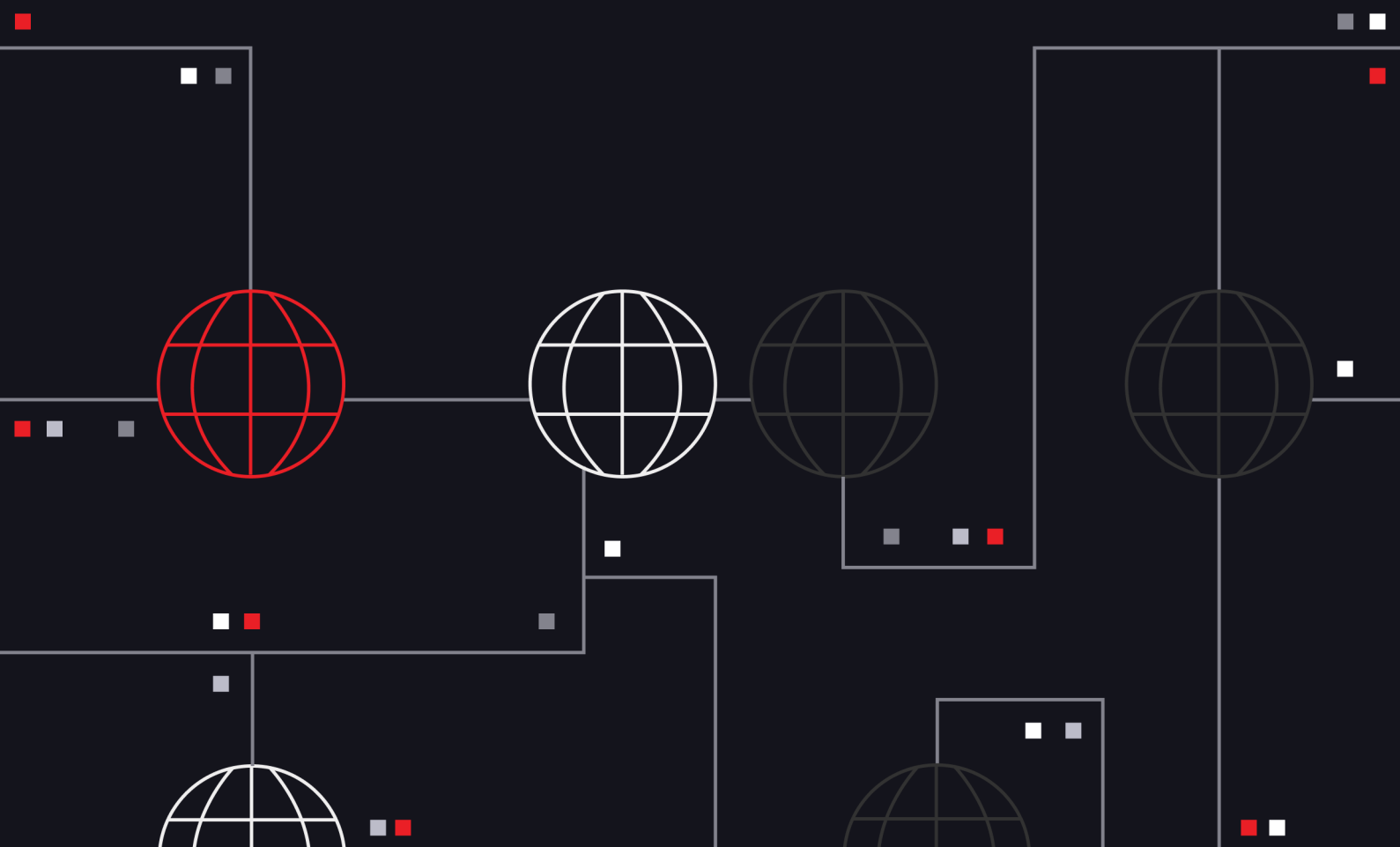
EngageMedia

The State of Digital Security Localization in Southeast Asia: A Snapshot

September 2022



EngageMedia is a nonprofit that promotes digital rights, open and secure technology, and social issue documentary. Combining video, technology, knowledge, and networks, we support Asia-Pacific and global changemakers advocating for human rights, democracy, and the environment. In collaboration with diverse networks and communities, we defend and advance digital rights.

We envision a world where human rights, democracy, and the environment are respected by Asia-Pacific businesses and governments — where civil society meaningfully participates in meeting social and environmental challenges.

EngageMedia was founded in 2005 to develop an Asia-Pacific open source social issue film platform and has evolved to lead and support advocacy on various issues, convening and collaborating with changemakers across the region.

