Ground SAFE

Assessing the digital security needs and practices of human rights defenders in Africa, MENA, South Asia, and Southeast Asia.

#groundsafe

March 2021

OPTF

The Oxen Privacy Tech Foundation

ASL19

blueprint for FREE SPEECH

EngageMedia.org

ppmn. Indonesian Association for Media Development

This report was produced on the unceded land of Bunurong Boon Wurrung and Wurundjeri Woi Wurrung peoples of the Eastern Kulin Nation.

We acknowledge and pay our respects to their Elders past, present and emerging.

ACKNOW-LEDGMENTS

We are grateful to everyone who contributed to the findings, recommendations, and snapshots that are contained in this report. Names of individuals interviewed about the state of digital security in their countries have been omitted due to security concerns. We thank all interviewees and respondents for their time and candid feedback. Their invaluable contribution has ensured this report is informed from the ground up.

We thank our partners for their support and generosity in making introductions and sharing contact details of individuals we interviewed as part of the research process.

Project Partners

- **ASL19**
- **Blueprint for Free Speech**
- **EngageMedia**
- **Indonesian Association for Media Development**
- **Oxen Privacy Tech Foundation**

We’d especially like to thank two parnters who preferred not to be acknowelged due to safety concerns.

OPTF Report Production Team

Alex LINTON, Brendan WINTER, Cameron LEE, Christopher PAVLESIC, Connor BROWN, Lucy LOVEGROVE, & Sam DE SILVA.

CONTENTS

INTRO-DUCTION

Digital Security And Human Rights Defenders

Over the past two decades, journalists and activists have become dependent on the internet and digital platforms for communications, organisation, and the amplification of their critical work.

During its early days, the internet was seen as a liberating force which would usher in a new era of equality and freedom. It was open, not controlled by a single entity or government, and gave people permissionless communication with anyone else around the world. Journalists established platforms which published news and investigations that mainstream media may have otherwise ignored, and activists used email and online forums to plan campaigns and strategise on a global scale — creating partnerships and solidarity which were simply not possible before.

However, the open and accessible design of the internet also made it vulnerable, and there was a recognition that it was important to practice digital security — especially for those challenging authority and power.

Over the past decade, technologies that provided digital protection and enabled work to be conducted under a secure environment started to emerge. At the same time, training programs that promoted digital security practices for activists and journalists were being developed and conducted around the world by NGOs, media support organisations, and media institutions themselves.

Despite the work promoting and building capacity in digital security, conversations with human rights defenders (HRDs) and digital security practitioners suggest there are still significant gaps and challenges in ensuring that those defending democracy and human rights are safe from digital attacks.

We felt it was important to make deeper inquiries into the current state of digital security needs and practices of journalists and activists, to better understand the risks they face and how they were being addressed. We were chiefly interested in the effectiveness of training programs, digital security practices, and secure tools being used.

In June 2020, the Oxen Privacy Tech Foundation approached a number of our allies to assist with this research. The project partners were:

- ASL19
- Blueprint for Free Speech
- EngageMedia
- Indonesian Association for Media Development (PPMN)

Project partners assisted with the interview process, including making introductions and conducting interviews. Partners also provided input on survey and research design, assisted with translations and deployment of empirical surveys, and provided us with invaluable contextual insights and support.

We also identified and worked with key stakeholders using personal networks. Interviewees were recommended by colleagues and friends working with HRDs and civil society organisations, as well as through contacts made at events like RightsCon.

No formal funding was secured for the project — we all contributed our own time and resources to the effort. A list of those who contributed to the project can be found in the Acknowledgements section.

The majority of our research effort was dedicated to understanding situations and challenges faced by HRDs in countries with flawed democracies, authoritarian-style leadership, significant limitations on political rights and civil liberties, or a lack of independent institutions. However, to provide a more complete global context, we also obtained insights into countries that were perceived to have stronger democratic traditions.
We focused our research on HRDs working in South East Asia, South Asia, the MENA region, and East Africa, who had similarities in terms of their digital security needs and practices. However, we identified significant variance between and within these regions in terms of HRDs' capacities to counter censorship efforts and defend against digital attacks.

Approach

Our research approach involved conducting online empirical surveys and interviews with individuals who could provide insight into digital security needs and practices in their countries, as well as desk research to better understand the political and internet freedom contexts of the countries examined. While the empirical survey work was useful, the perspectives gleaned from interviews with representatives of civil society organisations, journalists, and digital security experts about the digital threats being faced offered deeper insights.

We had conversations with over 40 HRDs and digital security trainers about the digital security landscapes in 13 different countries, gaining insight into the particular challenges faced by people in each country. We also discussed mitigation strategies and how to best improve the capacity to protect and defend against digital attacks.

As part of this research, we have also created a set of regional and country snapshots. These snapshots provide a brief summary of the varied political and digital security contexts in the regions examined. Where possible, snapshots also feature insights and quotes from interviewees.

Neither this report nor the research completed in service of this report are intended to provide an exhaustive analysis of digital security needs and practices. Rather, our aim is to signpost obstacles and provide recommendations to improve the digital security capacity of journalists, activists, and HRDs.

We hope this report will be used to inform the work being done by secure tool builders, digital security trainers, and civil society organisations to counter the ever-increasing digital threats faced by HRDs.

Terminology

HUMAN RIGHTS DEFENDERS

Throughout this report, we use the term ‘human rights defenders,’ or HRDs, to describe people who work to protect human rights. This can include journalists, lawyers, activists, educators, judges, humanitarian and development workers, and others who peacefully accept, defend, and promote the Universal Declaration of Human Rights.[1]

DIGITAL ATTACKS

The term ‘digital attacks’ in the context of this report broadly describes technological means of undermining the work of HRDs. In this context, digital attacks can include attempts to install malware and spyware on computers and mobile phones, account takeovers, online harassment and hate speech, and the restriction of internet and communications access.

[1] United Nations Human Rights Office of the High Commissioner. *OHCHR | Who is a defender?*, https://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Defender.aspx (accessed September 20, 2020).

FINDINGS

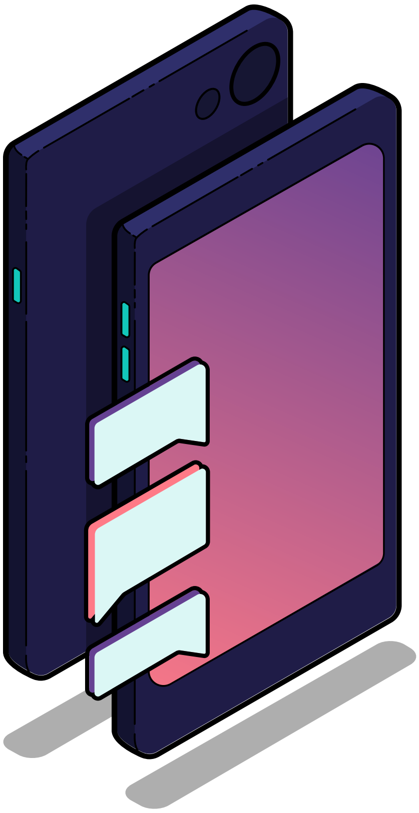
The tables have turned. We are now in an era where the apps and digital platforms HRDs use and depend on for their work are also used to exploit, attack, and undermine their efforts, with these attacks often exceeding HRDs' abilities to defend themselves.

While the HRDs we spoke with do have awareness of digital security risks, there is a lack of knowledge and capacity regarding tactics for minimising such risks. There was also a general sense of complacency across civil society organisations, and more work is required to establish internal policies and procedures which maximise digital security protections.

Many digital security trainers are aware of these issues; however, implementing effective solutions has been an ongoing challenge. Our findings point to a need for different methodologies to effectively strengthen digital security practices among HRDs.

High levels of use and dependency on social media, particularly Facebook, has exposed HRDs to not only monitoring and surveillance, but also public and online harassment from critics and organised troll armies. Many HRDs expressed feelings of helplessness when faced with such attacks, often resulting in their voices and work being silenced.

Ultimately, it is clear that there is significant room for improving the digital security practices of human rights defenders.



Digital Attacks, Cyber Laws and Secure Tools

The apps and services that make up the internet are now being used to attack changemakers, silence journalists, manipulate public opinion, and oppress citizens. Both democratic and more authoritarian governments are using laws related to national security and internet content regulation to justify online surveillance, arrest critics, and censor the internet. Social media is being used to generate hate speech against HRDs. There is a worrying trend of HRDs' accounts being either disabled or hijacked and used to generate fake news. This is then used by authorities to justify punitive action against these HRDs.

Secure communication is increasingly challenging and problematic due to over-dependence on popular messaging apps which have privacy and security vulnerabilities such as tying HRDs' mobile numbers to those they communicate with. In most countries, user identification details are linked to mobile phone numbers as part of the registration process for a mobile phone account, and it is extremely difficult to purchase 'burner phones' or Google-supplied mobile numbers without a credit card. Governments around the world are also enacting legislation that limits or weakens the use of encryption, further undermining private and secure communications.

The adoption and use of secure tech tools remains a challenge, with HRDs often preferring to use popular apps instead of purpose-built software that would provide them with a higher level of security. This is due to both usability and the access which popular apps provide to existing networks. For many activists, Facebook is the internet, and Messenger and WhatsApp — both Facebook-owned platforms — dominate when it comes to instant messaging, with WhatsApp perceived to be particularly secure and therefore used for sensitive communications.

There is a positive trend emerging — HRDs are increasingly using Signal for more sensitive communications. However local conditions, including bandwidth, cost of internet access, and the type of mobile device owned, shapes the ability of HRDs to practice digital security effectively. Many mobile providers sway users towards less secure platforms by offering low-cost data packages for specific digital platforms, such as Facebook.

Our research also found that there are stark digital security divides along geographical, generational, and socio-economic lines. Bandwidth quality varies by location, with outlying towns and regions often having poorer connections than urban areas. A secure tool such as Tor might work effectively in the city, but won't necessarily work in a regional town.

HRDs with higher levels of ICT literacy are more likely to adopt and use secure tech tools. However, feedback from interviewees suggests that veteran civil society and media leaders are less likely to take digital security risks seriously, put digital security policies in place, or provide training opportunities for HRDs – partly due to ignorance, and partly due to a sense of invulnerability.

Impacts on HRDs

Our research revealed four primary ways that HRDs and their work are being affected by digital attacks. These are:

1. Personal

Social media platforms and messaging app groups are being monitored, and those who are critical of government policies or speak out against rights violations are targeted, publicly and privately, with hate speech, and online threats such as doxxing. Some of these online threats incite physical attacks and lead to death threats, putting HRDs and their families in real, physical danger.

2. Reputational

When activists and civil society organisations advocate for issues or share findings and reports, they can face a barrage of disinformation — often from sources that position themselves as credible commentators but who are clearly aligned against change-makers, undermining the reputation of individuals and organisations. Activists and organisations can face scrutiny from authorities, and they often experience cyber-violence that can lead to offline violence.

3. Legal

Cyber laws are being used to quash freedom of expression and pursue critical voices on social media and websites. Posts that are deemed to break local content and censorship laws can result in the poster being arrested. There is also an increasing trend of social media and messaging app accounts being hijacked and taken over by unknown individuals, then used to generate libelous content or disinformation under the identities of HRDs, enabling authorities to arrest and prosecute these HRDs under cyber laws.

4. Infrastructure

The throttling or complete shutdown of internet services is increasingly being used to prevent activists from organising and sharing protest actions with the broader public, and to stifle information flow to and from the outside world. Device security is being compromised by the unintentional installation of malware through increasingly sophisticated phishing attacks, and social media and email accounts are being hijacked, blocked, and deleted. Civil society and media organisation websites are also vulnerable to being blocked, hacked, or flooded with DDOS attacks.

All interviewees indicated a high level of concern about digital threats, and believed the digital space for communications, organising, and change-making was becoming increasingly restrictive. The impact this has had on activism and journalism varied from person to person, as did the levels of anxiety and trauma they experienced. However, when it came to social media attacks, there was a general sense of helplessness and frustration — particularly with Facebook — for seemingly doing very little about hate speech and threats even after posts were reported.

All interviewees also indicated that while there was an increasing consciousness of digital security issues, the reality was that proper use of digital security best practices by HRDs and the organisations they worked with remained unacceptably low.

The main reasons given by interviewees for this low adoption and practice of digital security by HRDs were:

- Low awareness of digital security threats and their consequences
- Secure tools being difficult to use and often not working effectively

- Digital security training programs failing to engage and build capacity
- Organisation-level policies related to digital security being weak or non-existent

Devices, Apps, Connectivity, & Digital Platforms

We also gathered research about the operating environments of HRDs in terms of internet connectivity and the devices, apps, and digital platforms they used. This information, along with related trends and issues, is summarised below.

Mobile Devices

The use of mobile phones is now more prevalent than the use of desktops and laptops. Our research indicates that the majority of HRDs use Android mobile devices, with price being the main deciding factor for choice of operating system and model. Those who work for international organisations or in the diaspora often use iPhones.

A number of the HRDs and digital security trainers we spoke with understood the inherent security risks of Android phones — especially the low-cost models they dubbed “China phones” that come with customised versions of Android and which typically can’t be updated to the latest operating system version. While there are low-cost Android devices that can be updated, knowledge about these models appears to be lacking, and these devices can be difficult to obtain in the countries this report focused on.

Messaging Apps

Our research indicated that WhatsApp is the most widely used messaging platform by HRDs in the regions we examined. Facebook Messenger is also popular. Many HRDs we spoke with knew that the messaging apps they used could make them vulnerable, but were reluctant to give them up due to the convenience these apps offered, and the fact that all their contacts were already using them.

Importantly, HRDs are increasingly recognising the need for secure messaging, and are slowly shifting to more secure platforms such as Signal for conversations they deem more sensitive.

WhatsApp and Telegram remain popular due to their ease of use and group-based messaging. Telegram in particular is lightweight, doesn’t take significant storage space on mobiles, and allows very large groups. However, trust levels for Telegram fluctuate between HRDs.

Social Media Platforms

HRDs use Facebook both on a personal level and for their public activism. Many HRDs we interviewed did not have separate accounts to keep posts related to their personal lives separate from their work. Most acknowledged that online harassment was rampant on social media platforms, but stated that they felt disempowered and were unsure what could be done about it.

Social media surveillance is also on the rise. Interviewees expressed concern about the increase in state-sponsored cyber armies conducting surveillance, backed by legislation allegedly intended to protect national security and prevent cyber-crime. We were also told of concerns that social media accounts can be taken over and used to post fake or libelous material, resulting in HRD accounts being shut down by social media platforms. There was an awareness[2] of using two-factor authentication to protect accounts, but the practice has not been broadly adopted by HRDs.

Email

The rise of instant messaging apps has reduced the use of email, but it remains an important tool for more established HRDs and their organisations.

Gmail dominates the email landscape, and social media accounts are often established using Google accounts. However, HRDs who are more informed about email security, and those who are more vulnerable, are starting to use Protonmail. The use of PGP, a strong encryption system, was extremely low among respondents, with the vast majority of surveyed HRDs stating they did not know how to use it or that it was too difficult. Some also indicated that it was hard to use PGP on their mobile devices.

Data Storage

The secure storage of sensitive information was a major challenge faced by interviewed HRDs.

Many used messaging apps to store documents, with messaging apps being the primary method of receiving documents. However, they understood this wasn’t an ideal practice. Google Drive was also a popular choice for storing information, and Google Docs was the main choice for document collaboration. HRDs who worked in offices were often reliant on inhouse file servers, where all documents were centrally stored.

The use of file or folder encryption tools such as Veracrypt was extremely low, and many HRDs indicated that they did not have a secure way to store sensitive documents and data.

Mobile Operators

Mobile and telecommunications operators are the gateway for HRDs accessing the internet, and are therefore critical players in the safety and digital security of HRDs. In many surveyed countries, mobile operators are subservient to the government, either because operators are state-owned, or because they must maintain a positive relationship with government officials and authorities in order to operate. In practice, this means that internet shutdown orders will be carried out without question and that mobile and telecommunications operators will comply with informal requests for data about HRDs using their services.

Mobile operators also influence the adoption and use of secure tools by HRDs by bundling apps. WhatsApp and Facebook, for example, are often bundled together as part of mobile subscription or data packs, incentivising their use by making that bandwidth free, compromising the principle of net neutrality.[3] The use of Signal, on the other hand, incurs normal bandwidth charges, and our research indicates this is a key inhibiting factor to the adoption of Signal by HRDs on low incomes.

[2] It should be noted that SMS-based two-factor notification may increase vulnerability; however most social media accounts provide app-based 2FA.

[3] Net neutrality is the principle that all internet traffic should be treated in the same way by service providers: no traffic should be prioritised, excluded from data caps, artificially limited, or otherwise given artificial advantages or disadvantages over other similar traffic.

RECOM-MENDATIONS

These recommendations are intended for internet freedom and digital security advocates, civil society and non-government organisations, secure tool builders, and donors and investors who are committed to improving the digital security awareness and practices of HRDs around the world.

Improving digital security practices and the use of technologies that protect HRDs and their work will require a coordinated, collaborative, bottom-up approach. Importantly, there is a need to address the extremely high use of mobile devices by HRDs — training programs and initiatives must cater to this. It is also critical that local contexts are taken into careful consideration when building secure apps and designing training programs to improve the awareness and practice of digital security HRDs.

Increase awareness of digital threats and vulnerabilities

A common language is needed to describe threats, vulnerabilities, and mitigation strategies

We need to move beyond generic terms such as ‘hacking’ and ‘shutdowns’, and be more specific about terms such as ‘end-to-end encryption’. A shared understanding of terminology and language by HRDs and the digital security ecosystem will allow for more precise descriptions of digital threats and more specific mitigation strategies. Importantly, training materials and secure tools need to be translated, localised, and regularly updated.

