the authorities were purchasing. Most of the relevant tenders were from the MoTC.

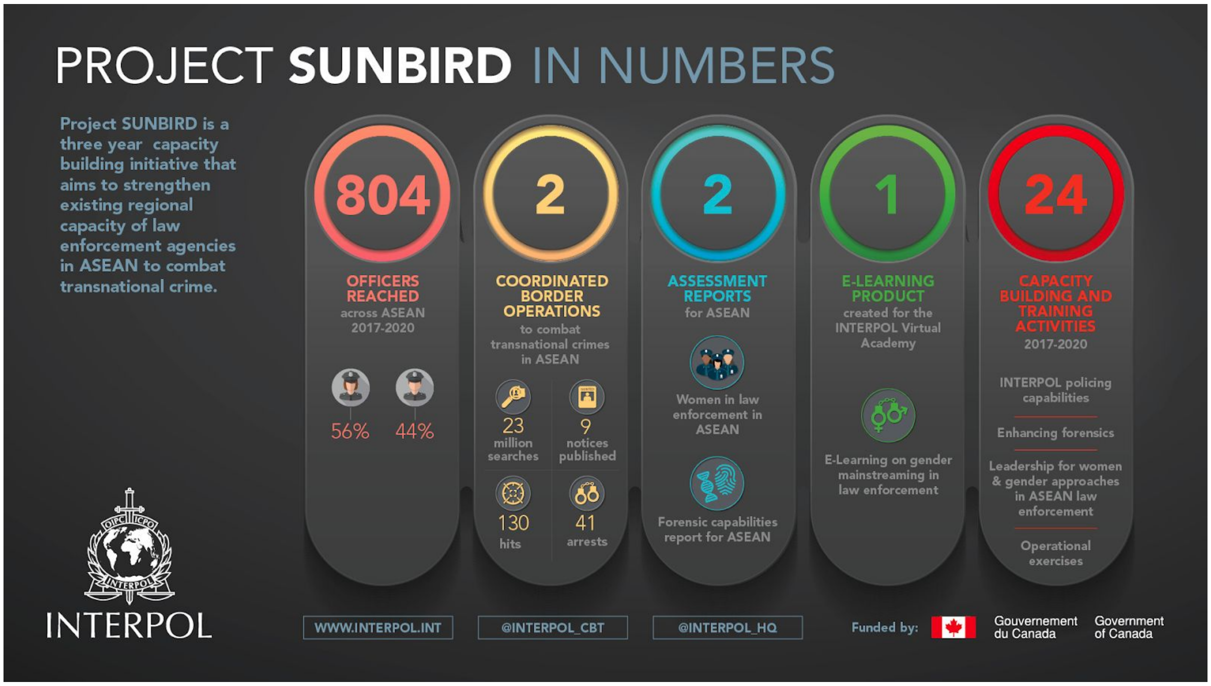
Notably, according to Article 64(a) of the Procurement Law, purchases related to national security do not need to go through the traditional procurement process (and therefore would not necessarily appear on the published list of tenders).

Police tactics

The police in Myanmar have the capability to surveil and seize devices and data. They have confiscated devices from human rights defenders, activists, and journalists and extracted information from the devices. As discussed, authorities confiscated the mobile phones of two journalists and used Cellebrite to extract data from the devices. The information extracted was later used to sentence the reporters to seven years in prison.

Notably, the government of Myanmar has received foreign support and assistance to help train and build the capacity of its police force. MyPol, an EU-based project started in 2016, supports Myanmar police reform in the areas of community policing, crowd management, crime investigation, and human resource management. Reporting also indicates that the Canadian government has provided financing through InterPol for police training and surveillance equipment to Myanmar and at least six other Southeast Asian countries with histories of human rights violations. The goal of the assistance is to help the police intercept irregular migrants and smugglers.

Through InterPol, Myanmar police receive support for projects, operations, and training. The projects Myanmar is involved with include: Project Relay, Project Trace, and Project Sunbird. Each project helps oversee various operations such as Operation Mandala and Operation Sunbird. Myanmar police also receive different types of support through InterPol's ASEAN Cyber Capacity Development Project (ACCDP). These projects and operations help address issues such as migrant smuggling, border security, cybercrime support, countering terrorism, and biometrics databases.


PROJECT SUNBIRD IN NUMBERS

Project SUNBIRD is a three year capacity building initiative that aims to strengthen existing regional capacity of law enforcement agencies in ASEAN to combat transnational crime.