Learn more at engagemedia.org.

Authors

Erin McConnell, Localization and Community Consultant

Khairil Zhafri, Digital Rights and Technology Manager, EngageMedia

Contributors

Ashraf Haque, Digital Security Specialist, EngageMedia

Ba Hein, Digital Rights Coordinator (Myanmar), EngageMedia

Kade Thossaphonpaisan, former Digital Rights Project Officer (Thailand), EngageMedia

Pradipa P. Rasidi, Digital Rights Program Officer (Indonesia), EngageMedia

Vino Lucero, Project and Communications Manager, EngageMedia

Yawee Butrkrawee, Digital Rights Manager (Mekong), EngageMedia

Editing

Katerina Francisco, Editorial Coordinator, EngageMedia

Sara Pacia, Communications and Engagement Manager, EngageMedia

Management and Oversight

Andrew Lowenthal, Board Member and Senior Adviser, EngageMedia

Egbert Wits, Research and Program Senior Manager, EngageMedia

Red Tani, Programs and Communications Director, EngageMedia

Published September 2022

Supported by the Swedish International Development Cooperation Agency (SIDA)

TABLE OF CONTENTS

I. INTRODUCTION

Journalists, activists, and civil society in Southeast Asia rely heavily on digital technologies and online media to do their work, more so now than before the COVID-19 outbreak. They are increasingly exposed to digital security risks and threats, as many use less secure tools and do not practise good digital hygiene in their day-to-day work. This happens, in part, because they have limited access to digital security resources that are localized for their specific regional and local contexts. It is, therefore, crucial that more secure, privacy-respecting digital solutions and resources are made available and accessible to these groups in their languages.

In this scoping review, we assess a selection of tools that have digital security as a core functionality. Most of the tools surveyed are free and open-source projects maintained by independently run communities. We also review ten digital security guides that cover a wide range of digital security topics.

Intended for human rights advocates – especially those focused on digital rights in Southeast Asia – the report has the following aims:

a. Provide a snapshot of the availability of digital security tools and guides in five major Southeast Asian languages: Burmese (မြန်မာဘာသာ), Filipino, Indonesian (Bahasa Indonesia), Khmer (ភាសាខ្មែរ), and Thai (ไทย);

b. Review the ecosystem that supports localization of the tools and guides into the five target languages; and
c. Inform future digital security localization initiatives, especially in Southeast Asia.

The localization of digital security tools and guides is especially important in Southeast Asia. The ongoing regional political and human rights crises have increasingly constricted civic spaces. Against this backdrop, journalists and activists are fast becoming targets of digital surveillance, online censorship, and other cyberattacks.

In Myanmar, for example, deposed elected officials and activists have turned to the internet to organise civil disobedience campaigns and protests in response to the February 2021 coup. In retaliation, the military has used internet censorship and shutdowns to stifle the pro-democracy movement. In Cambodia, the postponed rollout of the National Internet Gateway has raised serious concerns over mass surveillance and widespread censorship for around 9 million internet users. When implemented, all online traffic in Cambodia must pass through the gateway, making it a potent tool to restrict dissent, curtail rights, and stifle advocacy on the internet. Elsewhere, governments across Southeast Asia are using more sophisticated means to interfere with internet freedom. The proliferation of surveillance technologies like the Pegasus spyware makes journalists and activists more vulnerable.

Having tools and guides available and accessible in local languages will go a long way in helping protect journalists and activists. As they work and operate more in digital spaces, advocates for human rights and democracy in Southeast Asia will increasingly rely on localized digital security resources.

Localization is generally a two-step process: translate and review. First, the strings – text elements of the user interface – get translated from the source language into the target language. The translation is typically done string by string and may not be consistent or accurate across the whole user interface. Each translated string then gets reviewed for overall consistency and accuracy. The review process usually considers improvements of the translated strings for the tool as a whole.

This report assesses the extent to which selected digital security tools and guides are localized into five target languages using the following measures:

Rate of Translation – The percentage of strings translated into the target language out of the total strings in the source language.

Rate of Review – The percentage of strings reviewed in the target language out of the total strings in the source language.

We derive these measurements from the analytics information gathered from the collaborative localization platform – also known as globalisation management system (GMS) – for each digital security tool. We also observe where and how the localized versions are maintained. Where possible, we note the extent of localization done for each target language. All information gathered on the localization of these digital tools and guides represents the period between 16 February and 24 March 2022. This report may not reflect changes outside this review period.

II.