Documentation of digital security incidents faced by HRDs must be improved

The way digital attacks are tracked and documented is fragmented, and there is a need for a more comprehensive and inclusive approach. It is important to ensure that countries and locations that are not trending on the agendas of donors and NGOs are also covered in the documentation process. A standardised, open data approach that can be easily replicated by local organisations will produce an improved understanding of the threat landscape, and allow for useful comparisons across locations to determine where resources need to be allocated. It will also provide improved ‘market knowledge’ so secure tech builders and digital security training providers can better focus on needs and target their solutions and programs for specific threats and local conditions.

Increase media stories and public discourse about digital attacks targeting HRDs

The number of digital attacks aimed at HRDs and their work is increasing, as are restrictive laws and other attempts to obstruct digital security. More effort needs to be made to inform journalists about digital security threats and their impacts on HRDs and democracy. Local organisations should also facilitate cross-community events that involve the technology and legal communities in order to increase awareness of the dangers of digital attacks and how to minimise their impact.

Build secure tech tools and apps that work effectively

Improved analysis and understanding of the needs of HRDs in their local context

Secure tech builders need to improve their efforts to understand the problems faced by the HRD community. Ideally, tech builders should spend time in the field to better understand the requirements, workflows and conditions of HRDs. However, partnering with local CSOs and allocating sufficient resources for design ethnography would also contribute to the vital understanding of local needs and contexts. Investors and funders of secure tech tools should ensure their technology partners undertake a comprehensive needs analysis to inform the design and build process.

Localise for language

Secure tech tools must be made available in languages other than English. Multi-lingual support should be incorporated as part of initial rollouts, especially given that the majority of users who require secure tools are not from countries with English as a primary language. Instructional guides and documentation for secure tools should also be localised to ensure users are fully aware of those tools' functionality, features, and potential drawbacks.

Establish user-testing and feedback groups that represent the diversity of HRDs

Secure tech builders should adopt a comprehensive and standardised testing and feedback methodology that involves target end-users in the environments in which they will be using the tools. It is also important that the tools are tested by a diverse cross-section of the HRD community — not just those who are tech-savvy or tend to be early adopters. This should be a requirement made by investors and grant bodies who fund secure tool development.

Be transparent about the weaknesses and functionality gaps of tech tools

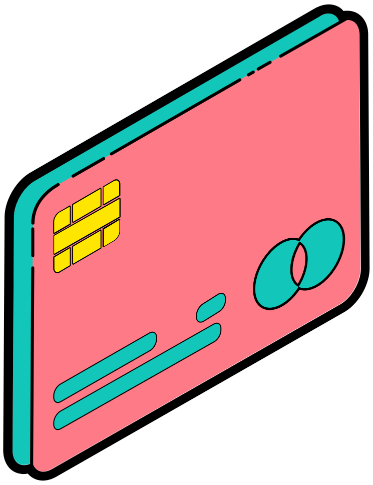
There are known issues with some secure tech tools that have not been clearly communicated to digital security trainers and HRDs. It is important that positive benefits and features, as well as potential weaknesses and vulnerabilities, be disclosed to users. Tor, along with many VPNs, for example, works well in high-bandwidth environments, but doesn't function effectively in low-bandwidth contexts. Tor traffic, and other forms of encrypted traffic, can also be detected by malicious actors monitoring network activities.

Diversify and decentralise the design and creation of secure tools

There is a need to foster and support secure tool builders outside of the US and Europe. South and Southeast Asia show potential for world-class technology capacity that could be harnessed to produce tools that protect and promote digital security. Investors and funders should make greater efforts to support tech teams outside of the US and Europe, and should look beyond their established recipients.

Identify new sources of funding and investment

The secure tool building community relies heavily on international NGO, government, and philanthropic funding to enable them to create and deploy secure tech and internet freedom technologies. As these funding pools dry up, new business models and funding sources need to be identified, including ethical and sustainable revenue streams that won’t compromise the intent of the tools being built. Criteria should be established to ensure the suitability of funding sources, to minimise scenarios where the integrity of secure tools is compromised due to interference or reputational damage by or to funders.



Improve digital security training and practice

Real and relatable examples of digital threats and attacks are needed

Unfortunately, there is an attitude of "it won't happen to me" among many HRDs and civil society organisations. To counter this, contextualised examples of real digital threats and attacks that are relatable to specific human rights and civil society communities should be incorporated into training curricula. Further, practical demonstrations that highlight vulnerabilities and data breaches will help HRDs appreciate the need to practise effective digital security.

Digital security training programs must be localised and led by local trainers

A greater commitment is needed by international organisations and donors to build digital security training expertise at the local level, and empower trainers to design and deliver programs in local languages and in a style and approach that engages local HRD / CSO communities. Our research indicated that participants felt examples and case studies provided in training programs were not relevant to them, and that involving local trainers in the curriculum design process and delivery along with conducting pre-training risk assessments on participants, would help address this issue.

Incorporate tool practice within training programs

Training programs must include dedicated time for participants to test out and practice using the secure tools being discussed. This may require programs to have more focused learning objectives, and target specific groups of participants with similar risk profiles and levels of ICT experience. Training programs must also include an assessment process to validate that participants can indeed use the secure tools being discussed as intended and with confidence.

Training programs must be designed to engage the target participants

Trainers must spend more time understanding and evaluating the digital security needs and ICT literacy of participants, and programs must be designed to engage and meet the needs of those who will be participating. There should also be flexibility in how training programs are delivered. Trainers should consider workplace-based workshops, or spreading curriculums over longer periods and delivering them outside of work hours so that participants who must work can also attend. Women-led programs designed to address the unique risks faced by women should be delivered at times and in environments that enable and encourage their participation. Likewise, the same considerations should be given to at-risk and marginalised groups.

Enhance organisation-level digital security practices

Inform management and board members of civil society organisations about digital threats to their work

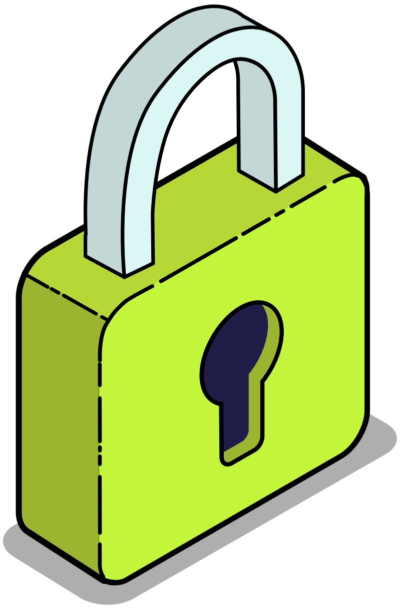
High-level information sessions and workshops aimed at senior management should be developed by digital security training organisations, and donors and other stakeholders should reinforce the importance of improving digital threat preparedness. Management buy-in is critical to enable and empower staff members to attend digital security training programs during work hours and to provide the necessary resources to strengthen both individual and organisational digital security. This buy-in could also enable training programs to be delivered in-house for all staff, including management.

Provide organisations with digital security procedures and policy templates

Many civil society organisations have procedures related to travel and physical security, but are underprepared when it comes to digital security. Robust digital security procedures and policies would ensure management and staff have the necessary guides to protect themselves and their organisations from digital threats, and would also help create a positive culture around digital security.

Digital security compliance as a prerequisite for donor funding

Grant applicants must prove their ability to meet financial compliance requirements, and should have to demonstrate their digital security capabilities in the same way. This would protect grantee organisations as well as donors and other partners from digital attacks, and would contribute to sector-wide compliance with digital security standards. Instead of ruling out grant applicants who lack digital security capabilities, donors should use this opportunity to provide the requisite support and knowledge to build capacity.

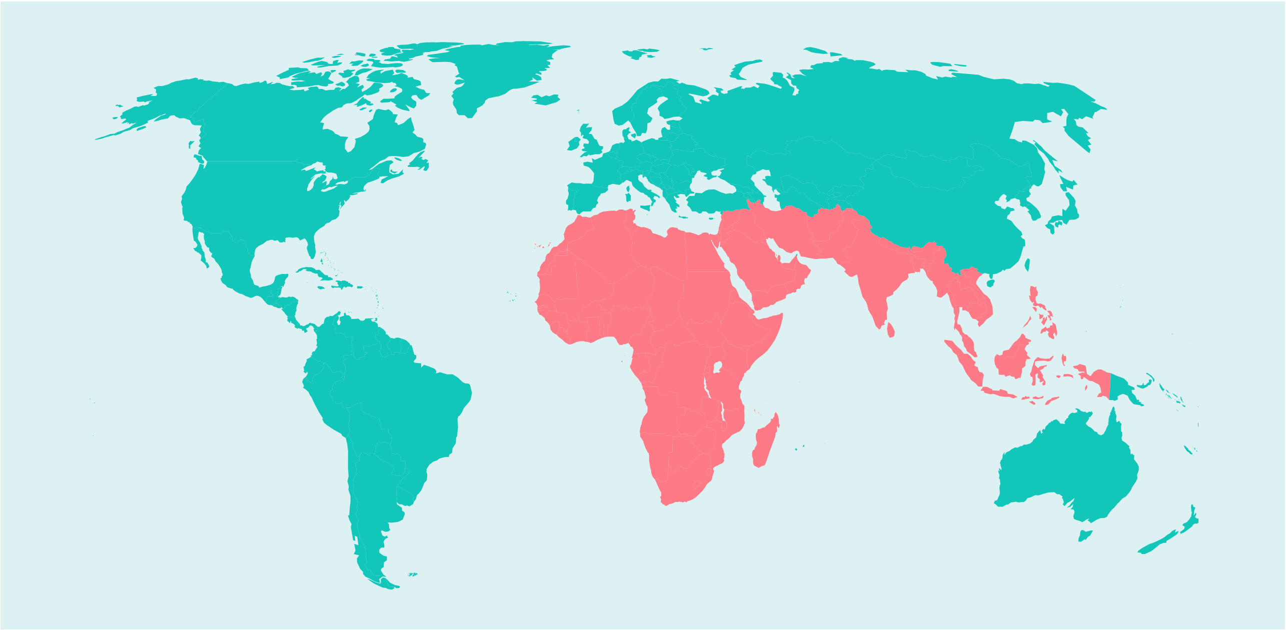


SNAP-SHOTS

This section contains high-level regional and country snapshots, highlighting the recent political history and context, and the state of internet freedom that HRDs are operating in.

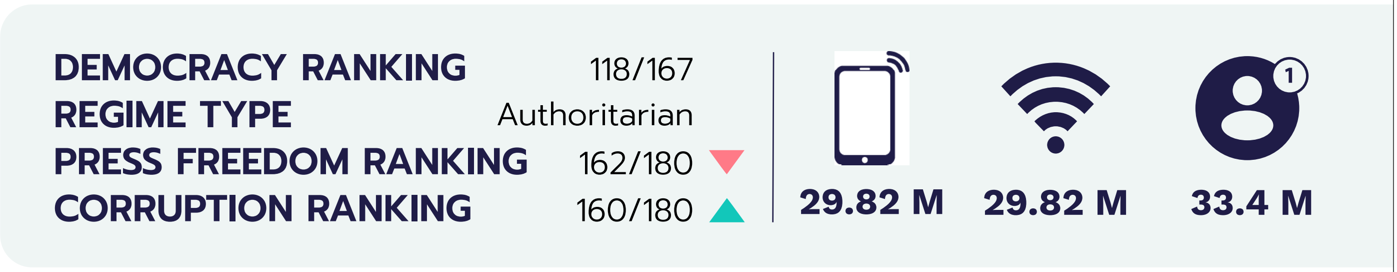
The quotations we have included — which have not been attributed due to safety concerns — are voices from the ground that help us better understand both the local situation, and the frustrations and concerns felt by people working in digital security and defending human rights.

These snapshots foreground the significant amount of work needed to strengthen digital security practices among HRDs, and the importance of localisation when delivering capacity-building programs. The snapshots also highlight the ways in which cyber laws are increasingly being used to target critical voices, and the importance of implementing more multidisciplinary approaches to promoting and strengthening digital security and digital rights.



This map infographic is stylised and not to scale. It doesn't reflect the legal status of any country or territory or the delineation of any frontiers. CREDIT: World map SVG taken from simplemaps.com

Understanding the snapshots statistics bar



DEMOCRACY RANKING	118/167
REGIME TYPE	Authoritarian
PRESS FREEDOM RANKING	162/180 ▼
CORRUPTION RANKING	160/180 ▲

29.82 M 29.82 M 33.4 M

DEMOCRACY INDEX RANKING

Democracy rankings are taken from the Democracy Index 2020[4] by The Economist, which ranks countries from highest (1) to lowest (167).

REGIME TYPE

Regimes are classified as "Full Democracies," "Flawed Democracies," "Hybrid Regimes," or "Authoritarian Regimes" as per the Democracy Index 2020.[5]

PRESS FREEDOM INDEX RANKING

Press freedom rankings are taken from the 2020 World Press Freedom Index[6] by Reporters Without Borders, which ranks 180 countries from highest (1) to lowest (180).

CORRUPTION PERCEPTIONS INDEX RANKING

Corruption perception rankings are taken from the Corruption Perceptions Index 2020[7] by Transparency International, which ranks 180 countries based on "their perceived levels of public sector corruption" from "very clean" (1) to "very corrupt" (180).

Where possible, ranking increases or decreases compared to the previous year have been indicated with a green-upwards pointing triangle (increase) or red downwards-pointing triangle (decrease).

MOBILE CONNECTIONS

This symbol indicates the number of mobile connections in a country.

INTERNET USERS

This symbol indicates the number of internet users in a country.

SOCIAL MEDIA USERS

This symbol indicates the number of social media users in a country.

"M" denotes "Million," and "B" denotes "Billion." Data for internet, social media users, and mobile connections was taken from DataReportal.[8]

● ● ● ●

[4] The Economist Intelligence Unit, "*Democracy Index 2020: In sickness and in health*," 2021, https://www.eiu.com/n/campaigns/democracy-index-2020/.

[5] Ibid.

[6] Reporters Without Borders, "*2020 World Press Freedom Index*," https://rsf.org/en/ranking.

[7] Transparency International, "*Corruption Perceptions Index 2020,*" https://www.transparency.org/en/cpi.

[8] DataReportal, "*Digital 2021: Local Country Headlines*," https://datareportal.com/reports/digital-2021-local-country-headlines.

Africa

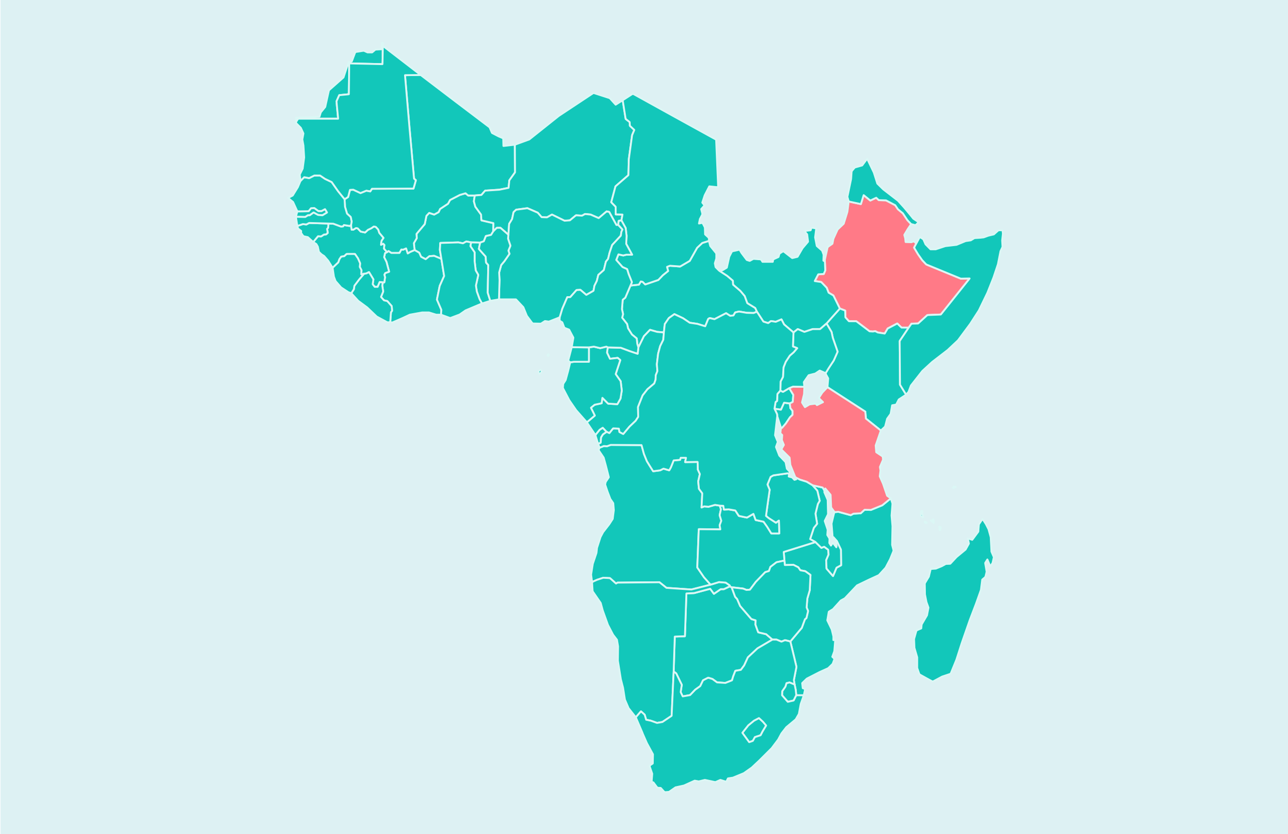
In recent years, some of Africa's longest-standing dictators have lost their grip on power. This is largely attributed to widespread peaceful protests that have united people across ethnic, religious, and economic lines, reducing the impetus "for security forces to repress or exploit divisions among them."[9]

However, Africa's struggle for democratic transformation continues, with authoritarian governments tending to enact draconian measures – especially in relation to freedom of expression.