***Image 5:** Project Sunbird data*

According to ACCDP, Myanmar police also receive Specialized Training through the project. Through practical training covering topics including digital forensics, malware analysis, cyber investigations and the Darknet, participants in the project improve their capabilities in data extraction and interpretation, cyber security, and online investigations. Although such tactics can be essential parts of proper police work, as addressed above there is evidence that the Myanmar police are using forensic and surveillance technology to extract data from individuals who are not criminals. More information regarding the training, operation, and support for Myanmar police can be found at Annex B.

Targeted groups

Public reports by Kaspersky indicates that Myanmar authorities have purchased malware and used it to target specific groups within the country. In response, this research study analyzed the devices and communications of at-risk individuals, as well as flagged phishing attempts and suspicious websites, in an effort to better understand the authorities' tactics.

Two main categories were addressed as part of this process: a security assessment via Emergency VPN and an assessment of tabloid websites on Facebook. Across eight months of analysis, no state-sponsored malware was found in either category. Unfortunately, no confiscated devices were able to be tested given that the devices were never returned from the authorities.

Security assessment via Emergency VPN

A security assessment via Emergency VPN was conducted across ten profiles (for individuals who focus on labour rights, minority rights, digital rights, human rights, peace process, freedom of expression) to investigate if their communications and/or devices were compromised by the authorities. If the communications or devices were compromised, further analysis was to be utilized to identify the methods and tools that were used by the authorities or any other groups.

Notably, no malware infection was detected on any of the devices that were assessed (it is possible that changing political situations can affect and change what specific groups are targeted by the authorities). Despite this, several medium and high risk events were found. Out of the ten profiles, four received high risks events and 1 received a warning. These risks can be categorized as described below.

Common high risk events include:

- Personal data being leaked via applications such as Joox Music, Candy Crush Jelly, B612, Photo Collage - Collageable, WeChat, or QQ.
- Suspicious connection attempts to IP addresses.

Common medium risk events include:

- Suspicious connection attempts to IP addresses.
- Information leaked via insecure HTTP requests.

Advertisement trackers were found for all ten profiles, with the number of trackers varying from 6 to 157 trackers. Emergency VPN recommendations were to minimize the number of applications showing advertisements on the phone, as well as using a privacy blocker browser to reduce the number of advertisements shown when browsing the web.

The complete list of risks can be seen at Annex C.

Assessment of suspicious Facebook network

Prior to the start of this research study, a monitoring organization in Myanmar identified a network of Facebook pages that was spreading disinformation to manipulate public opinion. Because other networks on Facebook have been used by the military in a similar manner, this study sought to examine whether the network in question was using malware to advance malicious actions by the authorities.

As part of this effort, the identified data set was provided to The Citizen Lab, which helped to investigate and analyze the network in April 2020. The Lab's analysis, however, revealed that the network's actions were commercially motivated. No explicit malicious payloads were detected in the slice of data that was investigated by the Lab.

Interview Findings

In addition to exploring the censorship and surveillance capabilities of the authorities, it is also important to understand the overall experience of individuals working in Myanmar on sensitive issues such as human rights, minority rights, and digital rights. This section of the research study therefore provides an overview of the project's interview findings, including personal experience with issues of safety, surveillance and censorship, and self-censorship. Interviewees also offered insights into future needs and challenges.

Out of 24 people interviewed, 29% identified as activists, 13% identified as civil society workers, and 13% identified as journalists. The remaining interviewees identified as an advocate, change maker, consultant, development worker, educator, explorer, human rights defender, peace builder, researcher, trainer, and writer. In general, participants in the study reported feeling unsafe both online and offline. These feelings come from encountering issues such as racism, harassment and intimidation, gender-based harassment, and violence in both spaces.

These findings are consistent with other related studies of surveillance in Myanmar. According to a report by Free Expression Myanmar, 62% of protesters in the country had reason to believe that they had been placed under surveillance after protesting. Of those surveyed, 48% had identified unknown persons watching or following them in the street after the protest, and 14% had identified signs that they were under electronic surveillance via their phones or online presence. Notably, women protesters were three times more likely than men to have identified signs of online surveillance.

Safety

Online safety

The vast majority (79%) of interviewees said they do not feel secure online. As the majority of these people have begun to use the internet to access information, mobilize communities, and coordinate advocacy efforts, the authorities' surveillance practices have also shifted into these online spaces. Primary online safety concerns include SIM registration, hacking, unlawful interceptions, and security on Facebook and other social media platforms.