DIGITAL SECURITY LOCALIZATION IN SOUTHEAST ASIA

The Localization Ecosystem

Over the past decade or so, localization has been prioritised by more organisations in the nonprofit and for-profit sectors alike to make content more accessible and relevant for a wider, global audience. This increased focus on making products 'world-ready' has meant that developers and content creators have begun to integrate localization considerations (internationalisation, translation, and design) earlier on in the development process, and more tools and resources are available to make that integration easy. This has also been the trend across open-source digital security software and resources. With few exceptions (tools that cannot support certain Southeast Asian scripts like Burmese and Khmer, such as the Signal Desktop app), every digital security tool surveyed for this project is being localized into more than one language, including Southeast Asian languages.

As the demand for 'world-ready' content increased, translation and localization tools evolved to meet localization needs, introducing web-based, collaborative localization platforms that support open-source-model community contributions. The majority of the digital security and productivity tools that we surveyed are hosted on these web-based localization platforms, where large communities of volunteers can provide crowdsourced translations and user feedback. Opening up the localization process

through these collaborative platforms, which also integrate computer-assisted translation tools (translation memory, concordancers, advanced search and filtration), has made contributing to localization as a volunteer non-professional translator significantly easier. This is particularly important for open-source projects that may not have funding to finance localization, and for speakers of underrepresented and marginalised language communities whose languages are not prioritised for localization. The reliance on a crowdsourcing model, however, also presents its own challenges, as the quality of translations would depend on the technical and linguistic skills of volunteer translators.

These web-based localization platforms were initially tailored for localizing software and websites, and not for localizing long-form text and documentation. For this reason, most of the digital security guides reviewed in this survey are still being localized in text files and collaborative tools like Google Docs, or directly in a content management system (CMS).

Of the web-based collaborative localization platforms, Transifex and Weblate currently host the majority of the tools reviewed in this survey.

Weblate is an open-source platform that offers free hosting for open-source projects on Hosted Weblate, and also offers self-hosting for projects (like SecureDrop and Tails) that need more customisation or increased security.

Transifex, once open-source but now closed, hosts by far the most digital security tools in large part through the Localization Lab Hub on the platform.

While a lot of headway has been made in localizing open-source and digital security software into Burmese, Filipino, Indonesian, Khmer, and Thai, it appears that much of that work has been done by individual volunteers and enthusiasts – and possibly local organisations. As far as this review could find, there are no regional networks or initiatives focused specifically on open-source software or digital security content localization into one or more of the survey languages. Organisations like Mozilla are well-known for their community-driven localization, and while they do have documented localization teams for all five languages reviewed in this survey, information on the language team pages of the

Mozilla localization wiki is out-of-date and it is uncertain how active the teams are. The Mozilla community also focuses exclusively on their own products, as do other groups of volunteers working on open-source projects like LibreOffice, GNOME, and OpenOffice. The only known organisation working across multiple open-source projects, and primarily digital security and safety tools and resources, is Localization Lab, which coordinates community-driven localization of digital security and circumvention technologies in collaboration with volunteers and local organisations and has built networks across all five target languages.

The following sections provide an overview of the state of digital security localization in Burmese, Filipino, Indonesian, Khmer, and Thai. At the end of this report, we explore ideas for moving digital security in Southeast Asia forward.

Burmese

Partial or Full Released Localizations: Bitmask (Android), Briar (Android, Desktop, User Manual), Censorship.no! (CENO), Firefox, GlobaLeaks, LibreOffice, Mailvelope, Orbot Psiphon (Android, iOS, Windows), Signal (Android, iOS), Tella (Android), Tor Browser (Desktop), VeraCrypt

Additional Tools with Localization Progress: Brave, ProtonMail, KeePassXC (Desktop, Browser Extension)

Localized Guides: Digital First Aid Kit, Holistic Security Protocol for Human Rights Defenders, Safe Sisters Guide

Partially Localized Guides: Security-in-a-Box, Surveillance Self-Defense

Despite Myanmar having limited access to externally developed technologies until the past decade, and the additional technical hurdle of the dominant Burmese font being non-Unicode until recent years, a relatively wide range of digital security tools and resources has been localized into Burmese. Prominent open-source productivity tools like Firefox and LibreOffice are available in Burmese along with end-to-end encrypted messaging, file

sharing, email and full-disk encryption, as well as circumvention tools that range from virtual private networks (VPNs) to tools using peer-to-peer technology and the Tor network.