Internet penetration levels are rapidly increasing, and social media use is growing, creating new spaces for journalists and HRDs to express their voices. However, voices of hate and misinformation are also flourishing, competing for attention and support. Cyber laws are also being enacted to monitor and arrest those who are deemed a threat to national security, and internet shutdowns remain a common tool for managing dissent and containing protests.

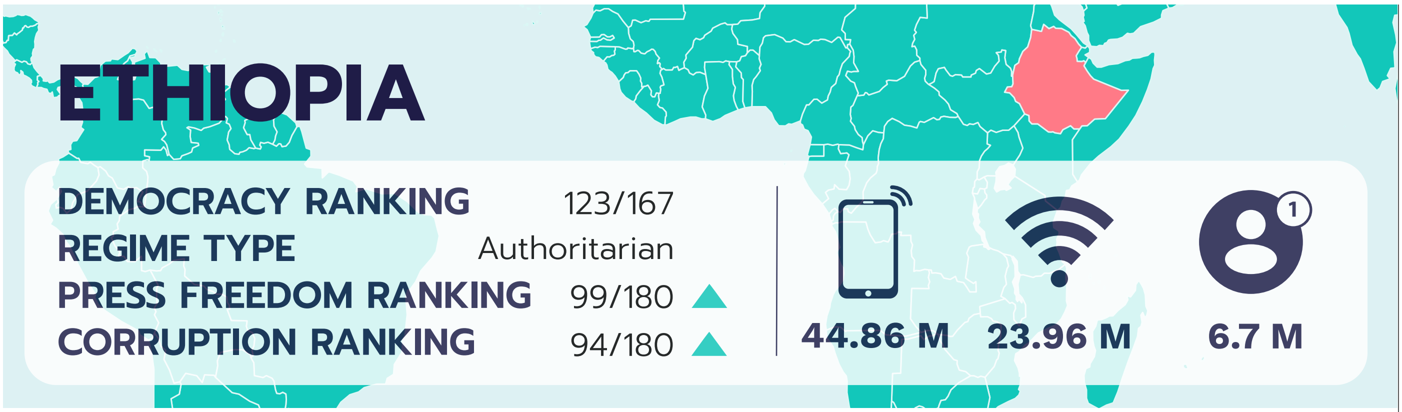
As citizens in African countries demand democratic reforms and accountability from their leaders, the continent is likely to experience increased conflict, putting HRDs at even greater risk.

Our research focused on countries in East Africa.



This map infographic is stylised and not to scale. It doesn't reflect the legal status of any country or territory or the delineation of any frontiers. CREDIT: World map svg taken from simplemaps.com

[9] Nathaniel Allen & Alexander H. Noyes, "*African Dictators Have Been Losing Power — Some to Democratic Governments. Militaries Can Tip the Scales Toward Democracy*," Rand, September 16, 2019, https://www.rand.org/blog/2019/09/african-dictators-have-been-losing-power-some-to-democratic.html (accessed August 20, 2020).



ETHIOPIA

DEMOCRACY RANKING	123/167	
REGIME TYPE	Authoritarian	
PRESS FREEDOM RANKING	99/180	▲
CORRUPTION RANKING	94/180	▲

☎		
44.86 M	23.96 M	6.7 M

Freedom of Expression: A Double-Edged Sword

In 2018, Ethiopia embarked on a reform agenda in response to intensifying anti-government protests. One of Africa's youngest leaders, Abiy Ahmed, was appointed the new Prime Minister, promising to pursue a new era of governance based on democracy and the rule of law. The previous draconian state of emergency was lifted and media freedom was given a boost, with activists and human rights defenders being able to discuss issues openly and without fear of retribution.

Ethiopia's internet freedom also improved dramatically, with previously censored sites being unblocked and imprisoned bloggers being released.

The lifting of restrictions on freedom of expression has increased the use of social media to drive change, but it has also given rise to hate speech and fake news — from both the ruling party and the opposition.

> *"There's so many Youtube channels promoting madness and crazy content."*
>
> *- MEDIA TRAINER*

Activists we spoke with accused Facebook of not doing enough to remove pages that are stoking hate, radicalisation, and ethno-political tensions.

On 30 June 2020, the Ethiopian government reverted to old habits and shut down the internet following the murder of popular musician and social activist Haacaaluu Hundeessaa. Protests calling for justice for the slain musician erupted, and during the ensuing internet shutdown, over 160 people were killed.[10] Full internet access was restored 23 days later.

Ethiopia's Information Networks Security Agency, which is charged with building cyber power to protect the country's national interests, is also accused of spying on opposition activists and critics of the government.

> *"The trend is very worrisome. But social media has the power to empower the silent people. They have the chance to speak for themselves. Every voice has a platform. That makes me enthusiastic."*
>
> *- HUMAN RIGHTS DEFENDER*

● ● ● ●

[10] "More than 160 killed in Ethiopia protests over singer's murder," *Al Jazeera*, July 5, 2020, https://www.aljazeera.com/news/2020/7/5/more-than-160-killed-in-ethiopia-protests-over-singers-murder (accessed September 2, 2020).

App Use Linked to Bandwidth Cost

There is a digital divide when it comes to using internet services. Ethiopia's internet penetration remains low, with less than 20% of the population connected to the internet.[11] Internet connectivity is expensive compared to other African countries, and the majority of people who are not paid well prefer to use apps that don't generate a lot of bandwidth. Social media use is concentrated in urban areas, with 8.2% of the population having Facebook accounts.

Interviewees indicated that Telegram is Ethiopia's most popular messaging app, standing in contrast to other African nations where WhatsApp tends to dominate. Some of the key reasons cited for this are cost savings for users due to Telegram's low bandwidth requirements, and the ease with which users can create and join large groups.

VPNs such as Psiphon are popular because of Ethiopia's history of internet censorship, but there is little awareness around encryption, and there is low use of two-factor authentication to protect accounts.

Increasing Risk for Journalists and Activists

Levels of digital security awareness and practice are low among activists and journalists, and it is challenging to convince them to take their digital security seriously.

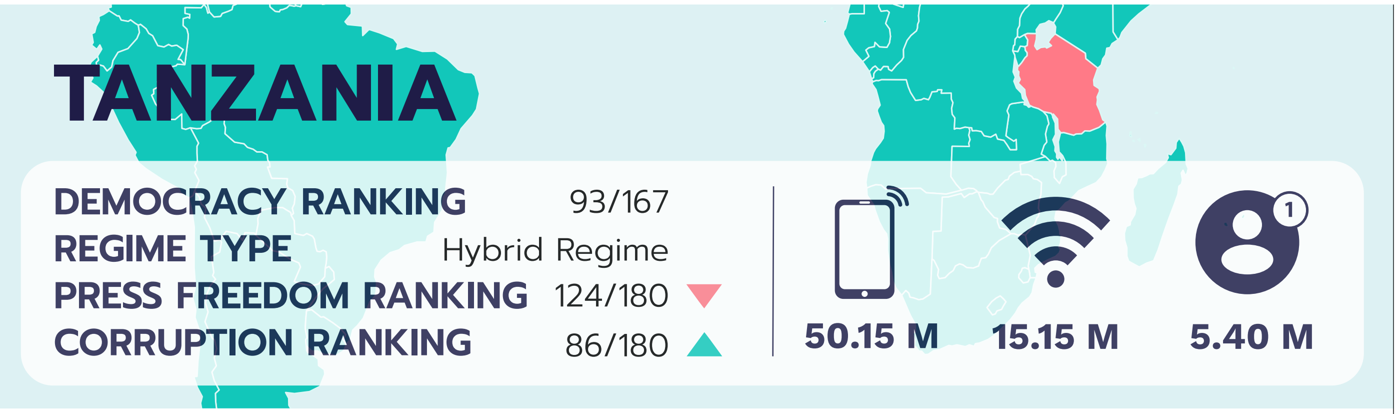
> ***"One of the challenges we have is how to convince journalists and activists to take their digital security seriously. In other places like Lebanon or Egypt, there is more awareness and experience."***
>
> *- DIGITAL RIGHTS ADVOCATE*

As of January 2021, conflict has erupted once again, and the country is facing civil war between government forces and the Tigray People's Liberation Force, which controls the autonomous northern Tigray region of Ethiopia. Internet and telephone services in the Tigray region have also been restricted.[12]

The impact this conflict will have on internet freedom for the rest of the country is unclear, but given the heightened military stance and the current state of emergency, increased online surveillance of government critics is more than likely, and journalists and activists will need to be more careful with their online behaviour.

[11] Internet World Stats, *Africa Internet Users, 2020 Population and Facebook Statistics*, https://www.internetworldstats.com/stats1.htm (accessed September 2, 2020).

[12] United Nations Office for the Coordination of Humanitarian Affairs, "*Ethiopia - Tigray Region Humanitarian Update: Situation Report*," January 15, 2021, https://reliefweb.int/report/ethiopia/ethiopia-tigray-region-humanitarian-update-situation-report-15-january-2021 (accessed 20 January 2021).



TANZANIA

DEMOCRACY RANKING	93/167
REGIME TYPE	Hybrid Regime
PRESS FREEDOM RANKING	124/180 ▼
CORRUPTION RANKING	86/180 ▲

📱 50.15 M

📶 15.15 M

👤 5.40 M

Online Surveillance and Self-Censorship

Tanzania is far from a thriving democracy. Since gaining independence, Tanzania has been controlled by the Chama Cha Mapinduzi (CCM, Party of the Revolution). A multi-party system was introduced in the 1990s, but opposition groups have not been able to dislodge the CCM, which has “relied on its incumbency, resource advantages, and patronage politics to strengthen itself and weaken the opposition”.[13]

The deterioration of Tanzania’s democratic landscape is being further accelerated by the country’s highly restrictive media freedom laws. In the past four years alone, 15 media outlets have been forced to close, and there has been “a climate of fear in which self-censorship is growing”.[14]

Websites and bloggers are also being restricted, with strict cyber laws[15] giving Tanzania’s Communications Regulatory Authority discretionary powers to censor online content, charge online content creators registration and licensing fees, and disclose the identities of contributors, sources, and financial sponsors.[16]

Clamping Down on Social Media

This climate has forced opinion-makers and journalists to turn to social media to express their views, with Facebook and with WhatsApp groups being used to source and share stories.

Pre-empting the significant role social media would play in the October 2020 presidential elections, the government amended cyber laws, banning the use of social media to promote “demonstrations, marches or the like which may lead to public disorder” and instituting vague content restrictions intended to quash freedom of expression.[17]

● ● ● ●

[13] Nicodemus Minde, “At the edge of democracy: what the general election holds in store for Tanzania,” *The Conversation*, August 23, 2020, https://theconversation.com/at-the-edge-of-democracy-what-the-general-election-holds-in-store-for-tanzania-144601, (accessed August 30, 2020).

[14] Reporters Without Borders, *Tanzania*, https://rsf.org/en/tanzania (accessed August 30, 2020).

[15] For example, Tanzania’s Electronic and Postal Communications (Online Content) Regulations, 2018.

[16] Shayera Dark, “Strict new internet laws in Tanzania are driving bloggers and content creators offline,” *The Verge*, July 6, 2018, https://www.theverge.com/2018/7/6/17536686/tanzania-internet-laws-censorship-uganda-social-media-tax (accessed August 30, 2020).

[17] ARTICLE 19, *Tanzania: New Content Regulations Criminalise Free Speech Online*, August 31, 2020, https://www.article19.org/resources/tanzania-regulations-criminalise-free-speech/ (accessed September 1, 2020).

A high level of social media surveillance has been put in place to monitor the ban, impacting freedom of expression and intensifying a culture of self-censorship.

> *"The Government has made sure the media space is totally regulated, so Facebook, WhatsApp, and Twitter are the places [HRDs] go to because they think the government can't get to them there.*
>
> *Prominent figures are using pseudonyms and running campaigns, creating content and whistleblowing."*
>
> *- TECH ENTREPRENEUR*

> *"They are monitoring social media accounts. They are trying to see what you are posting. Anything negative about the president or ruling party is not allowed. If you go against the government, then you become a victim."*
>
> *- DIGITAL RIGHTS ADVOCATE*

Cyber violence is also on the increase, with HRDs, opposition activists, and women in particular being heavily targeted.

Shutdowns and Fake Accounts

The presidential elections clearly demonstrated the weak state of Tanzania's democracy, and the CCM's power to suppress opposition both on the ground and online. In October 2020, John Maguful was once again declared the winner of the presidential election, ensuring the continued rule of the Chama Cha Mapinduzi. A widespread crackdown commenced, with opposition leaders being arrested and protests being banned. Analysis by internet monitoring organisation Netblocks indicated that leading social media and Google services, including Twitter, WhatsApp, and Gmail, had been blocked since the eve of the elections.[18]

> *"We are seeing fake accounts being opened up to create content for politicians and fake accounts being created to attack people."*
>
> *- TECH ENTREPRENEUR*

Interviewees said they expected an internet shutdown around the election, and that prior to the elections the government had indicated that WhatsApp would be blocked because it was being used to spread fake news and inaccurate information about the elections.

The cost of internet connectivity is also increasing. Facebook and WhatsApp come bundled as part of low-cost packages, but if the government decides to block these popular platforms, the cost of accessing the internet could become prohibitive for the majority of Tanzanians.

Civil society and human rights organisations are also being banned from operating in Tanzania, and opportunities to promote internet freedom tools and digital security strategies are limited. Nevertheless, there is a concerted effort by local organisations to conduct digital security training programs — but funding these programs remains a challenge.

[18] NetBlocks, *Internet disrupted in Tanzania on eve of general elections*, October 27, 2020, https://netblocks.org/reports/internet-disrupted-in-tanzania-on-eve-of-presidential-elections-oy-9abny3 (accessed October 30, 2020).

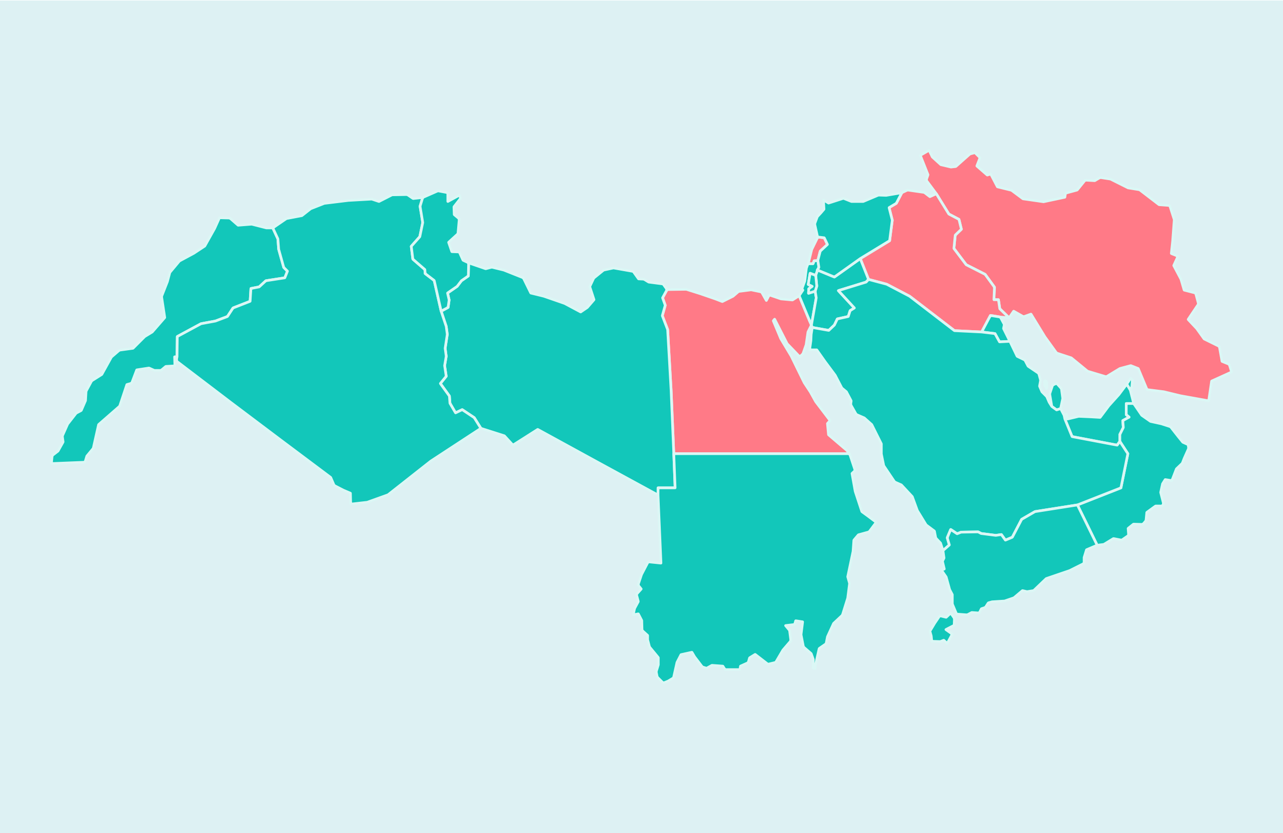
MENA

MENA's history is marked by violent conflicts fueled by sectarianism, driven by both regional and foreign actors. The region is overwhelmingly governed by dictatorships and authoritarian regimes intolerant of criticism and political opposition. However, MENA was also the first region to popularise social media as a tool to achieve political change.