Hacking attempts are commonplace for individuals in at-risk areas of work. Almost every participant reported receiving login alerts emails stating someone had tried to gain access to their accounts on Facebook. In addition, several of the individuals who worked on the peace process, conflict, and political content, reported receiving messages on their Gmail accounts saying "Government-backed attackers may be trying to steal your password." These messages were received in 2012, and then again in 2017 and 2018.

Online surveillance is reported to be widespread on Facebook (the use of which is omnipresent in Myanmar). Interviewees indicated that the police from the Special Branch of the Special Intelligence Department often create fake accounts and interact with them in ambiguous and difficult to understand ways. It also appears as though the police are monitoring the Facebook activities of outspoken individuals, as interviewees reported receiving intimidating calls within half an hour of posting content to Facebook.

Offline safety

Participants reported feeling less vulnerable offline as compared to online. Nonetheless, fears of offline intimidation, harassment, physical harm, and racism still existed. These concerns are inevitably tied to an individual's online presence.

Interviewees reported intimidation and surveillance increasing when they organize activities such as workshops or trainings outside the Yangon capital region. Police have shown up uninvited to these types of activities. In such instances, the authorities have joined the activities without asking for permission and later asked for personal information such as where the organizers are staying and their agenda.

Some of the participants, particularly the activists and journalists, have experienced having their family members, friends, and the partners intimidated by the police from the Special Branch. There have been several events where the police from the Special Branch have also visited the homes of activists or their parents and intimidated family members (asking for personal information such as what they do and their phone numbers).

Physical harm and threats to loved ones

At the beginning of the NLD government, many study participants felt safe. As time passed, however, these individuals started to feel different. Fears of being surveilled due to the nature of their work, as well as worries over the implementation of the SMMT became more common. Concerns over physical harm came to a head when U Ko Ni, a prominent member of Myanmar's Muslim minority and legal adviser for the NLD, was assassinated in January 2017. In the wake of the assasation, interviewees became far more aware of threats to their physical security.

Although participants generally reported feeling safer offline than online, a few still expressed significant fear of offline physical violence. This fear was also tied to concerns related to their friends and family's security. As one interviewee said, "They (the Special Intelligence Department of the police) also threaten friends and family. There have been a lot of cases and that the amount of pressure and the intimidation on the family is more concerning and stressful for me. It is even worse for the women activists. They would threaten via Messenger calls."

Gender-based harassment

One-third of the women activists who were interviewed reported, "We are being harassed relentlessly because we are women." The rest of the women indicated they were self-censoring by keeping low profiles from ultra-nationalist groups. This experience is common in Myanmar, where women are routinely harassed by pro-military groups and ultra-nationalist groups like MaBaTha. MaBaTha is an organization notorious for spreading anti-muslim sentiment across the country. Many of the women who counter hate speech on Facebook are monitored by MaBaTha and the pro-military groups. In turn, women have been harassed by having their Facebook pages flooded with comments, or their Messenger app inundated with inappropriate pictures.

Surveillance and Censorship

Surveillance threats and risks vary depending on location. In more rural areas, authorities exercise far broader - and more invasive - powers. Surveillance initially dropped when the NLD came to power in 2016. In the following years, however, surveillance levels have once again increased in Myanmar.

Most of the interviewees reported being surveilled by the authorities, primarily by the military and the police (especially the police from the Special Intelligence Department). Some of these individuals indicated it is possible that they are being surveilled due to the sensitive nature of their work. The majority of participants said the military has greater strategic surveillance capabilities than the NLD government. Many interviewees raised concerns about the need for user privacy, stressing the importance of gaining legal protection so that tech companies will respect and implement pro-user privacy policies.

Surveillance methods

In terms of technical surveillance methods, most of the participants raised concerns around the interception of phone calls, the extraction of data from confiscated devices (which some had witnessed or experienced), and the enforcement of SIM registration. Other concerns included state-sponsored malware, Wifi hacking, network traffic monitoring, account hacking, and the SMMT.

In terms of physical surveillance, most of the participants expressed concern about the authorities' massive use of human resources to conduct in-person surveillance. In the rural areas, interviewees reported that people are being harassed, assaulted, and abused. In certain situations, people are reportedly being arrested simply due to their ethnicity.