Half of the digital security guides selected for review are also fully or partially localized into Burmese. At the time of this survey, the Burmese localizations of the Digital First Aid Kit, Holistic Security Protocol for Human Rights Defenders, and Safe Sisters Guide are up-to-date with the original English guide. Currently, not all of the Surveillance Self-Defense guides and resources are available in Burmese due to the Electronic Frontier Foundation's ongoing update of guides; however, all of the guides currently available in Burmese are up-to-date with the original English versions edited before April 2021. Security-in-a-Box is also available in Burmese; however, it is important to note that the guides are not up-to-date with the English original which was fully revised from late 2021 to early 2022. While the content in many of the guides is still useful, the tool guides and references are outdated.

Though these tools and guides are currently available in Burmese, it is important to remember that as software and guide updates roll out, continued maintenance of localized resources will be necessary to ensure translations are still usable and will not be removed. Localization of a number of these projects was done by individuals and local organisations (many of whom contributed to the resources available in this repository). However, a large portion of the localization of digital security tools included in this survey was coordinated by international organisations in direct response to the military coup in early 2021. An influx of funding to support individuals in Myanmar resulted in the initial localization of digital security and safety resources. Going forward, the challenge will be maintaining the localization of these resources.

Filipino

Partial or Full Released Localizations: Firefox, Orbot, Signal Android

Localized Guides: Digital Hygiene 101, Holistic Security Protocol for Human Rights Defenders

Across the board – digital security-focused tools and open-source productivity tools like web browsers, email clients, and word processors – there is a severe lack of tools available in Filipino. Of the resources that were reviewed for this survey, only three tools – Firefox, Orbot, and Signal for Android – had full or partial translations in Filipino. Additionally, there is nearly zero Filipino localization in progress on any of the other tools surveyed. One possible reason for this lack of representation is the relatively high English literacy rates in the Philippines where English is also an official language. With such a large English-speaking population, investment in localization into Filipino and other languages spoken in the Philippines has likely not been prioritised by commercial and non-commercial organisations alike.

Of the 13 digital security guides reviewed for this project, two are fully localized into Filipino and up-to-date with the original English guides at the time of this survey. In both guides, content on physical safety and digital security best practices are provided; however, neither guide contains the range of technical digital security overviews and tool guides found in resources like Surveillance Self-Defense, Security-in-a-Box, Umbrella, or Totem. This leaves a gap in access for individuals who may use applications in English but would prefer to read technical documentation and learn about complex technical concepts in Filipino.

Indonesian

Partial or Full Released Localizations: Firefox, GlobaLeaks, KeePassXC, LibreOffice, Orbot, ProtonMail (Webmail, Android, iOS), Psiphon (Android, iOS, and Windows), Signal (Android, iOS, and Desktop), Thunderbird, Tor Browser (Desktop and Android)

Localized Guides: Digital First Aid Kit, Digital Hygiene 101

Partially Localized Guides: Security-in-a-Box, Surveillance Self-Defense

Compared to other target languages in this survey, the localization of digital security tools into Indonesian has shown the most progress. More than a third of the tools reviewed have been fully or almost fully translated into Indonesian (i.e., over 90 percent of the source words translated). These tools range from productivity and communication tools (Brave,

Firefox, LibreOffice, OpenOffice, ProtonMail, and Signal) to circumvention and encryption tools (such as GlobaLeaks, Orbot, Psiphon, Tor Browser, and VeraCrypt). On average, almost two-thirds of the source words of the tools surveyed have been translated into Indonesian. However, there is still a lot of room for improvement in the Indonesian localization reviews. The review rate is considerably lower at just above 15 percent.

Only two out of 13 digital security guides surveyed have been localized into Indonesian with up-to-date content. These guides – Digital Hygiene 101 and Digital First Aid Kit – provide elementary physical safety tips and digital security best practices. Both guides are useful for human rights defenders in general, but they lack the technical instructions available in resources like Security-in-a-Box and Surveillance Self-Defense, which are localized into Indonesian but have not been updated to match the English version. In our review, we also found inconsistencies concerning the quality of the translated guides. Security-in-a-Box, for example, contains phrases that were inadequately translated from English such as the usage of *garis api* to refer to "firewall". Parts of the Digital Hygiene 101 in Indonesian read like machine translation and the Indonesian version of the Digital First Aid Kit has HTML rendering issues that impair readability. Many practitioners stand to gain from the localized versions of other good technical guides like Umbrella and Totem, which are not yet available in Indonesian.