The Arab Spring, a series of uprisings against authoritarian rule that commenced in late 2010 and continued through 2011, clearly demonstrated the power of social media, not just as a communications medium but also as an effective organisation platform. Activists and ordinary citizens were able to share information freely through Facebook, Twitter, and Youtube, enhancing their ability to coordinate protests against corrupt and authoritarian regimes.

However, it wasn't long before social media was used as a retaliatory weapon by MENA regimes and their supporters. The work of activists was countered and discredited through disinformation campaigns and hate speech. Surveillance technology was used to monitor and track down critics, and internet throttling and shutdowns inhibited the ability of opposition groups to communicate and organise.

Regimes in the United Arab Emirates, Saudi Arabia, Bahrain, and Morocco are known clients of the Pegasus spyware suite developed by the NSO Group, which can be used to extract data from mobile



This map infographic is stylised and not to scale. It doesn't reflect the legal status of any country or territory or the delineation of any frontiers. CREDIT: World map SVG taken from simplemaps.com

devices and listen in on messages and voice calls.[19]

Countries in the region regularly shut down internet services and use cyber laws ostensibly intended to tackle terrorism and cybercrime to silence human rights activists and critical voices.

There are increasing signs that tech companies and social media platforms like Facebook and Twitter are complying with requests from authoritarian regimes in the MENA region to censor posts and shutdown accounts.[20]

The MENA region is once again experiencing popular mass protests.[21] However, this time, entrenched politicians and the ruling elite have a better grasp of online surveillance and censorship techniques, and of methods to quash critics and opposition groups.

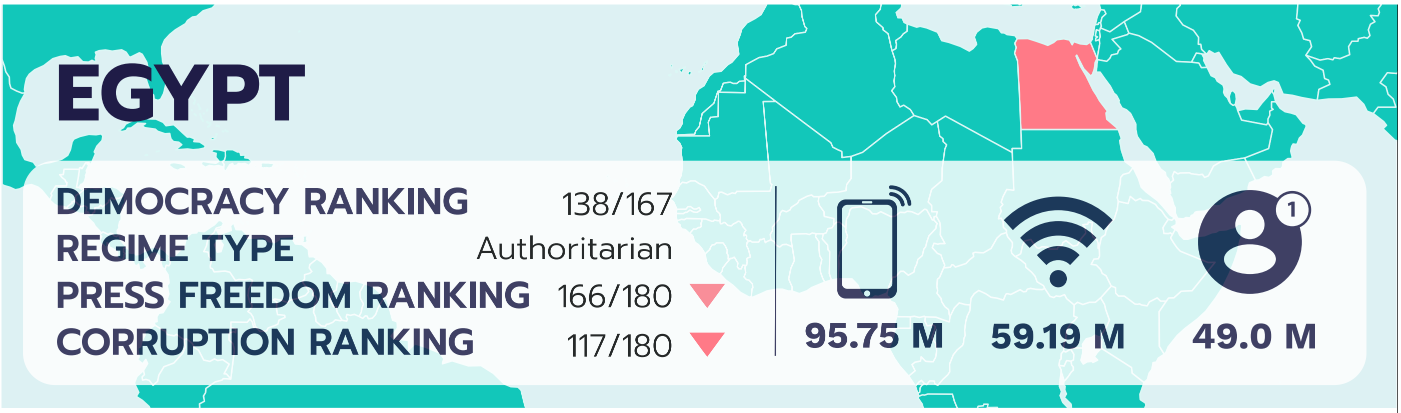
● ● ● ●

[19] Bill Marczak et al., *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, September 18, 2018, https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf (accessed August 15, 2020).

[20] Yarno Ritzen, "How Arab governments use cyberspace laws to shut down activism," *Al Jazeera*, July 25, 2019, https://www.aljazeera.com/news/2019/7/25/how-arab-governments-use-cyberspace-laws-to-shut-down-activism (accessed August 17, 2019).

[21] Ash-shab yurid isquat an-nizam," *Wikipedia*, https://en.wikipedia.org/wiki/Ash-shab_yurid_isqat_an-nizam (accessed August 15, 2020).

EGYPT



DEMOCRACY RANKING	138/167
REGIME TYPE	Authoritarian
PRESS FREEDOM RANKING	166/180 ▼
CORRUPTION RANKING	117/180 ▼

📱	📶	👤
95.75 M	**59.19 M**	**49.0 M**

Fuelling the Arab Spring

In 2011, protests erupted in Egypt fuelled by a sense of economic injustice and anger over the brutality of security personnel, forming part of the series of uprisings known as the Arab Spring.[22] Following the removal of then-President Hosni Mubarak,[23] the Muslim Brotherhood's Mohammed Morsi was elected President in 2012. A coup in 2013 saw Morsi deposed, with the coup leader, former Military Intelligence Director Abdel Fattah el-Sisi, elected President in 2014.

The 2018 presidential elections saw Sisi increase his authoritarian grip on the country, and several months later, laws were signed giving authorities increased powers to charge licensing fees from media outlet operators, popular websites, and social media platforms. Under these laws, those found to be spreading allegedly false news are subject to fines, imprisonment, and the deletion of their social media accounts.

Legalising Online Censorship and Intimidation

The blocking of websites deemed to be threats to the economy or national security was also legalised, though terminology used to define such "threats" was kept intentionally vague. Further, service providers were directed to retain user data for 180 days, and provide access to state authorities upon request.

Ahead of an April 2019 constitutional referendum to give President Sisi increased powers, more than 34,000 websites were blocked, including Batel, a petition site that collected over 60,000 signatures opposing the referendum.[24] Many commentators claim the referendum was "rigged from the outset," with critical voices being quashed during the period preceding the vote.[25]

● ● ● ●

[22] Yolande Knell, "The complicated legacy of Egypt's Hosni Mubarak," *BBC News*, January 25, 2013, https://www.bbc.com/news/world-middle-east-21201364 (accessed September 15, 2020).

[23] "Egypt country profile," *BBC News*, January 7, 2019, https://www.bbc.com/news/world-africa-13313370 (accessed September 15, 2020).

[24] "Egypt filters 34,000 domains in bid to block opposition campaign platform," *NetBlocks*, April 15, 2019, https://netblocks.org/reports/egypt-filters-34000-domains-in-bid-to-block-opposition-campaign-platform-7eA1blBp (accessed September 15, 2020).

[25] Ruth Michaelson and Adham Youssef, "Sisi wins snap Egyptian referendum amid vote-buying claims," *The Guardian*, Aprili 24, 2019, https://www.theguardian.com/world/2019/apr/23/sisi-wins-snap-egyptian-referendum-amid-vote-buying-claims (accessed September 15, 2020)

Almost 90% of voters supported the referendum, granting Sisi more power over the judiciary, enshrining the role of the military in the political system, and extending the presidential term to six years.

Egyptian political parties have also worked to manipulate content online through avenues including propaganda, attacks against the opposition, and directly suppressing online dissent.[26]

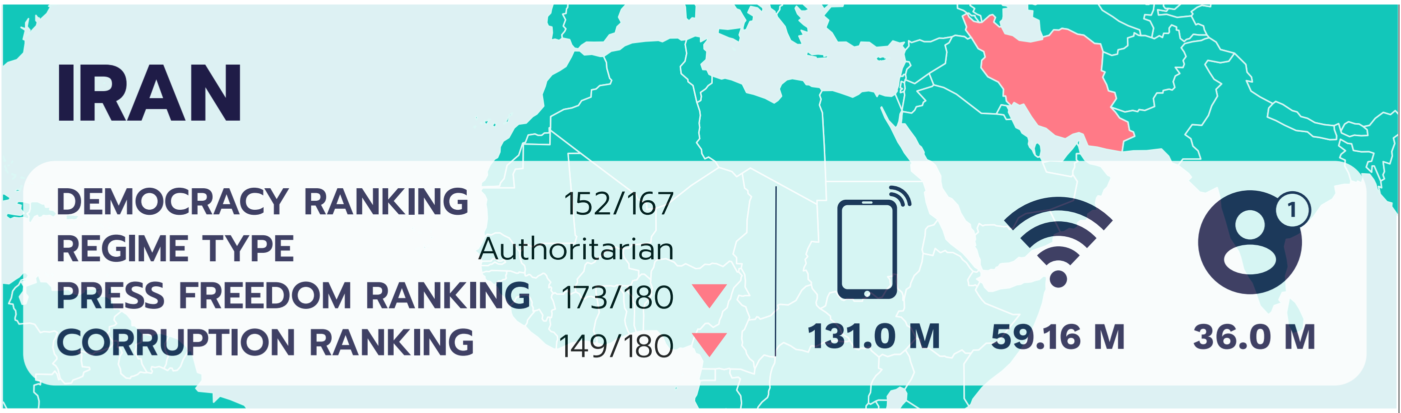
Cracking Down on Dissent

In September 2019, there were disruptions to Facebook Messenger, Twitter, Skype, the BBC, and other services and news websites in the wake of anti-government protests, and dozens of protesters were arrested.[27]

Journalists are often detained for 'spreading false news,' and are sometimes held without charge. Social media users also risk being jailed or dismissed from their jobs for their online activity.

[26] Samantha Bradshaw and Philip N. Howard, *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, 2019, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf (accessed September 15, 2020).

[27] Ellery Roberts Biddle and the Netizen Report Team, *Netizen Report: Anti-corruption protests across Egypt trigger internet blockages, arrests*, Global Voices, September 26, 2019, https://globalvoices.org/2019/09/26/netizen-report-anti-corruption-protests-across-egypt-trigger-internet-blockages-arrests/ (accessed September 15, 2020).



IRAN

DEMOCRACY RANKING	152/167
REGIME TYPE	Authoritarian
PRESS FREEDOM RANKING	173/180 ▼
CORRUPTION RANKING	149/180 ▼

📱	📶	👤
131.0 M	59.16 M	36.0 M

A Culture of Dissent

Like many countries in the MENA region, Iran's political landscape includes a complex mix of religious and military power, often resulting in an atmosphere of self-censorship and violent repercussions for those who speak out. Despite this repressive environment, there is a culture of dissent and a continuing struggle for freedom and democracy.

Iran's recent history of protests dates back to the 1979 revolution that "rejected American interference, but also saw Iranians demand freedom from a corrupt ruling class that flaunted its wealth."[28] However, what followed was the formation of the Islamic Republic, resulting in increased sectarian conflict – not just in Iran, but across the region. Since then, Iran has become increasingly isolated, and its Islamic Revolutionary Guard Corps (IRGC) are known to use torture and violence to supress internal dissent.

Controlling Dissent Through Censorship and Surveillance

Iran has actively censored and throttled internet access since the early 2000s, and the country is considered one of the world's worst internet freedom offenders.

Protests were triggered after hardliner Mahmoud Ahmadinejad was elected president in 2009, in what the opposition claimed were rigged elections.[29] Facebook and YouTube were blocked in response, as were Iran's mobile networks.

Prior to the 2013 presidential elections, high levels of online censorship were recorded, with almost half of the world's top 500 websites being blocked. Encryption protocols such as SSH were heavily throttled, limiting secure communications between opposition groups internally and externally.[30]

In December 2017, Iran blocked Telegram and other social networking apps to prevent protesters from organising effectively and to reduce communications

● ● ● ●

[28] Matt Peterson, "A Brief Modern History of Protest in Iran," *The Atlantic*, January 4, 2018, https://www.theatlantic.com/membership/archive/2018/01/a-brief-modern-history-of-protest-in-iran/549728/ (accessed September 2, 2020).

[29] Stephen Battersby, "Statistics hint at fraud in Iranian election," *New Scientist*, June 24, 2009, https://www.newscientist.com/article/mg20227144-000-statistics-hint-at-fraud-in-iranian-election/ (accessed September 2, 2020).

[30] Timothy B. Lee, "Here's how Iran censors the Internet," *The Washington Post*, August 16, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/08/15/heres-how-iran-censors-the-internet/ (accessed September 29, 2020).

during protests against "economic hardships and political repression".[31]

The November 2019 protests, triggered by a 50 per cent increase in gasoline prices, saw at least 304 protestors killed.[32] As the protests commenced, authorities disrupted internet services in major cities, which quickly expanded to a country-wide shutdown which lasted a week.

Interviewees indicated that despite being blocked, Telegram is still the most popular messaging app in Iran, with an estimated 40 million-plus users accessing the communications platform through VPNs and proxies to communicate internally and externally with the diaspora. WhatsApp, which is currently not blocked in Iran, has seen significant adoption in the country, and while some suspect that the Iranian authorities can monitor WhatsApp messages, there is no evidence that Facebook's messaging platform has been compromised. Signal, like Telegram, is blocked — but users are able to use it through VPNs.

> *"The level of trust of the government is almost zero — especially among the younger generation. I am pretty sure most of them are aware of the internet threats. But I don't think it's clear on how they can protect themselves."*
>
> *- DEMOCRACY ACTIVIST*

Regime-Sponsored 'Internet Freedom' and 'Digital Security'

Pro-government forces are increasingly using social media to counter critical viewpoints and disrupt protest movements. During the December 2017 protests, supporters of the regime used social media to publish the faces of protestors, calling for their arrest.[33]

> *"One concern that members of the diaspora who work with civil society have is having their aliases or pseudonyms being exposed. This would reveal their real identities and expose family members inside Iran to real threats."*
>
> *- DEMOCRACY ACTIVIST*

The Iranian regime has become highly cognisant of the power provided to activists by internet technologies. There are signs that the regime is analysing the work of the internet freedom community in order to undermine the effectiveness of technologies being designed to assist and protect activists.[34]

[31] "Iran protests: Why is there unrest," *BBC News*, January 2, 2018, https://www.bbc.com/news/world-middle-east-42544618 (accessed September 29, 2020).

[32] Amnesty International, "Iran: Details of 304 deaths in crackdown on November 2019 protests," May 20, 2020, https://www.amnesty.org/en/documents/mde13/2308/2020/en/ (accessed September 29, 2020).

[33] "Iran protests: Social media messaging battle rages," *BBC News*, January 7, 2018, https://www.bbc.com/news/world-middle-east-42566083 (accessed September 2, 2020).

[34] Steven Zhou, "Iranian Canadian Says Iran Detained Him, Tried to Force Him to Be a Spy," *VICE World News*, August 25, 2020, https://www.vice.com/en/article/5dz4va/iranian-canadian-says-iran-detained-him-tried-to-force-him-to-be-a-spy (accessed September 2, 2020).

"Another threat for people inside the country comes from using apps that are made by the IRCG. A couple of years ago they made and sold VPN software. They have also made messaging apps."

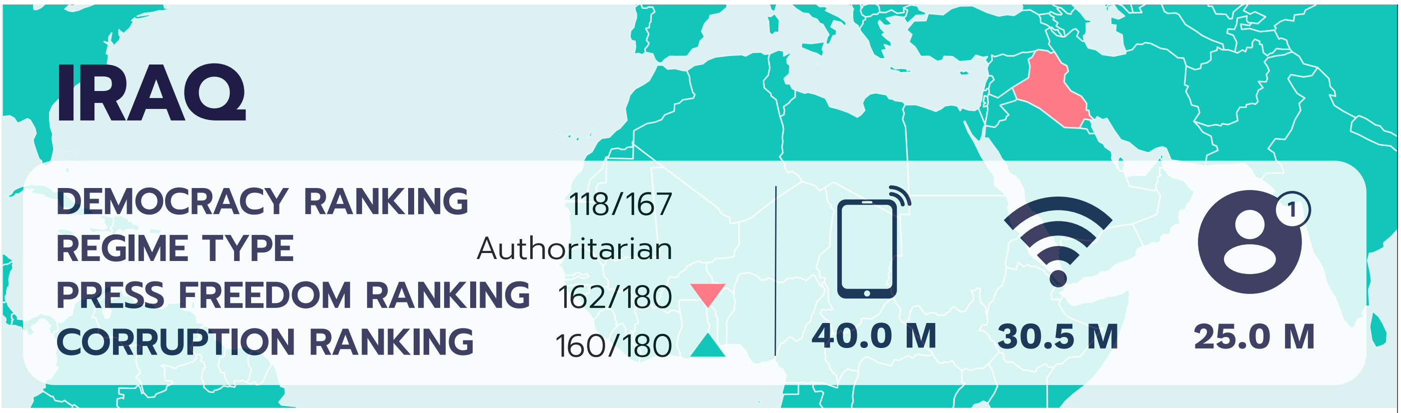
- DEMOCRACY ACTIVIST

Conducting digital security training programs inside Iran is near-impossible, but there are many Persian-language resources available online which HRDs inside the country can access through VPNs.

"I think everyone knows these days that digital security is important, but something that we lack are real examples, and details about how activists can be in danger, and what can happen to them if they don't activate the 2FA for example."

- DEMOCRACY ACTIVIST

IRAQ



DEMOCRACY RANKING	118/167
REGIME TYPE	Authoritarian
PRESS FREEDOM RANKING	162/180 ▼
CORRUPTION RANKING	160/180 ▲

📱	📶	👤
40.0 M	30.5 M	25.0 M

The Rise and Fall of Islamic State

Since the American invasion in 2003 which ousted President Saddam Hussein, Iraq has experienced high levels of instability. A violent sectarian-based insurgency followed, allowing the terrorist organisation Islamic State in Iraq (ISI) to grow in strength and number, taking control of parts of the country.

Iraqi forces fought back with the support of the US and other coalition countries, and in December 2017, Iraq's Prime Minister, Haider al-Abad, declared victory and claimed the country had been liberated.[35] ISI's defeat did little to bring peace and stability to the country, however, and Iraq has continued to experience waves of civil unrest and protest.