Self-Censorship

All the various forms of surveillance, censorship, and intimidation have a net negative impact causing interviewees to self-censor and limit their activities. Due to social media monitoring and surveillance, 45% of participants reported self-censoring to maintain a "low profile." Among those who engaged in self-censoring, 72% are women working on the peace process, human rights violation documentation, digital rights, and legal reform.

Women journalists also reported facing online attacks when covering sensitive issues. Attackers often post the journalists' personal information, or spread misinformation and publicly shame them on Facebook. Threats are primarily communicated on Facebook Messenger. Participants indicated that this type of intimidation is common for most activists (and has been the case for years). Accordingly, most of the interviewees have begun to self-censor their speech and activities on Facebook and other social media platforms.

On a related note, self-censorship has increased after the Gambia filed a case against Myanmar at the International Court of Justice (ICJ) regarding Myanmar's treatment of ethnic Rohingya Muslims. Since the filing of the case, Muslim human rights defenders in Myanmar said they are self-censoring online to avoid being attacked by NLD loyalists. Feelings of insecurity have increased as well in the wake of the ICJ hearings.

Looking to the Future

When looking to the future, many challenges and needs arise. These include the need for enhanced legal protections, the care of activists' psychological well-being, and the advancement of comprehensive digital safety.

Legal protection

Currently, many laws exist in Myanmar which can be used to harass or arrest activists and those who are critical of the government or military. Many of the participants therefore expressed concerns regarding the existing legal framework. For example, even though the Privacy Law is meant to protect the Myanmar people from state surveillance, the law has been heavily criticized due to its vague and overly broad provisions. As Free Expression Myanmar pointed out, Myanmar has no less than six criminal defamation laws (including the Privacy Law). These laws are routinely used to punish journalists, human rights defenders, and others who are attempting to hold the powerful to account. In the words of one of the participants, "My main concern is that the authority would and could use whichever law to file a case against us." This system - and the lack of legal protection it provides - must be addressed in the future.

Psychological well-being

Interviewees repeatedly brought up the need to take into account their psychological well-being. Prior to the NLD's assumption of power, public support existed for activists and journalists to uncover the injustices perpetrated by the military. Since the NLD came to power, however, pro-NLD supporters aggressively criticize activists and journalists if they attempt to hold the authorities accountable. These criticisms often get back to the families and friends of the activists and journalists. This can have a large negative impact on their psychological well-being, as family members will accuse them of being "traitors."

Some participants have been diagnosed with panic and anxiety disorders due to the stress of being intimidated, surveilled, and threatened (along with their loved ones). To make things better, most of the participants emphasized the need for a holistic approach where mental well-being is prioritized as much as physical and digital security. Activists and journalists outside of Yangon, who are at a particularly high risk and who have witnessed traumatizing events, stressed the need for long-term psychological support. In looking to the future, it is paramount for these needs to be acknowledged and addressed.

Digital safety needs

Comprehensive digital safety is a community-based (not individual) effort. Most of the participants expressed the need to expand digital safety not only to their organizations and colleagues, but also to their family and friends.

Individuals outside Yangon with limited resources face challenges with communications platforms, circumvention tools, emergency response, and a lack of connection with organizations working on digital safety support. For example, in the northern part of the country, activists and journalists are often forced to use WeChat (a Chinese messaging app) because the majority of people in the region use it. Increased access to more secure apps and affordable VPNs is needed to improve overall digital safety.

Conclusion

Censorship and surveillance are rising concerns in Myanmar under the NLD. Prior to 2020, internet censorship (such as the blocking of certain websites) was not a common tactic used by the government. Six months into the conflict in Rakhine, however, the NLD started shutting down the internet in townships where clashes were occurring. Soon media websites reporting on the conflict in Rakhine were censored. This research study helped illuminate some of the blocking that is ongoing (such as the website of a campaign collecting evidence to expose the business network funding oppression in Myanmar), but more work needs to be done. Little transparency from either the government or ISPs exists on the issue, as the list of blocked websites has never been made publicly available.

The majority of interviewees for this research study reported feeling less secure online as compared to offline. In light of recent government efforts like the SMMT, human rights defenders, activists, and journalists have started self-censoring themselves to avoid harassment from authorities. Even so, these individuals still face harassment, intimidation, racism, and surveillance in both the online and offline spaces.