Khmer

Partial or Full Released Localizations: Firefox, GlobaLeaks, Onion Browser, Orbot, OnionShare, OpenOffice, Psiphon (Android, iOS, Windows), Signal (Android, iOS, and Desktop)

Partially Localized Guides: Security-in-a-Box, Surveillance Self-Defense

Only a handful of digital security tools surveyed have been fully or almost fully translated into Khmer (i.e. more than 90 percent of the source words translated). These are mostly circumvention and anonymity tools like Onion Browser, OnionShare, and Tor Browser. Apart from these tools, the iOS and Android Signal apps have also been fully translated into Khmer. A number of tools such as Mailvelope, Psiphon, and Thunderbird show a promising

rate of translation driven by ongoing localization initiatives. The focus on localizing these categories of tools reflects the needs of activists working in the Khmer language. The localization review, however, needs more attention to match the translation effort.

Despite encouraging progress in the Khmer localization of tools, practical digital security guides in this target language are scarce. Only Security-in-a-Box and Surveillance Self-Defense are available in Khmer, although they have not been fully updated to match the English version. Given the shrinking space for civil society in Cambodia, having these guides localized into Khmer will be advantageous in mitigating digital security risks and threats among local human rights defenders.

Thai

Partial or Full Released Localizations: Firefox, GlobaLeaks, KeePassXC, LibreOffice, Mailvelope, Orbot, OpenOffice, Psiphon (Android, iOS, and Windows), Signal (Android, iOS, and Desktop), Thunderbird, Tor Browser (Desktop), TunnelBear (Android and iOS)

Localized Guides: Digital First Aid Kit, Digital Hygiene 101

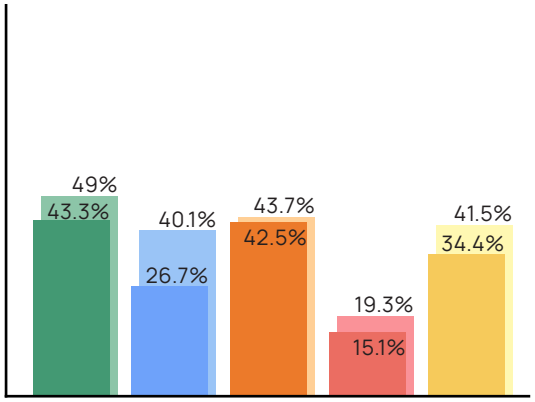
Partially Localized Guides: Security-in-a-Box, Surveillance Self-Defense

In general, Thai localization is focused on a range of productivity software and internet browsers, whistleblowing and file-sharing tools, circumvention and anonymity tools, and secure messaging apps. Tools like Firefox, GlobaLeaks, Orbot, OpenOffice, Signal, and Thunderbird are fully or almost fully translated (over 90 percent of source words translated) into Thai and their review rates do not fall far behind. Circumvention and anonymity tools like Onion Browser and Tor Browser show good localization potential. The translation and review rates for these tools are indicative of growing localization interest. One notable exception is Psiphon, a popular tool in the same category, which does not get the same level of attention for Thai localization.

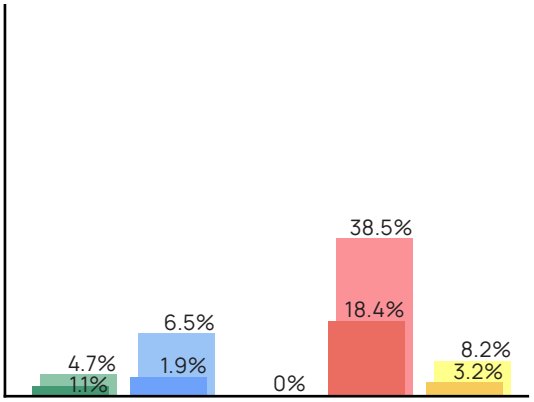
Of the 13 digital security guides in the survey, four have been localized into Thai to varying degrees. The Digital First Aid Kit and Digital Hygiene 101 have been fully translated into Thai while Security-in-a-Box and Surveillance Self-Defense are only partially translated. The latter two are around two to three years out-of-date compared to the English versions. Other important guides like Umbrella and Totem are not yet available in Thai.

III. DIGITAL SECURITY TOOLS

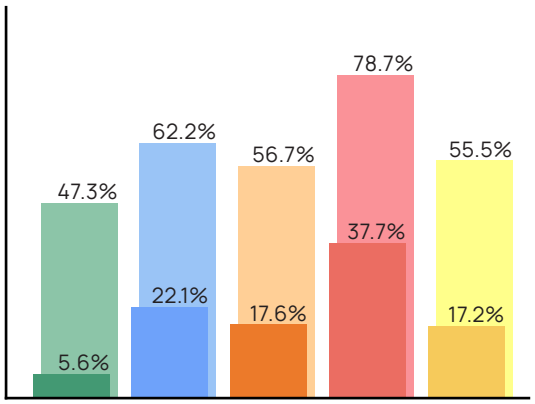
We have grouped the digital security tools surveyed into the four broad categories below, with the translation rate and review rate captured from the localization platforms for each language. A detailed description of each of the digital security tools within these categories is provided after a short analysis of this graph.