Controlling Internet Freedom

Iraqi journalists and activists have a history of using social media to criticise government policies and document protests.[36] However, internet censorship is on the rise, and Iraq is rife with online hate speech targeting activists and journalists.

According to one interviewee, this hate speech is predominantly generated by a government-controlled electronic army who are able to post violent messages without getting blocked. The Iraqis call them "electronic fleas".

> *"When activists get threats, their voices will be weaker, or they will avoid using Facebook altogether. Sometimes they move to Twitter."*
>
> *- DIGHTIAL RIGHTS ACTIVIST*

Another interviewee indicated that along with activist Facebook accounts being shut down, some activists were being killed off virtually, with their accounts being memorialised – a Facebook feature for account holders who have died.

[35] Sarhang Hamasaeed and Garrett Nada, "Iraq Timeline: Since the 2003 War," *United States Institute of Peace*, May 29, 2020, https://www.usip.org/iraq-timeline-2003-war (accessed August 15, 2020).

[36] Kristine Kristensen, "A network for social media activists in Iraq," *IMS*, May 25, 2011, https://www.mediasupport.org/a-network-for-social-media-activists-in-iraq/ (accessed August 15, 2020).

> *"Since the protests, there has been an increase in Facebook accounts of activists and journalists being shut down. We feel that there's some teams inside Facebook that are targeting these people. We feel there might be corruption happening."*
>
> *- DIGITAL RIGHTS ACTIVIST*

Going Dark — Iraq's Internet Shutdowns

Internet disruptions are a regular occurence in Iraq. Social media blackouts are commonplace, justified by the government as preventing security threats and cheating during exam periods. 25 distinct shutdowns were recorded in 2017.[37]

In July 2018, the internet was shut down for four days, during which peaceful protestors were attacked and shot at.[38] When protestors reorganised in October 2019 to challenge the government, the response was predictable and swift. The internet went dark for 20 days, during which over 700 protestors were killed and 20,000 were injured.

It is likely that this shutdown trend will continue.

Signal and Telegram are gaining in popularity

According to interviewees, Viber had been the most used messaging app in Iraq due to its usability, but more recently, people have shifted to Telegram – both because it isn't a US app, and because Telegram is used by militia groups who are assumed to be security experts. Signal is also gaining popularity as a communications app among activists, particularly after the violent October 2019 protests. Use of Wire is increasing.

Digital Security in Atmosphere of Fear

Evidence suggests that the NSO Group's Pegasus spyware is operating in Iraq,[39] giving authorities the capability to monitor the activities of mobile phone users.

There are efforts to increase digital security practices and promote the use of censorship- and surveillance-defeating technologies among HRDs, but progress is slow.

> *"Digital security education and awareness is very low, even among activists. Sometimes you may have the tools and knowledge, but you are missing the commitment. And some of these tools are very hard to use with low internet speeds."*
>
> *- DIGITAL RIGHTS ACTIVIST*

● ● ● ●

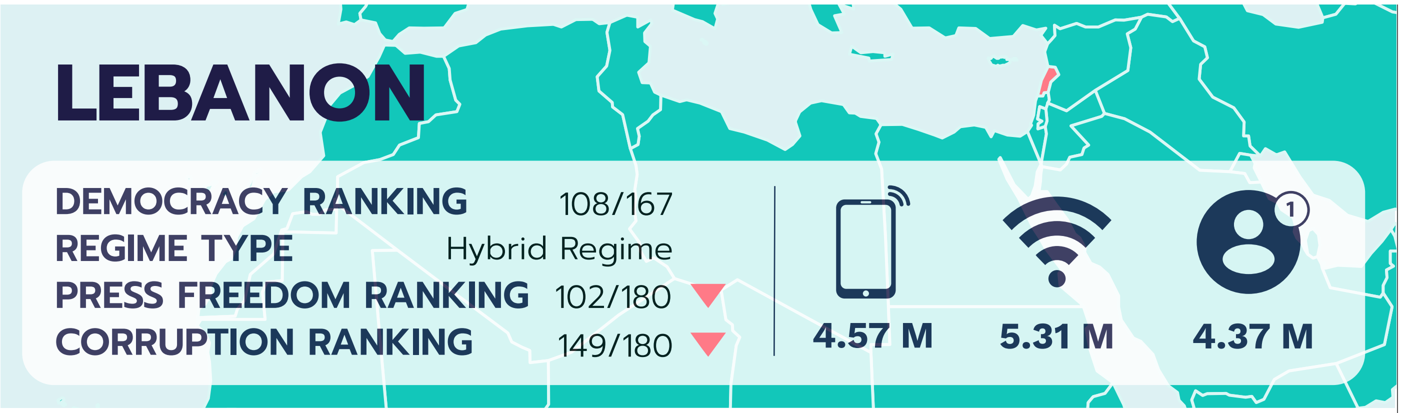
[37] SMEX, "*Iraq's Increased Use of Internet Shutdowns a Worrying Trend*," September 28, 2017, https://smex.org/iraqs-increased-use-of-internet-shutdowns-a-worrying-trend/ (accessed August 15, 2020).

[38] Amnesty International, "*Iraq: Security forces deliberately attack peaceful protesters while internet is disabled*," July 19, 2018, https://www.amnesty.org/en/latest/news/2018/07/iraq-security-forces-deliberately-attack-peaceful-protesters-while-internet-is-disabled/ (accessed August 15, 2020).

[39] Bill Marczak et al., *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, September 18, 2018, https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf (accessed August 29, 2020).

In August 2020, a number of activists were attacked and murdered. While those responsible are still at large, there is widespread acknowledgement that the violence is intended to create an atmosphere of fear, and prevent the formation of political movements prior to the parliamentary elections scheduled for mid-2021.[40]

[40] Mariya Petkova, “What is behind the killings in Basra?,” *Al Jazeera*, August 28, 2020, https://www.aljazeera.com/news/2020/8/28/what-is-behind-the-killings-in-basra (accessed August 29, 2020).



LEBANON

DEMOCRACY RANKING	108/167
REGIME TYPE	Hybrid Regime
PRESS FREEDOM RANKING	102/180 ▼
CORRUPTION RANKING	149/180 ▼

📱	📶	👤
4.57 M	5.31 M	4.37 M

Proportional Representation Insufficient for Peace

Lebanon has frequently been embroiled in Middle-Eastern conflict due to its location bordering Syria and Israel.[41] After gaining independence in 1943, its leadership created a system of governance that allowed for proportional representation of the country's three major religious groups – Maronite Christians, Shiite Muslims, and Sunni Muslims. However despite this, tensions between the groups continued to heighten, and civil war broke out in 1975, killing hundreds of thousands and requiring intervention from Syria and Iran.

After the war ended in 1990, a National Assembly was formed, aimed at dissolving militia groups — except the powerful Shia Hezbollah, which is backed by Iran. A treaty between Syria and Lebanon allowed Syrian forces to remain, protecting the country from external threats, though Syria withdrew its forces in 2005 following the assassination of Lebanese Prime Minister Rafiq Hariri.[42]

Unlike its neighbours, Lebanon doesn't have one strong leader, but many — representing different factions that aim to influence the country's direction.[43] Political instability has increased in the last decade, as have sectarian tensions and violence between Hezbollah and other Sunni groups. In 2019, there were widespread protests calling for economic and political change,[44] which led to the resignation of Prime Minister Saad Hariri.[45]

ISPs Tightly Controlled

The Lebanese government has tight control over internet service providers. From 2014 to 2017, mobile internet was inaccessible in Arsal, a town in Lebanon's northwest which has become home to Syrian refugees, for 'security reasons'.[46] In

[41] BBC News, "*Lebanon country profile*," August 11, 2020, https://www.bbc.com/news/world-middle-east-14647308 (accessed September 12, 2020).

[42] Council on Foreign Relations, "*Political Instability in Lebanon*," n.d., https://www.cfr.org/global-conflict-tracker/conflict/political-instability-lebanon (accessed September 14, 2020).

[43] Reuters, "*Explainer: Why is Lebanon in an economic and political mess*?," November 7, 2020, https://www.reuters.com/article/us-lebanon-protests-causes-explainer-idUSKBN1XG260 (accessed September 14, 2020).

[44] Elena Hodges, "A Country on Fire: Lebanon's October Revolution in Context," *Lawfare*, November 20, 2019, https://www.lawfareblog.com/country-fire-lebanons-october-revolution-context (accessed September 14, 2020).

[45] BBC News, "*Lebanon country profile*," August 11, 2020, https://www.bbc.com/news/world-middle-east-14647308 (accessed September 12, 2020).

[46] Elham Barjas, "Two Years of Collective Punishment: Mobile Data Remains Inaccessible to Arsal Residents," *SMEX*, March 31, 2017, https://smex.org/two-years-of-collective-punishment-mobile-data-remains-inaccessible-to-arsal-residents/ (accessed September 13, 2020).

December 2018, a judicial order cited the Israel Boycott law of 1963 to block website hosting service Wix, and in January 2019, the telecommunications minister ordered telecom operators to block Grindr, a popular dating platform for LGBTQI+ individuals.

On a handful of occasions, telecom operator OGERO blocked the Vonage voice-over-Internet protocol (VoIP) service, though the decision was reversed after pressure from businesses, civil society and politicians.[47]

Your Criticism Isn't Welcome Here

Since 2017, Lebanon has cracked down on online freedom of expression. Internet users accused of breaching regulations have been subjected to long interrogations, pressured to apologise for their posts, and forced to delete posted content.

In July 2019, there were 25 cases of people being detained for criticising top government officials such as the President and Foreign Minister, with at least 2 of those cases resulting in detainees serving prison sentences.

In 2020, journalists and activists covering protests were frequently harassed by the police, the army, and counter-protesters, with police reportedly confiscating people's phones and forcing detainees to give up passwords so authorities could access their data.[48] Lebanon's Cybercrimes Bureau is also accused of infiltrating WhatsApp groups to identify and track protest leaders.[49]

Surveillance: At Home and Abroad

In January 2018, a major surveillance operation with nation-state level capabilities was discovered running out of a General Directorate of General Security in Beirut. The operation, dubbed Dark Caracal by the researchers who investigated it, has developed a spyware tool, Pallas, which was able to extract gigabytes of information from Android devices by prompting them to download malware. Among those targeted were military personnel, government officials, journalists, activists and lawyers in 21 countries.[50]

● ● ● ●

[47] Freedom House, "*Freedom on the Net: Lebanon*", 2019, https://freedomhouse.org/country/lebanon/freedom-net/2019 (accessed October 1, 2020).

[48] Faten Bushehri, "In Lebanon, journalists and activists who cover protests face threats," *Global Voices*, February 14, 2020, https://globalvoices.org/2020/02/14/in-lebanon-journalists-and-activists-who-cover-protests-face-threats/ (accessed October 1, 2020).

[49] Deborah Amos and Lama Al-Arian, "Lebanon's Government is Accused of Swarming WhatsApp to Catch Protesters," *National Public Radio*, March 9, 2020, https://www.npr.org/2020/03/09/809684634/lebanons-government-is-accused-of-swarming-whatsapp-to-catch-protesters (accessed October 1, 2020).

[50] Lookout and Electronic Frontier Foundation, "*Dark Caracal: Cyber-espionage at a Global Scale*," 2018, https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf (accessed October 1, 2020).

South Asia

South Asia is home to the world's most populous democracy — India. Despite its democratic government, India's recent history has been dogged by nationalism and anti-secularism, leading to an assault on digital privacy and freedoms.

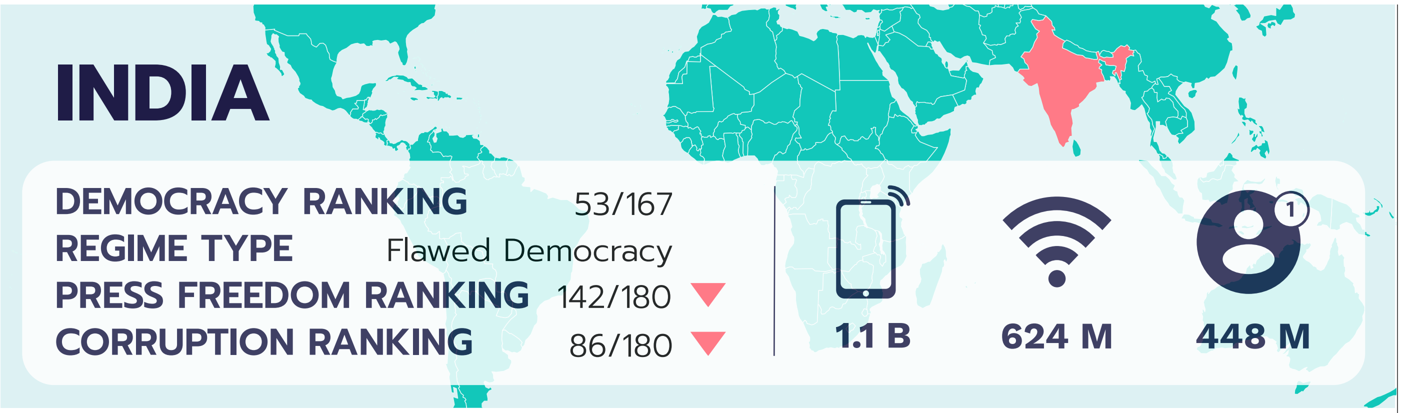
The policies and attitudes towards internet access in the region are typified by the ongoing shutdowns in Kashmir. Disrupted internet access and ongoing digital surveillance in the Kashmiri region is one example of how shutdowns, surveillance, and censorship are used as a political weapon in South Asia to silence perceived opponents or dissidents.

This practice has also been adopted in neighbouring Pakistan, where efforts to censor critics online have increased rapidly since the election of populist Prime Minister Imran Khan in 2018. The country's internet regulator has broad powers allowing it to censor online content, with social media companies required to comply with censorship requests within 24 hours. These laws have drawn criticism from media and rights groups in the country.

HRDs in other countries in South Asia, including Sri Lanka and Maldives, are also facing digital security challenges and more effort (in terms of training and resources) is needed to resist tactics of internet shutdowns and censorship by these countries' increasingly authoritarian governments.

Much like other regions of the world, South Asia is observing a rise in populist and authoritarian governance, resulting in an overall decrease in democratic freedoms and human rights protections.

This map infographic is stylised and not to scale. It doesn't reflect the legal status of any country or territory or the delineation of any frontiers. CREDIT: World map svg taken from simplemaps.com



INDIA

DEMOCRACY RANKING	53/167	
REGIME TYPE	Flawed Democracy	
PRESS FREEDOM RANKING	142/180	▼
CORRUPTION RANKING	86/180	▼

1.1 B

624 M

448 M

World’s Largest Democracy Treading an Authoritarian Path

India, the world’s most populous democracy, has a post-independence history scattered with conflict and ongoing tension. The 2019 re-election of hard-line Hindu nationalist Prime Minister Narendra Modi emboldened his Bharatiya Janata Party (BJP) and its supporters to promote a Hindu nationalist agenda for the country — sidelining secular ideals and marginalising the country’s Muslim population (195 million, or 10%), painting them as enemies to the Hindu majority.

The Indian government, along with 76% of the general population, perceives Pakistan as a threat – and the historical tension between the two countries over Kashmir is considered a “very big problem”.[51]

With privacy under assault and India’s internet freedom rapidly deteriorating, the country is heading down a dangerous path of authoritarian politics and right-wing populism.

Most Internet Shutdowns of Any Country

India is one of the world’s leaders when it comes to internet shutdowns. During 2019, there were at least 121 internet shutdowns,[52] with the shutdown in Kashmir being the longest ever imposed by a democracy. Indian Foreign Minister Subrahmanyam Jaishankar justified the shutdown on national security grounds, claiming it disrupted activity by militant groups allegedly supported by Pakistan.[53] Connectivity was restored in March 2020, but activists are concerned government agencies are monitoring their online habits and tracking VPN users.

Pegasus Spyware Hacking WhatsApp Accounts

In October 2019, reports began to emerge that the WhatsApp accounts of Indian HRDs and journalists had been hacked using the NSO Group’s Pegasus spyware.[54] India has been proven to be a client of Israeli surveillance spyware maker NSO

● ● ● ●

[51] Kat Devlin, “*A Sampling of Public Opinion in India*,” Pew Research Centre, March 25, 2019, https://www.pewresearch.org/global/2019/03/25/a-sampling-of-public-opinion-in-india/ (accessed August 20, 2020).

[52] Access Now, “*#KeepItOn: Targeted, Cut Off, and Left in the Dark*,” 2019, https://www.accessnow.org/keepiton-2019-report (accessed August 20, 2020).

[53] Niha Masih et al., “India’s Internet shutdown in Kashmir is the longest ever in a democracy,” *The Washington Post*, December 16, 2019, https://www.washingtonpost.com/world/asia_pacific/indias-internet-shutdown-in-kashmir-is-now-the-longest-ever-in-a-democracy/2019/12/15/bb0693ea-1dfc-11ea-977a-15a6710ed6da_story.html (accessed August 20, 2020).

[54] “Pegasus breach: India denies WhatsApp hack amid outrage,” *BBC News*, November 1, 2019, https://www.bbc.com/news/world-asia-india-50258948 (accessed August 20, 2020).

Group.[55] The NSO Group denied direct involvement, implying that the Indian government deployed the spyware.[56]

Online and Offline Attacks

An interviewee who is an environmental activist stated that he has received a number of threats, and has actually been physically assaulted on account of his work. In March 2020, he experienced an attack on a crucial component of his digital infrastructure: his Gmail account, along with his Google Drive that carried important documents, was inexplicably suspended by Google. While he cannot prove it, the timing makes him suspect it was related to his campaigning work against the Adani Group.