It is of grave concern to see the government implementing a surveillance system in a country where no legal framework to protect people's rights exists. Without sufficient legal protection, there are immense concerns regarding government projects such as smart cities, a national ID system, and the use of artificial intelligence. Legal reform, in which all stakeholders can take part, is therefore needed to ensure new frameworks are compliant with international human rights and data privacy laws. In addition, newly bestowed legal protection must go beyond just Myanmar citizens to encompass minorities who are not being granted citizenship due to their religious or ethnic affiliations.

With regards to safety, digital security alone cannot be considered. Rather, it is essential to approach security and safety in a holistic manner where physical and psychological well-being are taken in account as well. Such an integrated security approach must also incorporate the needs of individuals as well as groups.

Looking to the future, the hope is that this study will serve as a stepping stone off which additional studies will be conducted. There are many other areas of interest that need to be explored, such as:

- Censorship
    - The Citizen Lab's test list needs to be reviewed and updated. While acknowledging the risk running the tools such as OONI, it is important to measure various forms of internet censorship, such as the blocking of websites, instant messaging apps, and circumvention tools to potentially serve as evidence of Internet censorship. Of particular note, it would be interesting to see how the blocking varies across the states and regions.
- Surveillance
    - The source of funding for the surveillance capacity of the police should be investigated. Learning more about which surveillance technology is being used, and documenting instances of its abuse, would be particularly useful.

Acknowledgements

I would like to thank Roya Ensafi for hosting me and making this project come alive. The project and its findings would not have been possible without OONI and their continuous support. I am also very grateful to Emergency VPN by Civilsphere Project, Access Now Helpline, and Jakub Dalek from Citizen Lab for their important contributions. Notably, this report would not be complete without the participation of the human rights defenders, researchers, journalists, and activists who shared their experiences and the participants who agreed to run the Emergency VPN in an effort to better understand Myanmar's surveillance and censorship landscape.

In addition, I would like to thank Ko Oo Zin and Ma Htaike Htaike Aung for reviewing this report and providing insightful comments and suggestions. I am indebted to John Stith from Learning Lab (Open Technology Fund) for the revision of the report. I am also grateful to Ma Khine Myat, Don Le, Rei Nakano, A, and Z for all the support they gave me throughout this journey.

Finally, I will always be grateful to the Open Technology Fund for this opportunity and Adam Lynn for his advice and support.

Annex A: Interview Questionnaire

1. What is the nature of your work?
2. How do you identify yourself--activist, researcher, civil society, journalist, etc?
3. Have you been surveilled by authorities?
    a. If yes, can you describe your experience?
    b. Do you have any evidence?
4. Have you been hacked before by the authorities?
    a. If yes, can you describe your experience?
    b. Do you have any evidence?
5. Do you know of any other methods they have used?
6. What do you think about the capacity/ capability to conduct surveillance?
7. Do you feel secure online?
8. Do you feel secure offline?
9. Do you have any other concerns regarding surveillance?
10. What are the challenges you face to keep yourself secure?
11. Do you have any current or future needs to follow you to feel more secure?
12. Is there anything else you would like to share?

Annex B: Training, operation, and support for Myanmar police

	Date and place	Issues	Countries involved	Dept involved
Project Relay [2]	September 2017, Colombo, Sri Lanka	migrant smuggling, border security.	Bangladesh, Bhutan, India, Myanmar, Nepal, Sri Lanka, Thailand.	Police, investigation, customs, immigration, INTERPOL National Central Bureaus (NCBs), frontline border units.
Operation Mandala [3] (Part of Project Relay)	2018	INTERPOL's policing capabilities and technical systems, migrant smuggling investigative skills and standard operating procedures for border management. INTERPOL's nominal and Stolen and Lost Travel Documents (SLTD) databases	Bangladesh, Bhutan, Myanmar, Nepal and Sri Lanka	
Project Trace [4]	2017-2020	skills, tools and methodologies needed in order to effectively gather and exploit information from online platforms, including social media, for counter-terrorism investigations	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam	National counter-terrorism units, intelligence and investigation officers from cyber units, and any other national agencies responsible for investigating and combating the use of Internet for terrorism purposes
Project Trace - Basic Training 1	February and March 2018, Bangladesh	countering the use of the Internet for terrorist purposes, analytical investigation methods	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam	Officers from cybercrime and counter-terrorism units and INTERPOL National Central Bureaus (NCBs)
Project Trace - Basic Training 2	January 2019, Siem Reap, Cambodia	one-week basic training session to counter the use of the Internet for terrorism purposes	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam	
Project Trace - Basic Training 3	October 2019, Manila, Philippines		Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam	Law enforcement officials