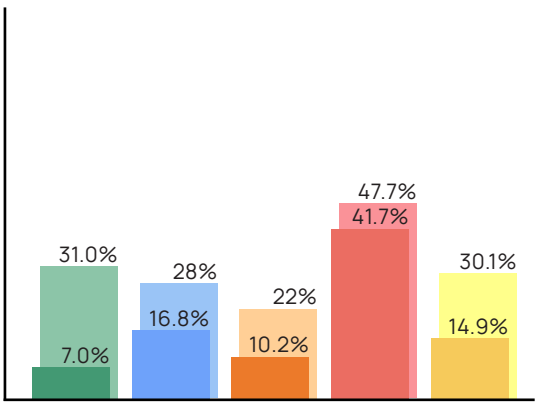
BURMESE
(မြန်မာဘာသာ)



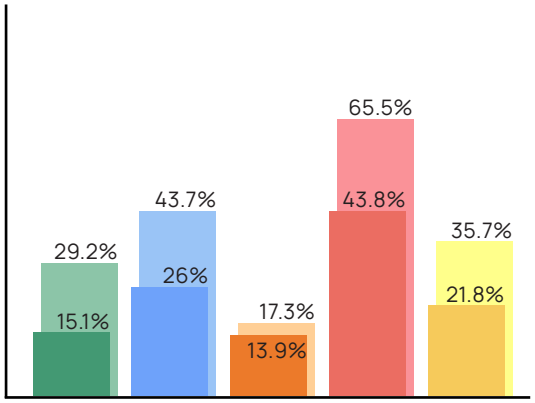
FILIPINO



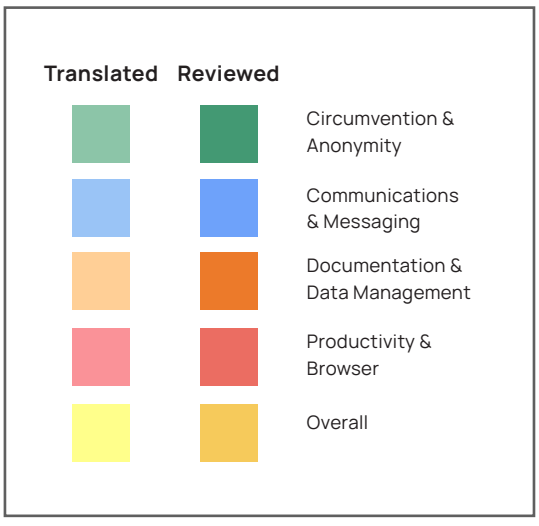
INDONESIAN
(BAHASA INDONESIA)



KHMER
(ភាសាខ្មែរ)



THAI
(ไทย)



Average rates of translation and review by language and category from 6 January until 20 February 2022. The full table is publicly accessible here: http://airtable.com/shrOqDL9SsRssPtsN.

Overall, the localization of digital security tools into Indonesian has the highest rate of translation for all but one category: *Circumvention and Anonymity*. This could be due to the large number of Indonesian language users who demand localized versions of these tools and a higher number of translators to support such localization. Burmese, Thai, and Khmer translation rates do not fall far behind Indonesian, reflecting the increasing need for digital security tools by users of these three languages. The rate of translation for Filipino is significantly lower compared to the other target languages, most likely due to the lack of demand among users of this language, who typically have competency in English.

The tools in the *Productivity and Browser* category have the highest rates of translation and review on average. It is only Burmese that has more *Circumvention and Anonymity* tools translated and reviewed. This trend could be due to Myanmar advocates' higher demand for localized tools like CENO, Psiphon, TunnelBear, and others.

We observe that the rate of review lags behind the rate of translation, which is consistent across all target languages and all types of tools. This is because the review process is typically more complex and usually takes more time. This translation-to-review gap is more or less consistent across all four types of digital security tools but varies considerably among the five target languages. This may be due to several factors:

- the more urgent need for localized digital security resources in countries like Myanmar, Thailand, and Cambodia that have seen a clampdown on democratic rights in recent years;
- the low demand for localized digital security resources among Filipino speakers who are also proficient in English; and
- the more established Indonesian localization community, who supports initiatives to localize digital security tools and guides from English.