> *"The government is more powerful and has an upper hand when we are talking about offensive security technologies. On one level it's for national security, but they may be using these same technologies for surveillance of activists."*
>
> *- DIGITAL SECURITY TRAINER*

There are digital security training opportunities in India, but, according to one trainer, the programs need to be more comprehensive and widespread, and need to target participants in both major cities and smaller towns.

Phishing attacks are becoming more sophisticated, and malware runs rampant on the devices of journalists and activists. Identity theft is also a frequent occurrence, and trolling and hate speech present significant issues.

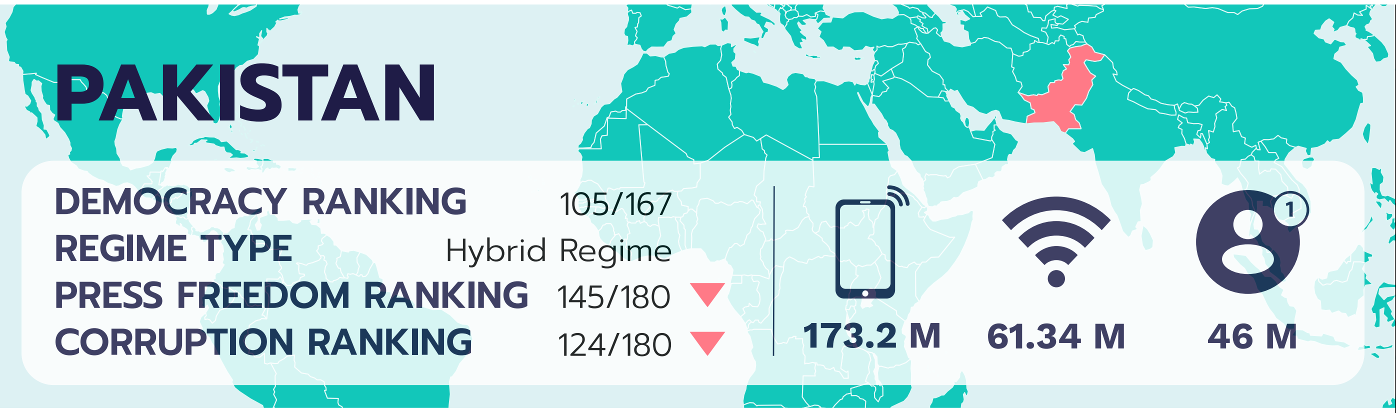
> *"Hackers are targeting low profile journalists like sports journalists to get to their editors, or other people on their network... The Indian media organisations are not very strict. I would say they are not interested in digital security."*
>
> *- DIGITAL SECURITY TRAINER*

Interviewees also indicated that cyber-security firms are increasingly involved in attacking and undermining the work of activists and journalists, on a fee-for-service basis.

[55] Bill Marczak et al., *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, September 18, 2018, https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf.

[56] Sushovan Sircar, "Govts Deployed Pegasus Spyware on People: NSO Group Tells US Court," *The Quint*, May 5, 2020, https://www.thequint.com/news/india/government-clients-used-pegasus-spyware-on-people-nso-group-whatsapp-case (accessed August 19, 2020).

PAKISTAN



DEMOCRACY RANKING	105/167	
REGIME TYPE	Hybrid Regime	
PRESS FREEDOM RANKING	145/180	▼
CORRUPTION RANKING	124/180	▼

173.2 M

61.34 M

46 M

Critics Not Tolerated

The political context of Pakistan is complex, and there is a long history of hostility with neighbouring India. Relations with Afghanistan are also fraught, with the Pakistan-Afghanistan border region often used by insurgents and Islamist groups.

Intolerance towards critics has steadily increased, with Pakistan's military intelligence and Islamist groups targeting journalists and activists — killing, attacking, or imprisoning hundreds over the past two decades.

> *"The threat landscape is increasing and getting sophisticated. For local journalists, they don't have the necessary tools, technologies or even the training to stay secure. It is really challenging. The number of trainings have gone down."*
>
> *- HUMAN RIGHTS LAWYER*

Pakistan has poor media freedom and human rights records. While the internet provides an opportunity for freedom of expression, it has rapidly become a dangerous space, with both government authorities and militant groups targeting individuals and groups which they deem a threat to national security or religious values.

> *"There are a lot of threats to people who speak out. We thought things would be more open under Imran Khan — but what we are experiencing is more like a dictatorship."*
>
> *- DIGITAL RIGHTS ADVOCATE*

Legalising Surveillance and Censorship

Pakistani authorities are supported in their efforts to monitor and censor internet communications by a number of laws,[57] including the draconian Prevention of Electronic Crimes Act (2016) and the more recent Citizens Protection (Against Online Harm) Rules (2020), which have tightened government control over social media.[58] These laws empower authorities to carry out electronic surveillance and data collection, block content, and crack down on free speech and privacy rights.

● ● ● ●

[57] Privacy International, "*State of Privacy Pakistan*," January 26, 2019, https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan (accessed August 19, 2020).

[58] Seerat Chabba, "Pakistan's new internet laws tighten control over social media," *Deutsche Welle*, February 2, 2020, https://www.dw.com/en/pakistans-new-internet-laws-tighten-control-over-social-media/a-52375508 (accessed August 19, 2020).

In October 2019, reports emerged[59] that Pakistan had contracted the services of Canadian cyber surveillance company Sandvine to build an internet monitoring system capable of deep packet inspection.

These laws and surveillance technologies, combined with the capabilities of its intelligence agencies, make Pakistan a deadly place for critical voices.[60]

Internet Shutdowns and Demand for Internet Rights

> *"In major cities, if there's a protest or a religious procession, the internet might be shut down. In certain parts — like the North West frontier — the internet is shut down. In other regions, where there is a lot of human rights work, there can be throttling or filtering."*
>
> *- HUMAN RIGHTS LAWYER*

Internet censorship and restrictions are not a new phenomenon in Pakistan. In the northwest tribal region (formerly known as the Federally Administered Tribal Area, or FATA), residents have not had internet access since June 2016, when the government shutdown services following armed clashes with Afghanistan.[61]

Other parts of Pakistan regularly experience shutdowns and restrictions, especially during times of political activities or unrest. However, according to interviewees, increased dependence on the internet (due to the Coronavirus pandemic) has brought with it a growing awareness of internet rights among the public. While critical mass is some way off, there is hope that public demand for an open and reliable internet will offset some of the draconian measures that are currently being implemented.

> *"Online communication is the least secure thing in Pakistan. So whenever it is possible, we always try to conduct meetings in public spaces, where there are no electronic devices."*
>
> *- HUMAN RIGHTS LAWYER*

● ● ● ●

[59] Umer Ali & Ramsha Jahangir, "Pakistan moves to install nationwide 'web monitoring system," *Coda*, October 24, 2019, https://www.codastory.com/authoritarian-tech/surveillance/pakistan-nationwide-web-monitoring/ (accessed August 20, 2020).

[60] Kiran Nazish, "Pakistan's military is waging a quiet war on journalists," *Vox*, May 3, 2018, https://www.vox.com/2018/3/27/17053776/pakistan-military-isi-journalists-abductions (accessed August 20, 2020).

[61] Hija Kamran, "A Year Without the Internet," *Slate*, August 21, 2017, https://slate.com/technology/2017/08/the-internet-has-been-shut-down-in-pakistans-fata-for-more-than-a-year.html (accessed August 20, 2020).

Southeast Asia

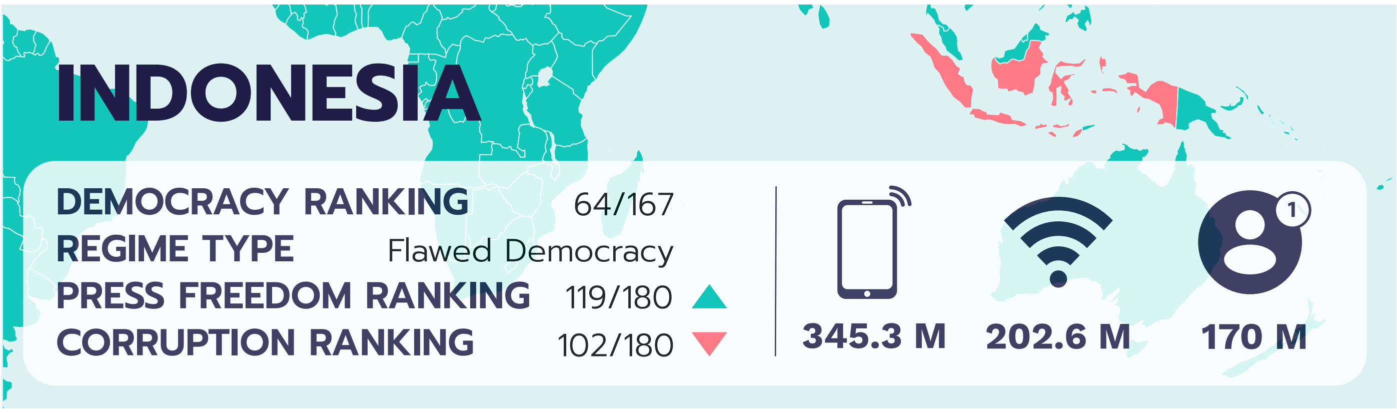
Use of internet and digital services in Southeast Asia is rapidly increasing, with 40 million new people coming online during 2020 alone. While internet availability and access levels are increasing, countries in the region are also enacting dangerous regulations and legislation which can be used to target critics and journalists.

The strength and stability of democracies in many Southeast Asian countries is deteriorating. In many cases this is due to populist and autocratic leaders who attack and undermine the political, human, and civil rights of the region's citizens. A number of countries, including those featured in this section, can be described as being run by 'strongman' rulers or one-party states. The February 2021 military coup in Myanmar demonstrates the fragile nature of democracy in the region.

Protests are also becoming more frequent and highly-attended, with activists expressing themselves both online and on the streets. Internet shutdowns have been used to curtail the use of social media — intended to stifle dissent, conceal human rights violations, and limit external communication and aid. Disinformation campaigns, hate speech, and online surveillance are used to target critical voices and civil society.

Human rights defenders and journalists depend on digital platforms (such as instant messaging and social media) for their work, making digital security a crucial aspect of ensuring HRDs' safety. However, the scaling of digital security practice has been unsuccessful overall. As citizens fight for their rights, the value of digital technologies will remain limited unless there is a more concerted effort to promote and build digital security capacity among defenders of democracy in Southeast Asia.

This map infographic is stylised and not to scale. It doesn't reflect the legal status of any country or territory or the delineation of any frontiers. CREDIT: World map svg taken from simplemaps.com



INDONESIA

DEMOCRACY RANKING	64/167
REGIME TYPE	Flawed Democracy
PRESS FREEDOM RANKING	119/180 ▲
CORRUPTION RANKING	102/180 ▼

📱 345.3 M

📶 202.6 M

👤 170 M

Widodo Turning From Democracy?

Following colonisation by the Dutch and the Japanese, Indonesia experienced prolonged periods of political instability due to coups, corruption, and bids for self-determination.[62] The provinces of Papua and West Papua continue their struggle for independence, with support from inside and outside of Indonesia.[63] Islamic radicalisation and terrorist attacks are also an ongoing challenge for the country.[64]

Indonesian President Joko Widodo was elected in 2014, winning against more established politicians. He was seen as relatively untouched by corruption thanks to his working-class background.[65] In 2019, Widodo was re-elected for a second presidential term with an ongoing commitment to reforming Indonesia's bureaucracy, cracking down on extremist ideology, and prioritising infrastructure and economic growth. However, a proposed law to limit the power of the anti-corruption agency, and a new criminal code that included provisions that violated minority and women's rights, triggered massive student protests across Jakarta and other major Indonesian cities.[66]

Declining Internet Freedoms

Widodo is often portrayed as tech-savvy, but Indonesia's record on internet freedom has declined under his watch.[67] During the 2019 presidential elections, many social media platforms were blocked — supposedly to prevent the spread of

● ● ● ●

[62] BBC News, "*Indonesia profile — Timeline*," April 17, 2019, https://www.bbc.com/news/world-asia-pacific-15114517 (accessed September 26, 2020).

[63] Tasha Wibawa, "*Why nearly 2 million people are demanding an independence vote for West Papua province*," ABC News, January 30, 2019, https://www.abc.net.au/news/2019-01-30/west-papuans-fight-for-another-independence-referendum/10584336 (accessed September 25, 2020).

[64] Zachary Abuza and Alif Satria, "How Are Indonesia's Terrorist Groups Weathering the Pandemic?," *The Diplomat*, June 23, 2020, https://thediplomat.com/2020/06/how-are-indonesias-terrorist-groups-weathering-the-pandemic/ (accessed September 25, 2020).

[65] BBC News, "*Indonesia country profile,*" October 2, 2018, https://www.bbc.com/news/world-asia-pacific-14921238 (accessed September 26, 2020).

[66] Associated Press in Jakarta, "Indonesian students clash with police in protests over new law," *The Guardian*, September 30, 2019, https://www.theguardian.com/world/2019/sep/30/indonesian-students-resume-anti-corruption-protests (accessed September 26, 2020).

[67] Freedom House, "*Freedom on the Net 2019: Indonesia*," 2019, https://freedomhouse.org/country/indonesia/freedom-net/2019 (accessed September 26, 2020).

disinformation and quell election-related unrest.[68]

In July 2018, Indonesia blocked TikTok, citing the app as being a medium for negative content. However, a week later, the block was overturned, with reports indicating that TikTok had agreed to remove negative content, and establish a team that censored content inappropriate for its Indonesian users.[69]

Connectivity was restricted during 2019 West Papuan self-determination protests, and websites carrying stories of the Papuan independence struggle were also blocked.

> *"I know how to be safe in real life. It's a lot easier than trying to be safe on digital platforms"*
>
> *- HUMAN RIGHTS DEFENDER*

> *"We have seen DDOS attacks target alternative media and sites that cover issues related to women's rights and LGBTIQ+ issues."*
>
> *- MEDIA FREEDOM ADVOCATE*

Online "Buzzers" Discrediting Civil Society

Interviewees indicated that online harassment and hate speech was common — and highly effective in terms of quashing dissent.

> *"Doxing is on the rise. They spread your personal details and intimidate you — saying we know where you live and where your family lives. Females are an easy target. In 2019, a female journalist wrote a story about a religious leader and was targeted."*
>
> *- MEDIA FREEDOM ADVOCATE*

Activists, and their work, are often discredited by teams of "buzzers" — a term used to describe people who create social media buzz using hundreds of fake accounts on Twitter, Facebook, and messaging platforms such as WhatsApp. These "buzzers" counter the arguments made by civil society, and generate disinformation at a scale designed to overwhelm. During student protests in 2019, buzzer teams promoted the belief that students were being paid to attend the protests and were responsible for rioting.[70]

> *"Social media is still very beneficial. There's so many campaigns that we use it for. But there's threats that we have to deal with. I get threats on social media when I criticise the government."*
>
> *- DEMOCRACY ADVOCATE*

● ● ● ●

[68] NetBlocks, "*Indonesia blocks social media as election protests escalate*," May 22, 2019, https://netblocks.org/reports/indonesia-blocks-social-media-as-election-protests-escalate-XADE7LBg (accessed September 27, 2020).

[69] Reuters, "*Indonesia overturns ban on Chinese video app Tik Tok*," July 11, 2018, https://www.reuters.com/article/us-indonesia-bytedance-idUSKBN1K10A0 (accessed September 27, 2020).

[70] Ikhwan Hastanto, "Indonesian Government Denies Involvement in Spreading Hoaxes About Student Protesters," *Vice*, October 9, 2019, https://www.vice.com/en_asia/article/7x5egd/indonesian-government-denies-involvement-spreading-hoaxes-about-student-protesters (accessed September 26, 2020).

Social media accounts of government critics have been taken over to spread libelous information and discredit their owners.[71] In August 2020, an epidemiologist who had been critical of the government's Covid-19 policies had his Twitter account taken over, and pictures aimed at damaging his reputation were posted.[72]

Lack of Localised Digital Security Training

According to interviewees, digital security awareness is very low, and many activists don't see digital security as an issue. There are also concerns that training programs and materials are difficult to understand, and that even for HRDs with higher levels of tech literacy, the workshops on digital security are simply too complicated.

> *"Digital security trainings are coming from a very western perspective. I can't imagine how the local journalists who don't know English can understand these. There is very little information in Bahasa. We have some, but digital security practices are always updating. So it's hard to keep up to date."*
>
> *- DIGITAL RIGHTS ADVOCATE*

The popularity of video conferencing has exploded in Indonesia due to Coronavirus. One interviewee suggested that digital security training workshops could be delivered online, increasing accessibility while also cutting costs.

> *"We include digital security in our standard operating procedures — but I don't think it's enough to just write it in our SOP. We need to regularly raise awareness and discuss digital security practices. We need to make this discussion more regular, like one day a month."*
>
> *- HUMAN RIGHTS DEFENDER*

Newsrooms and civil society organisations must pay more attention to the digital vulnerabilities of journalists and HRDs — and until that happens, digital security practices in Indonesia will remain inadequate.

> *"It is not fair for journalists to try and learn and find help by themselves. The newsroom management should schedule the training workshops and allow journalists to participate. They need to free the journalists so they can learn about digital security."*
>
> *- MEDIA FREEDOM ADVOCATE*

● ● ● ●

[71] Pitra Hutomo, "#BebaskanRavio: Free Ravio Patra and reveal the WhatsApp hackers," *Coconet*, April 24, 2020, https://coconet.social/2020/bebaskan-ravio-patra-privacy/ (accessed September 26, 2020).