Project Trace - Advanced Training 1	July 2018, Hanoi, Vietnam,	Regional terrorism context, the online radicalization process, developing the skills to effectively gather and analyze information from online sources, including social media, Human rights, legal and gender considerations, evidence collection standards and open source and social media investigation techniques	Participants who attended the basic session	
Project Trace - Advanced Training 2	March and December 2019, Jakarta Centre for Law Enforcement Cooperation in Semarang, Indonesia		Participants who attended the basic session	
Project Trace - Advanced Training 3				
Global Complex for Innovation (IGCI)	2017	Specific cybercrime situations in each country. Additional cyber intelligence was also provided by China.	Indonesia, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam	Investigators from the invited countries, Singapore Police Force Trend Micro, Kaspersky Lab, Cyber Defense Institute, Booz Allen Hamilton, British Telecom, Fortinet and Palo Alto Networks
ASEAN Cyber Capacity Development Project (ACCDP)	2016 - 2018	A total of 15 training sessions and related meetings were conducted during the two years, bringing together more than 380 participants from across the region and more than 50 trainers and expert speakers from all over the world.	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam	
National Cyber Reviews (Part of ACCDP)	2016 - 2018	A National Cyber Review was conducted in each beneficiary country; this is a comprehensive assessment of a country's capability to prevent, detect and investigate cybercrime, looking at law enforcement capabilities as well as legislation. Following the review, a tailored report was produced outlining recommendations for enhancing the existing institutional, operational, legal and technical frameworks for dealing with cybercrime.	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam	
Specialized training (Part of ACCDP)	2016 - 2018	Practical training covered topics including digital forensics, malware analysis, cyber investigations and the Darknet. As a result, participants improved their capabilities in data extraction and interpretation, cyber security and online investigations.	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam	

Research seminars (Part of ACCDP)	2016 - 2018	a platform for law enforcement, academia, and the public and private sectors to discuss current cybercrime threats and trends, both globally as well as those more prevalent in Southeast Asia. Some 30 law enforcement officers across the ASEAN region shared experiences on national cyber efforts and challenges with their peers, researchers and experts from both the private sector and INTERPOL.	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam	
Sharing best practice workshop 1 (Part of ACCDP)	August 2017	A platform to exchange information and best practices for combating cybercrime. Processes and challenges related to identifying and obtaining digital evidence legally. Support was provided by instructors from the US Department of Justice.	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam	
Sharing best practice workshop 2 (Part of ACCDP)	2018	Scenario-based table-top exercise on multi jurisdictional challenges and sharing of best practices. The exercise was supported by instructors from the Hong Kong and Singapore Police Forces, while speakers came from both the public and private sector.	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam Extended to participants of 12 countries from South America, Africa, Asia and the Pacific	

Annex C: Emergency VPN Analysis

Risks Level	Description	Explanation
High	Information Leaked Via Insecure HTTP Requests	The mobile device is communicating without encryption (plain HTTP) with several websites. These insecure connections leak information about the user increasing the security risk of the user. The information leaked includes but is not limited to operating system type, operating system name and version, public IP address, and some of the applications installed. The public IP address is considered high risk sensitive information because it can be used to physically locate the user. We recommend uninstalling all applications that are not strictly necessary, and avoid opening links using the Facebook app. Use a VPN when using public and not trusted networks.
High	WeChat or QQ Application Leaks Data	The WeChat application connects to a WeChat servers (203.205.219.149, 203.205.219.208) on port 9000, sending important information about the device in clear text, not using encryption. The information leaked includes a unique user ID, device ID and current version. These values can be used to unequivocally identify the device in large amounts of data. We recommend uninstalling the WeChat application immediately.
High	Suspicious connection attempts to IP 203.205.146.46	The mobile phone performs multiple connection attempts to IP address 203.205.146.46 on ports 14000/TCP, 443/TCP, 80/TCP and 8080/TCP. The connections are never established, meaning that the phone is unable to transfer and exchange information with the server. This is highly usual in a mobile device.
High	Suspicious behavior associated with sandai.net	The mobile device is performing repetitive connections to a non existing domain 'res.res.res.res' on port 80. These connections are sent to multiple IP addresses. The data transferred seems to be encrypted. The IP addresses are associated with sandai.net, which has been tied to malicious applications. We recommend factory reset your mobile device to make sure this behavior stops.
High	Phone IMEI Leaked in Plain Text to Baidu Servers	The mobile phone communicates with Baidu servers using the HTTP insecure protocol, leaking device and personal information in the network without encryption. The information leaked includes IMEI, language, application, mobile phone type and version, operating system version, SDK, and others. This cannot be avoided unless the user stops using Baidu applications.