The digital security tools surveyed are as follows:

Circumvention and Anonymity

1. **Bitmask** (Android, Desktop) is an open-source virtual private network (VPN).

2. **CENO** – Censorship.no! – is a mobile web browser for Android OS that creates peer-to-peer networks for storing and sharing web content so that users can bypass internet surveillance and censorship without needing proxies, VPN servers, or relays.

3. **Onion Browser** is a web browser that reroutes all traffic through the Tor network to protect privacy, circumvent surveillance, and evade censorship on the internet.

4. **Orbot** is a proxy app for Android devices that reroutes internet traffic through the Tor network to protect the user's privacy and identity online.

5. **Psiphon** (Android, iOS, Windows, Mac) is an open-source internet censorship circumvention tool that uses a combination of secure communication and obfuscation technologies to allow users to access blocked or censored content.

6. **Tails** is an open-source portable computer operating system that protects users from surveillance and helps them circumvent censorship.

7. **Tor Browser** is an open-source private internet browser that protects users from tracking, surveillance, and censorship.

8. **Tunnelbear** is a secure VPN service.

Communications and Messaging

9. **Briar** (Android, Desktop) is an open-source secure message app for Android OS. With Briar, users can send and receive messages through encrypted Bluetooth, WiFi, or Tor connections to avoid surveillance and censorship.

10. Jitsi is an open-source private video conferencing software that limits the user's digital footprint when meeting virtually.

11. Mailvelope is an open-source extension for Chromium-based and Firefox-based web browsers that provides an interface for Pretty Good Protection (PGP) email encryption on popular web-based email services.

12. ProtonMail (Web, Android, iOS) is an open-source email service that uses end-to-end encryption and zero-access encryption to protect the user's data and privacy.

13. Signal (Desktop, Android, iOS) is an open-source secure messaging and calling app that uses end-to-end encryption to protect the user's privacy.

14. Thunderbird is an open-source desktop email client that has built-in security and safety features including remote image linking protection, phishing protection, PGP encryption, and more.

15. Wire is a private communication suite that offers secure messaging, video conferencing, and file sharing.

Documentation and Data Management

16. GlobaLeaks is a free and open-source secure reporting and documentation system that protects the whistleblower's identity.

17. KeePassDX is an open-source secure password manager for Android mobile devices.

18. KeePassXC is an open-source secure password manager for Linux, MacOS, and Windows.

19. OnionShare is an open-source secure file sharing tool that uses the Tor network to protect the users' data and privacy.

20. **Save** is an open-source secure documentation app for Android that helps users preserve, protect, authenticate, and amplify their work.

21. **SecureDrop** is an open-source whistleblowing system designed for media practitioners to receive information from sources securely and anonymously on the web.

22. **Tella** is an open-source secure reporting and documentation Android app that encrypts and hides saved data on the device.

23. **VeraCrypt** is an open-source disk encryption tool for Windows, Mac, and Linux.

Productivity and Browser

24. **Brave** is a privacy-focused internet browser built off the open-source Chromium codebase. The Brave browser blocks invasive ads and cross-site trackers by default. Users also benefit from built-in functionalities for added security with automatic secure HTTP connections and Tor-based anonymous network routing. Brave is available in desktop, Android, and iOS versions.

25. **Firefox** is an open-source web browser that protects the user's privacy on the internet.

26. **LibreOffice** is a free and open-source office productivity suite that contains a word processor, a spreadsheet program, a presentation application, and more.

27. **OpenOffice** is a free and open-source office productivity suite.

28. **PhishDetect** is an extension for Chromium-based and Firefox-based web browsers that protects the user from phishing attacks.

IV. DIGITAL SECURITY GUIDES

Digital Security Guides

The guides selected for the survey cover a range of digital safety and security topics and are written for a range of users with varying technical literacy and threat models. The 13 selected digital security guides represent resources that are most commonly used by civil society practitioners in Southeast Asia today. Most are web- and text-based guides; however, some are interactive, multimedia resources (Totem, Consumer Reports Security Planner) or are in the form of mobile applications (Umbrella).

1. **Consumer Reports Security Planner** - *Consumer Reports*
   Guide that walks users through a series of questions about their digital habits to provide customised digital security recommendations.

2. **Data Detox X Youth** - *Tactical Technology Collective*
   Toolkit that helps young people reflect on their digital lives and manage their digital hygiene.

3. **Digital First Aid Kit** - *RaReNet (Rapid Response Network), CiviCERT*
   Resource for rapid responders, digital security trainers, and tech-savvy activists

to better protect themselves and the communities they support against the most common types of digital emergencies.