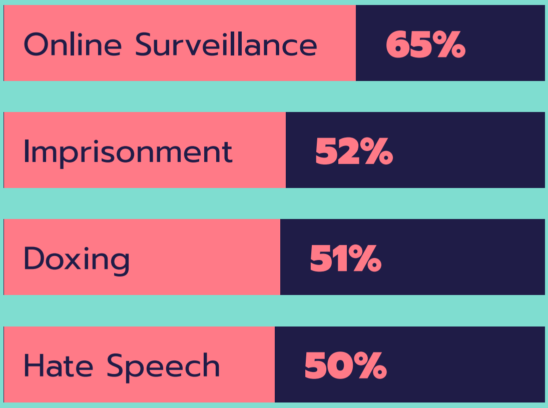
[72] Alya Nurbaiti and Budi Sutrisno, "Civil groups condemn cyberattacks on Indonesian government critics," *The Jakarta Post*, August 23, 2020, https://www.thejakartapost.com/news/2020/08/23/civil-groups-condemn-cyberattacks-on-indonesian-government-critics.html (accessed September 26, 2020)

INDONESIA: DIGITAL SECURITY PRACTICES

During our research for **Ground Safe**, we deployed an online survey through our partners to gather empirical data about digital security needs and practices. Human rights defenders were surveyed to learn about their digital security practices, thoughts, and concerns.

The data presented below comprises responses from 90 journalists, activists, and digital rights advocates living and working in Indonesia.

Perceived Risk Level



Email

94%	use **GMAIL**
23%	use **YAHOO**
23%	use **PROTONMAIL**
11%	use **OUTLOOK**

SECURE STORAGE

How often on device storage is encrypted

42%	27%	31%
Encrypted	Unencrypted	Unsure

Video Calls

Most people use WhatsApp and Zoom for video calls. Over 50% of people use WhatsApp multiple times a day, and 25% of people use Zoom every day.

PGP

22%	Use **PGP** to encrypt their emails
29%	Don't use **PGP** at all
31%	Don't know how to use **PGP**
18%	Aren't sure if they are using **PGP**

Safety through anonymity & encryption

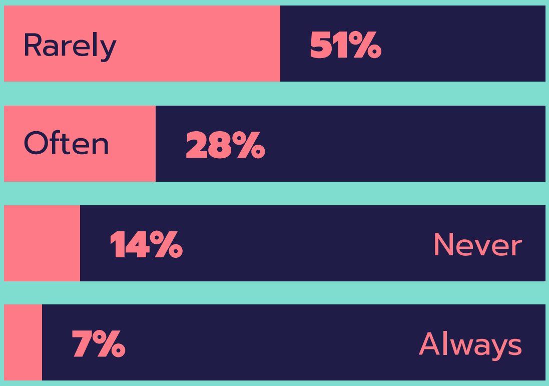
90% Believe encrypted communications are important for their safety

74% Believe anonymous communications are important for their safety

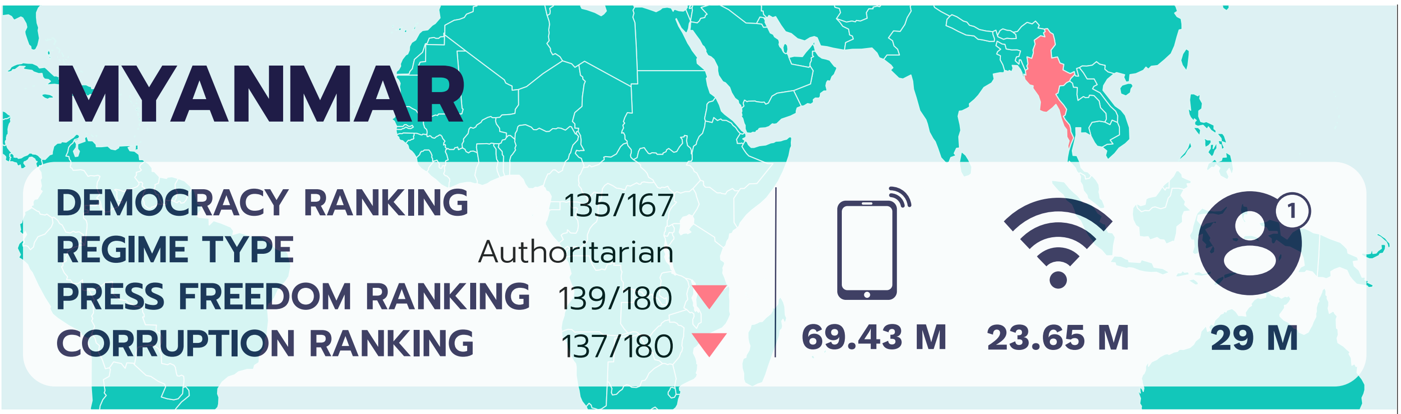
Instant Messaging Daily Use

98%	Use **WHATSAPP**
20%	Use **TELEGRAM**
19%	Use **SIGNAL**
12%	Use **WIRE**

Tools & strategies that improve digital security: FREQUENCY OF USE



45% Are **NOT** confident using secure tools



MYANMAR

DEMOCRACY RANKING	135/167	
REGIME TYPE	Authoritarian	
PRESS FREEDOM RANKING	139/180	▼
CORRUPTION RANKING	137/180	▼

69.43 M	23.65 M	29 M

Coup Disrupts Path to Democracy

After almost 50 years of dictatorship, Myanmar's military leaders signalled a transition to civilian rule in 2011. A political reform process began; media restrictions were relaxed, and new laws were passed protecting the right to demonstrate and form unions.

Myanmar's movement towards democratic reform attracted much-needed foreign investment as new telecommunications actors entered what was previously a state-dominated telco environment. Access to telecommunication technologies rapidly increased, for example: the cost of SIM cards fell from several thousand US dollars under the military dictatorship to as low as a few US dollars.

Smartphone prices also plummeted due to an influx of low-cost Chinese imports, giving millions of people easy access to social media and a vastly increased capacity to communicate in ways which were unimaginable prior to the reforms.[73]

In November 2015, the first free general elections since 1990 were held, resulting in a victory for the National League for Democracy (NLD). A new government was formed, with former political prisoner and Nobel Peace Prize winner Aung San Suu Kyi as State Counsellor.

However, the democratically elected NLD's power has been limited by constitutional provisions and laws which continue to give the military power and influence.[74]

As of time of writing, Myanmar has once again returned to military rule following claims of voting irregularities by the opposition and the military. A coup in January 2021 saw Suu Kyi placed under house arrest and a state of emergency declared by the military.

Internet freedom in Myanmar is expected to dramatically decline over the coming months, and digital attacks against critics and protests will likely increase. Reports of internet access restrictions have already begun to surface in the immediate aftermath of the coup, and it is likely this will continue in the upcoming months.

Weaponising Social Media and Internet Access

Despite political reforms in Myanmar, underlying tensions have worsened over the past decade, especially between the majority Buddhist Burmese and minority

[73] Susan Cunningham, "Myanmar: 45 Million Mobile Phones and the $19 3G Smart Phone," *Forbes*, August 10, 2016, https://www.forbes.com/sites/susancunningham/2016/08/10/myanmar-45-million-mobile-phones-and-the-19-3g-smartphone/?sh=b5536af4d4b4 (accessed September 26, 2020)

[74] Kristian Stokke et al., "*Myanmar: A Political Economy Analysis*," Norweigian Institute of International Affairs, 2018, https://reliefweb.int/report/myanmar/myanmar-political-economy-analysis (accessed on September 26, 2020).

Rohingya Muslims, who are not considered citizens of Myanmar.

In 2017, the Myanmar military conducted an offensive to root out the Arakan Rohingya Salvation Army (ARSA) — a militant group that claims to defend and protect the Rohingya people — after ARSA attacked police and army stations. This offensive resulted in 700,000 Rohingya fleeing to neighbouring Bangladesh.[75]

There is clear evidence that social media posts have fuelled hatred and violence towards the Rohingya, with Facebook eventually removing accounts and pages belonging to "specific hate figures" targeting the Rohingya.[76]

In June 2019, the government cut off internet access to over a million people in parts of the Rakhine and Chin states, where the Myanmar military is engaged in conflict with the Arakan Army, an armed group fighting for the autonomy of the Rakhine people. This shutdown is now known as the longest of its kind in history.[77]

More than a year later, internet access in Rakhine and Chin remains heavily restricted. Some townships have limited access to the internet through 2G cellular networks, but internet access remains shut down in the majority of the region. This continues to hamper the free flow of information, and civil society groups have expressed concern that this has affected Myanmar's COVID-19 response.[78]

Controlling the Truth

Despite movements towards democratic reform over the past decade, it soon became clear that critics of the government and the military would still not be tolerated under this new government.

In 2017, Myanmar Now chief editor Ko Swe Win was arrested for 'defaming' the anti-Muslim monk Ashin Wirathu after he allegely shared a Facebook post criticising the monk. This had a chilling effect on journalists in the country.[79]

In September 2018, two Reuters correspondents were convicted under the Official Secrets Act and sentenced to seven years in prison for their investigation into the murders of 10 Rohingya men by the army. The journalists spent over 500 days in prison before a presidential amnesty secured their release.[80]

● ● ● ●

[75] Eleanor Albert and Lindsay Maizland, "The Rohingya Crisis," *Council on Foreign Relations*, January 23, 2020, https://www.cfr.org/backgrounder/rohingya-crisis (accessed September 27, 2020).

[76] BBC News, "*The country where Facebook posts whipped up hate*," September 12, 2018, https://www.bbc.com/news/blogs-trending-45449938 (accessed September 27, 2020).

[77] Andrew Nachemson and Lun Min Mang, "Fighting in Rakhine, Chin states rage as Myanmar limits internet," *Al Jazeera*, March 5, 2020, https://www.aljazeera.com/news/2020/3/5/fighting-in-rakhine-chin-states-rages-as-myanmar-limits-internet (accessed September 27, 2020).

[78] John Liu, "Internet restrictions undermine COVID-19 response in Rakhine," *Myanmar Times*, September 6, 2020, https://www.mmtimes.com/news/internet-restrictions-undermine-covid-19-response-rakhine.html (accessed on September 26, 2020).

[79] Joseph Hincks, "A Journalist Has Been Detained in Myanmar For 'Defaming' an Anti-Muslim Monk," *Time*, July 31, 2017, https://time.com/4880102/myanmar-journalist-arrested-defamation-wirathu/ (accessed on September 26, 2020).

[80] BBC News, "*Wa Lone and Kyaw Soe Oo: Reuters journalists feed in Myanmar*," May 7, 2019, https://www.bbc.com/news/world-asia-48182712 (accessed on September 26, 2020).

In August 2020, Justice for Myanmar, a website promising to expose systemic corruption within the military, was blocked in Myanmar for spreading 'fake news'.[81]

Manipulation of online content is commonplace. Military officials were found to have been involved in social media misinformation designed to provoke racially motivated violence in several separate incidents over a five-year period.[82]

In the lead-up to the November 2020 elections, Facebook was used to spread a torrent of fake news and hate speech. The social media giant acknowledged their removal of accounts belonging to a PR firm that supported the military-backed Union Solidarity and Development Party. Facebook also removed approximately 280,000 pages during the second quarter of 2020.[83]

Digital Security Training a 'Trend'

Myanmar's civil society has strengthened considerably during the last decade — and international donors have supported media freedom projects and training programs aiming to strengthen digital security among journalists and HRDs.

One interviewee, a digital security trainer who works with organisations to create cyber security policies, says it is challenging to explain the seriousness of digital attacks because people can't imagine them.

> *"We have to make them scared. Telling a story is not enough. We have to hack them".*
>
> *- CIVIL SOCIETY ACTIVIST*

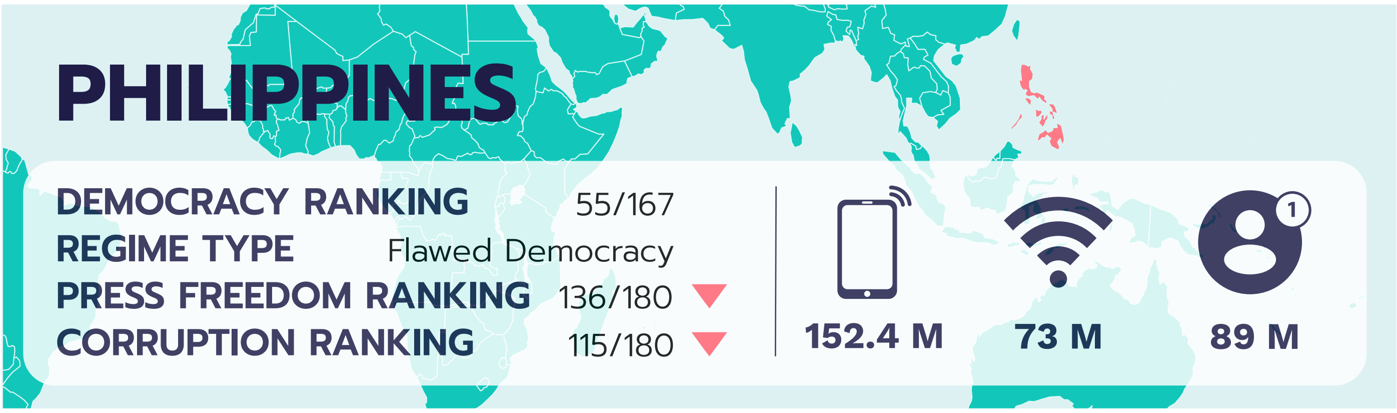
The number of digital security trainers in Myanmar is low, which also poses a challenge in scaling awareness and practice among HRDs. One interviewee expressed concern about the lacking impact of existing programs.

> *"Honestly, they just want to be part of the training workshop — it's like a trend. There is a need but we are not quite sure if there is a real demand for digital security training ... They are just attending the training, and they are not practicing digital security."*
>
> *- DIGITAL SECURITY TRAINER*

[81] Mong Palatino, "Website exposing military corruption blocked in Myanmar," *Global Voices*, September 11, 2020, https://globalvoices.org/2020/09/11/website-exposing-military-corruption-blocked-in-myanmar/ (accessed on September 26, 2020).

[82] Paul Mozur, "A Genocide Incited on Facebook, With Posts From Myanmar's Military", *The New York Times*, October 15, 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html (accessed on September 26, 2020).

[83] ABC News, "*Myanmar election see Facebook fight hate speech, misinformation*," https://www.abc.net.au/news/2020-11-08/spreading-like-wildfire:-facebook-fights-hate-speech,-misinfo/12860698 (accessed on December 10, 2020).



PHILIPPINES

DEMOCRACY RANKING	55/167	
REGIME TYPE	Flawed Democracy	
PRESS FREEDOM RANKING	136/180	▼
CORRUPTION RANKING	115/180	▼

152.4 M

73 M

89 M

Dissenters as “Terrorists”

Post-independence, the Philippines’ political landscape has remained patronage-based. Since experiencing martial law during the Marcos presidency, the Philippines has continued to grapple with corruption and inequality, with democracy eroding under the leadership of President Rodrigo Duterte.[84]

The Duterte administration has targeted those who are critical of the regime. Libel charges are continually filed against journalists and bloggers (and even ordinary users) who write critical Facebook posts. Online news network Rappler is a frequent target. Rappler CEO Maria Ressa was arrested in February 2019 for libel, found guilty in July 2020, and is currently on bail pending an appeal. If that appeal fails, Ressa could face 6 years imprisonment.[85] This precedent has led to instances of news websites proactively removing content once threatened with legal action, or at the request of authorities.

In July 2020, Duterte signed off on controversial anti-terrorism laws, giving authorities sweeping powers including the ability to conduct surveillance and wiretapping without warrants. Critics say that the “loose definition of terrorism allows the government to essentially tag any and all dissenters as terrorists without any judicial oversight”.[86]

Troll Armies: A Growth Industry

Content manipulation and disinformation occurs frequently in the Philippines, and there is evidence of government agencies and political parties spreading propaganda, attacking critics, and suppressing dissent online.[87] Troll armies

● ● ● ●

[84] Andrea Chloe Wong, “The Philippines’ Democratic ‘Backsliding’ in the Time of Duterte,” *International Policy Digest*, September 12, 2020, https://intpolicydigest.org/2020/09/12/the-philippines-democratic-backsliding-in-the-time-of-duterte/ (accessed September 25, 2020).

[85] Firstpost, “*Rappler CEO Maria Ressa faces upto six years in jail as questions emerge about freedom of media in Philippines*,” June 16, 2020, https://www.firstpost.com/world/rappler-ceo-maria-ressa-faces-upto-six-years-in-jail-as-questions-emerge-about-freedom-of-media-in-philippines-8488011.html (accessed September 25, 2020).

[86] Alec Regino, “Another nail in the coffin of the Philippines’ waning democracy,” *The Washington Post*, June 9, 2020, https://www.washingtonpost.com/opinions/2020/06/08/another-nail-coffin-philippines-waning-democracy/ (accessed September 7, 2020).

[87] Samantha Bradshaw and Philip N. Howard, “*The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*,” 2019, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf (accessed September 15, 2020).

are a growth industry in the Philippines, where they can be hired to create disinformation campaigns and spread fake news to "build artificial buzz around a product, a celebrity — or a political figure".[88]

According to one interviewee, troll armies create fake accounts that impersonate activists. These fake accounts then spread disinformation and fake news to discredit the activists, potentially exposing them to libel charges, ruining their reputations, and resulting in the dismissal of their work.

> *"Our photos are circulated online, saying we are recruiters of rebel organisations. We are getting hate messages from all over the place."*
>
> *- INDIGENOUS RIGHTS ACTIVIST*

Interviewees indicated that social media is being monitored closely by authorities, and there is a real anxiety over being doxxed and their families becoming involved.