High	Information leaked to ooredoo.com.mm	The application Ooredoo Selfcare is communicating using the HTTP insecure protocol, leaking device and personal information in the network without encryption. The information leaked includes country, mobile carrier name, operating system, screen resolution, device model, application name, network type, network, and language among others. We recommend uninstalling or disabling this application immediately.
High	Joox Music Application Leaks Personal Data	The application Joox Music is communicating using the HTTP insecure protocol, leaking device and personal information in the network without encryption. The information leaked includes country, mobile carrier name, operating system, current phone orientation, device model, application name, network type, network operator, language, and gender among others. We recommend uninstalling this application immediately.
High	Joox Music Application Leaks Personal Data	The application Joox Music is communicating using the HTTP insecure protocol, leaking device and personal information in the network without encryption. The information leaked includes country, mobile carrier name, operating system, current phone orientation, device model, application name, network type, network operator, language, and gender among others. We recommend uninstalling this application immediately.
High	Photo Collage - Collageable Leaks User Data	The application Photo Collage - Collageable is communicating using the HTTP insecure protocol, leaking device and personal information in the network without encryption. The information leaked includes the operating system, application name, city name, GPS coordinates based on IP address, country, language, and internet connection type, among others. We recommend uninstalling this application immediately.
High	Pictures Leaked via Insecure Connections to myqcloud.com	We identified insecure connections to myqcloud.com on port 80/TCP using HTTP. These pictures seem downloaded by the user, and may be associated with the user or with close contacts of the user. There are clear faces visible on the pictures, which we consider a high risk. We recommend not using the service for exchanging personal data.
High	B612 - Beauty & Filter Camera Communicates Insecurely	The mobile device communicates with servers b6g-api.snow.me, log.snow.me associated with the photo and video application “B612 - Beauty & Filter Camera”. The application communicates using HTTP without encryption on port 80/TCP. These connections leak every use of the application, every click and action, the country of the user, how the user is connected to the internet. We recommend uninstalling this application immediately.

High	Candy Crush Jelly Application Communicates Insecurely	The mobile device is communicating with the server candycrushjelly.king.com using the insecure HTTP protocol on port 80/TCP. These insecure communications leak device and user information, including possible friends' names in Facebook, how the user is connected to them, and their profile pictures. We recommend uninstalling this application immediately.
High	Joox Music Application Leaks Personal Data	The application Joox Music is communicating using the HTTP insecure protocol, leaking device and personal information in the network without encryption. The information leaked includes country, mobile carrier name, operating system, current phone orientation, device model, application name, network type, network operator, language, and gender among others. We recommend uninstalling this application immediately.
Medium	Suspicious Connection to Server 119.28.109.138 port 8002	The mobile device is communicating with server 119.28.109.138 on port 8002. The communication is in a non standard port. The data transferred appears to be encrypted. The owner of the IP is Tencent, however we could not associate this specific behavior with any particular application. We recommend uninstalling all non-essential applications and perform this analysis again to make sure this behavior is no longer happening.
Medium	Suspicious domain name contacted: loc.map.baidu.com	There are multiple requests to the host loc.map.baidu.com. This host is related to multiple malicious applications. It could be an indicator of unwanted behavior in the mobile phone. We suggest factory reset the phone, and keeping applications installed to the essential.
Medium	Information Leaked Via Insecure HTTP Requests	The mobile device is communicating without encryption (plain HTTP) with several websites. These insecure connections leak information about the user increasing the security risk of the user. The information leaked includes but is not limited to operating system type, name and version, internet connection type, and some of the applications installed. We recommend uninstalling all applications that are not strictly necessary. Use a VPN when using public and not trusted networks.
Low	Information Leaked Via Insecure HTTP Requests	The mobile device is communicating without encryption (plain HTTP) with several websites. These insecure connections leak information about the user increasing the security risk of the user. The information leaked includes but is not limited to operating system type, name and version, public IP address, device type, and some of the applications installed. We recommend uninstalling all applications that are not strictly necessary. Use a VPN when using public and not trusted networks.