4. **Digital Hygiene 101** - *EngageMedia*

   Digital hygiene and security guide providing best practices for working and collaborating safely in an online environment.

5. **Digital Safety Trainer's Assistant** - *Natasha Msonza*

   Guide for digital security trainers that provides step-by-step approaches for teaching digital security concepts and practices.

6. **The Holistic Security Manual** - *Tactical Technology Collective*

   Holistic security manual that integrates digital security, psycho-social well-being, and organisational security processes to improve the security strategies of individuals and organisations.

7. **Holistic Security Protocol for Human Rights Defenders** - *Open Briefing*

   Guide to holistic security (physical safety, digital security, well-being, and resilience) for individuals and organisations, with a focus on safe practices rather than technical solutions.

8. **Safe Sisters Guide** - *Internews*, *Defend Defenders*, *Digital Society*

   Beginner's guide for women and nonbinary people seeking to improve basic digital hygiene and security online.

9. **Security-in-a-Box** - *Frontline Defenders*

   Series of digital security tools and strategy guides for high-risk human rights workers.

10. **Surveillance Self-Defense** - *Electronic Frontier Foundation*

    Series of digital security how-to and strategy guides for beginner to advanced users.

11. **Totem** - *Free Press Unlimited, Greenhost*

    Web-based digital security courses covering a range of topics for human rights activists, journalists, and general users.

12. **Umbrella** - *Security First*

    Mobile application with digital security tool guides and practical digital security and physical safety steps for beginner to advanced users, particularly for non-governmental organisation (NGO) workers, journalists, and activists.

13. **Safe + Secure** - *Doc Society*

    Handbook containing information and resources about digital security, journalistic accountability, legal security, and more for documentary filmmakers.

Across the board, the localization of the selected guides into the five Southeast Asian languages was minimal, with just over half of the guides localized into at least one of the target languages. The survey additionally found that of those localized guides, half of the localized versions were either out-of-date with the updated English guide, or were only partial localizations of the full resource.

It is important to note that the majority of the digital safety and security guides included in this survey were developed by non-governmental and digital rights organisations based in the Global North. While most were developed with a global audience in mind, frames of reference and recommendations may be less relevant for users in the Global South, specifically Southeast Asia. Some resources like Totem, however, embrace an approach of full localization or 'contextualisation' by first editing the original guide to include references, resources, and recommendations customised for specific regions prior to translation.

Recognising that there are digital safety and security guides in local languages that the survey team may not be aware of, the 13 guides in this review were selected based on the following criteria:

- Ease of localization into multiple languages from an English original text;
- Active maintenance of the resource – while many of the existing localizations of

the guides were either partially complete or out-of-date, the English originals have been recently developed or updated;

- Familiarity with the publisher – the developers of the guides are known and trusted organisations; and
- Focus on free and open-source resources – the tool recommendations in the selected guides mostly, but not exclusively, cover open-source, publicly audited tools that are free of cost.

V.
MOVING FORWARD

While localization in Southeast Asia has generally improved in recent years, the challenges that inhibit the localization of digital security resources, in particular, are still substantial. Quality localization requires a high technical literacy and a deeper understanding of complex technical concepts and terms. Technologies are also constantly changing and evolving, and this comes with an ever-expanding list of newly coined terms or 'neologisms'. New term creation presents a challenge when there is a lack of popularly accepted linguistic institutions focused on language development and term creation, or there is disagreement over approaches to creating new terms. Additionally, across many languages, the creation of new technical terms lags drastically behind their inception. The lack of accessible linguistic resources to support localization (such as technical glossaries and style guides) present an additional hurdle across many languages. These hindrances significantly inhibit localization and have no doubt affected localization efforts across the five target languages of this survey.

Localization of non-commercial projects faces additional challenges due to the reliance on volunteer contributions and using a crowdsourcing model. The crowdsourcing contribution model allows end-users and enthusiasts to shape the language in the tools that they themselves use, but it is also dependent on volunteers having the technical and linguistic skills to provide quality translations, as well as the time to localize resources and keep them up to date. Without quality controls put in place by the project – like clear translation

guidelines, contributor vetting, or a review process – the quality of volunteer localization can suffer. Without large, active language teams, project localization can stagnate, if it even begins. This survey found that the number of contributors to digital security projects who are competent in Burmese, Filipino, Indonesian, Khmer, or Thai is limited. The absence of regional groups and organisations focused on digital security localization indicates a clear need for more outreach and community building across Southeast Asia.