> *"It causes friction across the family. There's thinking that all those who criticise the government are activists, and all activists are terrorists. And this being normalised across society."*
>
> *- INDIGENOUS RIGHTS ACTIVIST*

Digital Surveillance, Training, and Practices

There is evidence that the British government sold a range of spying equipment to the Duterte regime, including tools to monitor internet activity, and IMSI-Catchers, which can be used to listen to mobile phone conversations.[89] There are also concerns that WhatsApp groups are being monitored, and that mobile number harvesting is on the increase.

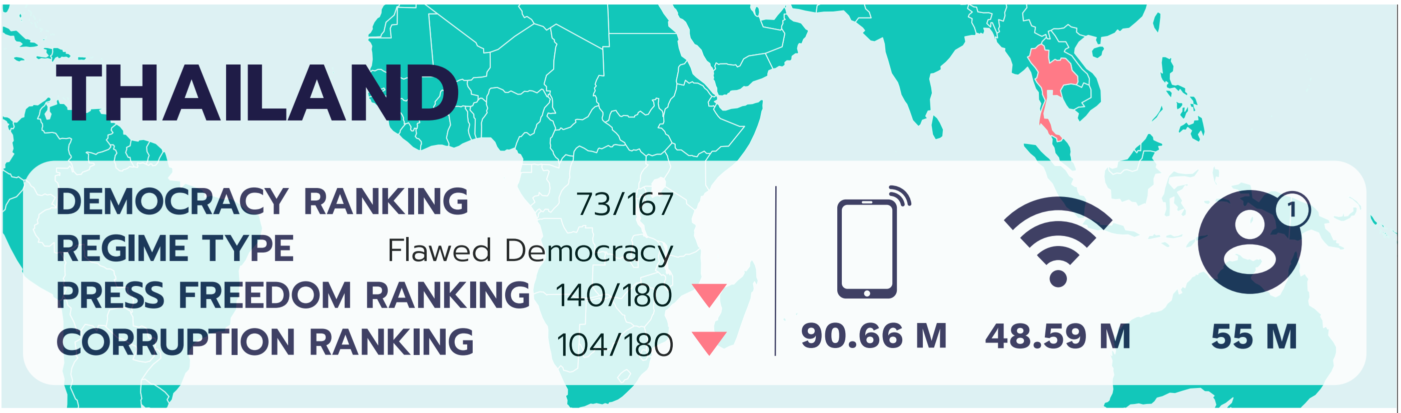
Digital security practice within the HRD community and civil society at large is generally weak. While HRDs are aware of digital threats, many use Facebook Messenger as their main means of communication because "everyone is on it". However, HRDs are increasingly using Signal for more sensitive calls.

> *"The challenge is that not everyone does the minimum required in terms of digital security."*
>
> *- DIGITAL SECURITY TRAINER*

With authoritarianism in the Philippines on the rise, there is a renewed interest and desire to use secure tools. However, effective digital security training is still a long way off, with interviewees suggesting that smaller, more personal group training programs are needed — with HRDs working in smaller towns a particular priority.

[88] Shashank Bengali and Evan Halper, "Troll armies, a growth industry in the Philippines, may soon be coming to an election near you," *The LA Times*, November 19, 2020, https://www.latimes.com/politics/story/2019-11-19/troll-armies-routine-in-philippine-politics-coming-here-next (accessed September 5, 2020).

[89] Hannah Ellis-Petersen, "Britain sold spying gear to Philippines despite Duterte's brutal drugs war," *The Guardian*, February 21, 2018, https://www.theguardian.com/world/2018/feb/21/britain-sold-spying-gear-to-philippines-despite-dutertes-brutal-drugs-war (accessed September 25, 2020).



THAILAND

DEMOCRACY RANKING	73/167
REGIME TYPE	Flawed Democracy
PRESS FREEDOM RANKING	140/180 ▼
CORRUPTION RANKING	104/180 ▼

📱	📶	👤
90.66 M	48.59 M	55 M

Pro-Democracy Protests Threatening Monarchy

Thailand is a constitutional monarchy ruled by King Maha Vajiralongkorn, whose father, King Bhumibol Adulyadej, was the world's longest reigning monarch.

Since 2005, an active Malay-Thai separatist movement has been fighting for autonomy in Southern Thailand, leading to human rights violations and the restriction of news and information dissemination in the country's South.

Thailand's Prime Minister, General Prayuth Chan-ocha, came into power following a coup in 2014, and his position was re-confirmed in the 2019 general elections. Pro-democracy activists are critical of Prayuth, who has restricted free speech and dissolved political parties in order to weaken opposition voices.

Pro-democracy protests arose in early 2020, demanding constitutional reforms. The government sought to counter this opposition and unrest by shutting down websites and social media pages connected to the protests. Google and Facebook complied with government requests,[90] taking down hundreds of videos, pages, and groups — including one group with over one million members.

With protesters demanding democratic reform and a new constitution to hold the royalist establishment accountable, it currently appears the protests will continue for some time.

Lèse Majesté Leads to Self-Censorship

A strictly enforced lèse majesté rule renders the media and the public vulnerable to imprisonment for reporting or sharing anything critical of the royal family. As a result, journalists tend to practise self-censorship on stories featuring the military or the judiciary.[91]

Thai authorities are supported by comprehensive laws to quash online dissent. The Computer-Related Crimes Act, passed in December 2016, restricts freedom of expression online. In February 2018, the National Broadcasting and Telecommunications Commission enforced a 2017 resolution requiring telecommunications operators to collect fingerprints or face scans from SIM card registrants. This information is stored in a central database, enabling easy identification of registrants by authorities.

In May 2019, the Cyberspace Emergency Act was enacted, giving the government

[90] Apornrath Phoonphongphiphat, "Thailand to block 2,000 websites ahead of pro-democracy protests," *Nikkei Asia*, September 18, 2020, https://asia.nikkei.com/Politics/Turbulent-Thailand/Thailand-to-block-2-000-websites-ahead-of-pro-democracy-protests (accessed on September 26, 2020).

[91] BBC, "Thailand country profile", *BBC News*, March 7, 2019, https://www.bbc.com/news/world-asia-15581957 (accessed on September 25, 2020).

sweeping powers to access personal data and communications without judicial review. Nine internet users were charged for sharing false information during elections in 2019, and three newly elected members of congress from the Future Forward Party (FFP) were charged under the act for criticising the junta.[92]

From Theory to Practice

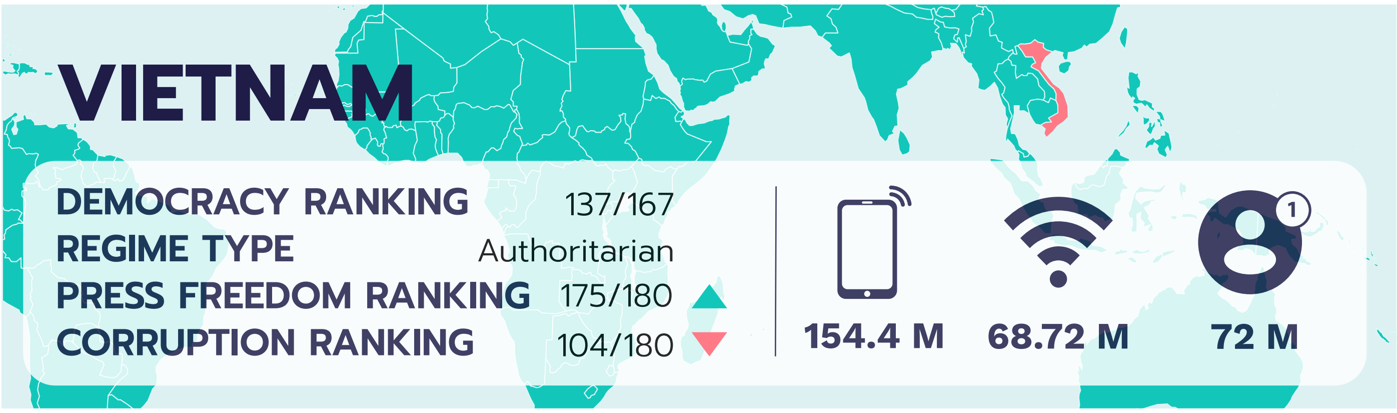
High levels of ICT literacy among young activists have made it easier for trainers to promote digital security awareness and proper use of digital security tools. However, trainers are unsure if activists will have the discipline or resources to practice what they learn.

According to an interviewee working as a digital security trainer, Line is more popular than WhatsApp amongst average members of the public. Activists and HRDs are beginning to use Telegram or Signal to communicate sensitive information — or otherwise whenever they feel the need for additional security. Interviewees indicated that a pressing threat is when activists are arrested and forced to surrender passwords to their accounts, giving authorities access to sensitive information and enabling them to monitor closed groups.

We learned of one international organisation which has invested the necessary resources to conduct digital security training programs for local trainers, aiming to improve local engagement. However, such instances are rare, with most organisations opting to send in expert trainers from outside the country to conduct digital security workshops. Reliance on external trainers can lead to issues with comprehension and engagement in training workshops.

> *"In the deep south of Thailand, they did not understand my central Thai accent so we recruited trainers who were local and put them through training of the trainer programs"*
>
> *- DIGITAL SECURITY TRAINER*

[92] Freedom House, "Thailand", *Freedom House*, May 31, 2019, https://freedomhouse.org/country/thailand/freedom-net/2019 (accessed on September 26, 2020).



VIETNAM

DEMOCRACY RANKING	137/167
REGIME TYPE	Authoritarian
PRESS FREEDOM RANKING	175/180 ▲
CORRUPTION RANKING	104/180 ▼

📱 154.4 M

68.72 M

72 M

Detained Over Facebook Posts

Vietnam's recent history is marked by the ideologically-driven war between Russia- and China-backed North Vietnam, and US-backed South Vietnam. Following the withdrawal of American troops in 1973, fighting continued despite a ceasefire, and by mid 1975, South Vietnam fell to communist North Vietnam. The country was formally re-unified and continues to be ruled by the Communist Party of Vietnam.[93]

Vietnam has pursued a market-oriented economic transition known as 'Doi Moi', or 'revolution', and has seen impressive economic growth, positioning the country to become a middle-income country before 2030.

However, Vietnam has an appalling human rights record, and the Communist Party keeps a tight reign over its people, controlling all political and social organisations and punishing those who criticise its rule.[94] Since the country began to gain widespread internet access in the late 1990s, the Community Party has attempted to mitigate the internet's potential threat to its authority. A cybersecurity law introduced in January 2019 ramped up government power to monitor information and communication systems, and block and delete online content and data. This law also required user data to be hosted only on servers within Vietnam.[95]

By December 2019, 274 activists were reportedly in detention in Vietnam — many of them for critical posts on Facebook.[96]

Enforcing Social Media Compliance

There are an increasing number of reports indicating that Vietnam uses sophisticated digital monitoring and surveillance technologies, and is moving towards China's model of internet control.[97] Authorities claim they have

[93] History.com, "*Vietnam War Timeline*," February 26, 2020, https://www.history.com/topics/vietnam-war/vietnam-war-timeline (accessed 24, 2020).

[94] Human Rights Watch, "*World Report 2019: Vietnam — Events of 2018,*" 2019, https://www.hrw.org/world-report/2019/country-chapters/vietnam (accessed September 25, 2020).

[95] Justin Sherman, "Vietnam's Internet Control: Following in China's Footsteps?," *The Diplomat*, December 11, 2019, https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/ (accessed September 25, 2020).

[96] Civicus, "*Alarming Number of Activists Being Jailed in Vietnam for "Anti-State" Facebook Posts*," December 13, 2019, https://monitor.civicus.org/updates/2019/12/13/alarming-number-activists-being-jailed-vietnam-anti-state-facebook-posts/ (accessed September 25, 2020).

[97] Justin Sherman, "Vietnam's Internet Control: Following in China's Footsteps?," *The Diplomat*, December 11, 2019, https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/ (accessed September 25, 2020).

a 10,000-strong internet task force to monitor online posts, with the capacity to scan up to 100 million news items a day.[98]

Crackdowns intensified in 2020. Between January and March, 654 people were summoned to police stations in relation to Coronavirus-related Facebook posts — 146 of them were fined, and the rest were forced to delete their posts.[99]

Following a decree in April,[100] Facebook agreed to increase the censorship of posts deemed 'anti-state,' after its local servers were taken offline by authorities, slowing traffic to the platform to a crawl — a decision which received much criticism from rights organisations.[101]

Google also complied with government requests to remove content, removing over 5000 videos that the government claimed were defamatory.[102]

P2P Digital Security Training

Vietnam will continue to be a dangerous place for activists and journalists. Among high-risk HRDs, there is an awareness of digital security practices, but phishing and malware attacks are increasing. HRDs are concerned their emails have been hacked, and some interviewees indicated that there was an increase in their WhatsApp accounts being taken over or accessed.

> *"I got a message saying that my WhatsApp account had been accessed by two other devices. On the same night, I got a notification from Google that someone was trying to access my email."*
>
> *- HUMAN RIGHTS DEFENDER*

Facebook and Facebook Messenger remain popular, especially as tools for advocacy and mobilisation, because they provide quick and easy access to large audiences. WhatsApp is also very popular, though HRDs are slowly switching their sensitive calls to Signal. But despite the use of a more secure messenger, there is a lack of familiarity with features like disappearing messages and two-step authentication.

> *"We conduct digital security training programs for activists, but after that they don't have that habit of practicing it."*
>
> *- HUMAN RIGHTS DEFENDER*

It is extremely dangerous and difficult to conduct effective digital security training programs inside Vietnam, so digital security education is predominantly peer-based. Some organisations based outside of Vietnam have residency programs to upskill Vietnamese HRDs so they

● ● ● ●

[98] The Straits Times, "*Vietnam Rolls out Web Monitor to Control 'False Information'*," November 1, 2018, https://www.straitstimes.com/asia/vietnam-rolls-out-web-monitor-to-control-false-information (accessed September 25, 2020).

[99] Amnesty International, "*Viet Nam: Facebook must cease complicity with government censorship*," April 23, 2020, https://www.amnesty.org/en/latest/news/2020/04/viet-nam-facebook-cease-complicity-government-censorship/ (accessed September 25, 2020).

[100] Luong Dinh Khai, "Vietnam: Regulation of online activity," *Data Guidance*, May 2020, https://www.dataguidance.com/opinion/vietnam-regulation-online-activity (accessed September 25, 2020).

[101] James Pearson, "Exclusive: Facebook agreed to censor posts after Vietnam slowed traffic - sources," *Reuters*, April 22, 2020, https://www.reuters.com/article/us-vietnam-facebook-exclusive/exclusive-facebook-agreed-to-censor-posts-after-vietnam-slowed-traffic-sources-idUSKCN2232JX (accessed September 25, 2020).

[102] Freedom House, "*Freedom on the Net 2019: Vietnam*," 2019, https://freedomhouse.org/country/vietnam/freedom-net/2019 (accessed September 25, 2020).

can return to Vietnam and share their knowledge with others. However, the low technical literacy of most HRDs, combined with the country's restrictive environment, make it difficult to scale up digital security capacity.

> *"We need a lot of help. Every time something happens, we don't have someone to go to. We need an expert."*
>
> *- HUMAN RIGHTS DEFENDER*

NEXT STEPS

Digital security and internet freedoms for HRDs is a global issue.

This report focuses on Southeast Asia, South Asia, MENA, and East Africa, and further research is needed to understand the digital security challenges and requirements of HRDs in other regional contexts.

Early indicators in Europe, Australia, and the Pacific from research undertaken by our partners, indicate that HRDs do have an awareness of digital security threats, but that they have limited willingness and/or capacity to sufficiently protect themselves.

While concerns over online surveillance are common, Western European HRDs were found to have higher technological and digital security literacy compared to their Eastern European counterparts. Feedback from Hungarian and Czech Republic whistleblowing organisations highlighted the “first contact” problem, with only 15% of whistleblower disclosures coming via their secure dropbox — and “lots” coming through Facebook. An interviewee from Spain indicated duty of care by journalists was lacking when it came to the safety of their sources, and that most whistleblowers were not familiar with identity-protecting digital security tools.

In Australia, a slew of cyber laws have undermined the privacy and digital security of journalists and activists. In late 2015, the government passed Australia’s metadata retention scheme, making it compulsory for telecommunications and internet providers to store metadata for a period of two years. In late 2018, the Assistance and Access Bill was passed, which can compel technology companies to create vulnerabilities that give authorities access to encrypted communications. Journalism groups and activists we spoke with did indicate awareness of the surveillance capabilities of governments and corporations, but for most, digital security practice was not a priority.

Across the Pacific, the level of internet use has dramatically increased in recent years. Interviewees working on issues related to extractive and logging industries were aware of the need to increase digital security practices, but indicated the accessibility and usability of tools needed to improve. Interviewees also suggested that given the increased geo-political interest in the region, and the rise in critical local voices, there is an urgent need to increase the digital security practices of journalists and activists.

Further Research

We are eager to continue our research into other countries and regions, and we look forward to collaborating with regional partners to better understand the digital security needs and practices of HRDs.

If you are interested in working with us, contributing to future research, or providing constructive comments or feedback on this report, please contact us at team@optf.ngo

If you would like to follow our work and keep up to date with our progress, you can subscribe to our email lists here:

ASL19

https://asl19.org

EngageMedia.org

https://engagemedia.org

blueprint for FREE SPEECH

https://blueprintforfreespeech.net

OPTF

https://optf.ngo

ppmn. Indonesian Association for Media Development

https://ppmn.or.id/

Ground Safe

Assessing the digital security needs and practices of human rights defenders in Africa, MENA, South Asia, and Southeast Asia

Published March 5, 2021

ISBN 978-0-646-83468-9

9 780646 834689 >