Low	Insecure Connections by PopcornTime Application	The device seems to have installed the PopcornTime application. This application connects to the domains upd-pct.info, popcorn time-update.xyz, popcorntime-upd.xyz, and others using the non-encrypted HTTP protocol on port 80/TCP. These connections leak the application installed, the operating system version OSX 10.15.4, and a user id among other information. This information can put the user at risk when sent unencrypted. We recommend uninstalling this application.
Low	Information Leaked Via Insecure HTTP Requests	The mobile device is communicating without encryption (plain HTTP) with several websites. These insecure connections leak information about the user increasing the security risk of the user. The information leaked includes but is not limited to operating system type, name and version, public IP address, and some of the applications installed. We recommend uninstalling all applications that are not strictly necessary. Use a VPN when using public and not trusted networks.
Low	STUN Connection with Amazon Server 52.77.231.85	The mobile phone communicates with the IP 52.77.231.85 on port 59835/UDP. This connection seems to use the STUN protocol, which is used nowadays for video calls. This STUN connection is likely associated with Signal, the secure messaging application. The connection is encrypted, however the STUN protocol leaks the public IP address of the user, in this case the VPN IP address of our University. Public IP addresses can be used to locate the approximate geographical location where the mobile phone is connected from. We recommend using a VPN when in public networks, or when the knowledge of the IP address needs to be protected.
Low	Not Encrypted Communications by WeChat QQ Music Application	The application WeChat Music, or the Music functionality of the WeChat application, communicates using HTTP without encryption. We identified more than 400 HTTP requests to WeChat Music servers. Each request leaks the device type and operating system version, and the activities of the user in the application (streaming music, which music, etc.). While this is not a high risk behavior we recommend to uninstall this application.
Low	Information leaked to Xiaomi servers	The mobile phone communicates with Xiaomi servers using the HTTP insecure protocol, leaking device and personal information in the network without encryption. The information leaked includes internet connection type, operating system and version, and country code, among others. This cannot be avoided unless the user changes mobile devices.

Low	Unencrypted Connections to Xiaomi Servers Leak Device Data	The mobile device is communicating without encryption (plain HTTP) with Xiaomi servers. These 232 encrypted connections leak the following data: device ID, SDKversion, app keys, applications installed, and others. Use a VPN when using public and not trusted networks.
Low	Insecure Connections by WeChat to QQ Servers	We identified 338 unencrypted HTTP connections to QQ servers. These unencrypted connections leak data, specifically: analytics of the user, session tokens, zone IDs, application being used, and others.
Low	Information Leaked Via Insecure HTTP Requests	The mobile device is communicating without encryption (plain HTTP) with several websites. These insecure connections leak information about the user increasing the security risk of the user. The information leaked includes but is not limited to operating system type, name and version, and some of the applications installed. Apple updates should not happen via HTTP. Make sure your device is correctly configured. We recommend uninstalling all applications that are not strictly necessary. Use a VPN when using public and not trusted networks.
Low	Information Leaked Via Insecure HTTP Requests	The mobile device is communicating without encryption (plain HTTP) with several websites. These insecure connections leak information about the user increasing the security risk of the user. The information leaked includes but is not limited to operating system type, name and version, internet connection type, and some of the applications installed. We recommend uninstalling all applications that are not strictly necessary. Use a VPN when using public and not trusted networks.
Low	Information Leaked Via Insecure HTTP Requests	The mobile device is communicating without encryption (plain HTTP) with several websites. These insecure connections leak information about the user increasing the security risk of the user. The information leaked includes but is not limited to operating system type, name and version, and some of the applications installed. We recommend uninstalling all applications that are not strictly necessary. Use a VPN when using public and not trusted networks.
Low	Information Leaked Via Insecure HTTP Requests	The mobile device is communicating without encryption (plain HTTP) with several websites. These insecure connections leak information about the user increasing the security risk of the user. The information leaked includes but is not limited to operating system type, name and version, and some of the applications installed. We recommend uninstalling all applications that are not strictly necessary. Use a VPN when using public and not trusted networks.

WARNING	Microsoft Products Communicate with US Government Owned Domains	The device has installed Microsoft Applications, possibly Microsoft Teams, that communicate with multiple IP addresses and domains associated with the US Government. This behavior is not malicious, and is common for some Microsoft Products. However the user should be aware that these connections are occurring and possibly user data is passing through and/or being stored on those servers.