A COMMUNICATION GUIDE

FOR AFGHAN CIVIL SOCIETY

2024

RIGHT TO CONNECT
RTC

A COMMUNICATION GUIDE

For:

AFGHAN CIVIL SOCIETY

To develop this guide, RTC conducted interviews with various Afghan CSO representatives, both in Afghanistan and in exile. Additionally, RTC consulted with numerous HRDs and journalists inside Afghanistan and in neighboring countries. This guide was developed in response to the numerous challenges faced by Afghan CSOs, HRDs, and journalists in their professional environments and while in exile.

A Communication Guide for Afghan Civil Society

Disclaimer:

The opinions expressed herein are those of the author(s) and do not necessarily reflect the views of our donors and RTC. While RTC retains the intellectual property rights of these guidelines, individuals and organizations are authorized to use, reproduce, and distribute any part of this material solely for non-commercial, educational, or scholarly purposes, provided that the use is accompanied by an acknowledgment of the copyright holder's name and a citation of the original source.

A Communication Guide for Afghan Civil Society

Table of Contents

Acronyms

2FA	*Two-Factor Authentication*
AI	*Artificial Intelligence*
CSO	*Civil Society Organization*
DVD	*digital versatile disc*
GDPR	*General Data Protection Regulation*
HRD	*Human Rights Defender*
ID	*Identity*
IDP	*Internal Displaced Person*
ITA	*Interim Taliban Authorities*
NGO	*Non-Governmental Organization*
PIN	*Personal Identification Number.*
QR Code	*Quick Response Code*
SEO	*Search Engine Optimization*
SMT	*Senior Management Team*
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
TOR	*The Onion Router*
UN	*United Nations*
USB	*Universal Serial Bus*
VPN	*Virtual Private Network*

Section one: NGOs' communication

What is an NGO's communication?

NGO communication refers to the strategies and methods NGOs use to share information, engage with various stakeholders, advocate for their causes, and promote their activities and achievements. Effective communication is crucial for NGOs to gain support, mobilize resources, influence policy, and achieve their mission. The scope of NGOs' communication encompasses both internal and external dimensions. Effective NGOs' communication is dynamic and evolves with the changing background of media, technology, authorities, donors, and audience behaviors. It requires consistency, clarity, authenticity, and a deep understanding of the authorities, donors, and audience's values and concerns. By mastering these aspects, NGOs can strengthen their relationships with stakeholders, enhance their safety, visibility, and impact, and better achieve their missions.

What are the components of NGOs' communication?

Here are a few specific components of NGOs' communication, but they are not the only ones:

1. Internal communication:

NGOs ensure their members, staff, and volunteers are safe, informed, motivated, accountable, and aligned with their goals and missions. NGOs use different tools internally, including email, intranets, newsletters, meetings, and team collaboration platforms like Jitsi, Slack, or Microsoft Teams. The NGOs' internal communication component includes internal accountability, daily updates, training and educational programs, policy changes and reforms, and facilitating feedback and daily discussions among members, staff, and volunteers.

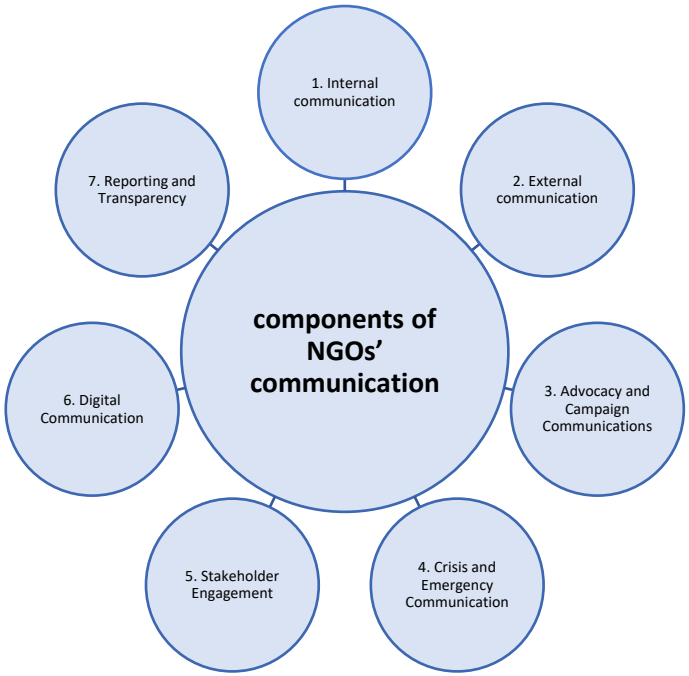


Figure 1: Components of NGOs' Communication

2. External communication:

NGOs ensure any possible and agreed-upon communication with donors, partners, government regulators, beneficiaries, the media, and the public. NGOs use a variety of tools and platforms for external communication, including websites, social media platforms, communication tools, press releases and position papers, emails, blogs, and media appearances. The external communication component varies based on several factors and includes campaigns to raise awareness or funds, reports on activities and impacts, stories from beneficiaries, positioning, advocacy messages, and promotional materials.

3. Advocacy and campaign communications:

NGOs influence public opinion, policy, and legislation related to the NGO's cause and missions. They are using a variety of tools and approaches, including public rallies, lobbying, petition drives, social media campaigns, partnerships with influencers, and public service announcements. NGOs try to be strategic by developing clear, compelling messages, identifying target audiences, and choosing the right mix of channels to reach and mobilize supporters.

4. Crisis and emergency communication:

NGOs aim to manage and mitigate the negative impacts of crises on their operations. To accomplish this, they are using different approaches, including the preparation of crisis communication plans, rapid response teams, clear and transparent communication during crises, and post-crisis evaluation and reporting.

5. Stakeholder engagement:

NGOs are determined to build and maintain positive relationships with individuals and organizations that have an interest in or stake in the NGO's project or overall operations. They are using several methods, including regular updates, invitations to participate in events or projects, surveys to gather input, and acknowledgment of support.

6. Digital communication:

NGOs use digital communication because, in today’s world, digital platforms are essential for reaching a wider audience efficiently and cost-effectively. They are using several tools and strategies, including SEO (Search Engine Optimization) for better visibility online, content marketing, video storytelling, email newsletters, and analytics to measure engagement and impact.

7. Reporting and transparency:

NGOs ensure to demonstrate accountability to government regulators, donors, partners, and beneficiaries by openly sharing information about activities, financials, and outcomes. They are using different accountability mechanisms and reports, including semi-annual and annual reports, financial statements, project reports, organizational reports, financial audits, and impact assessments, often shared on the NGO's website and, in some cases, through social media.

What are the main challenges NGOs face while communicating online in Afghanistan?

NGOs' communication in Afghanistan faces distinctive challenges, and they operate within a highly restrictive and sensitive environment, impacting how these entities communicate both internally and externally. The operating environment for NGOs requires a strategic, flexible approach to communication, emphasizing security, adaptability, and sensitivity to the complex socio-political context. Remaining effective and impactful while ensuring the safety of staff and beneficiaries is a delicate balance that NGOs must navigate with great caution. Here's an overview of the major challenges affecting NGO communication:

1. Censorship and media control:

There have been strict controls imposed on free speech and the media, directly affecting how NGOs communicate with the public. There's an atmosphere of self-censorship among NGOs to avoid attracting negative attention from ITA.[1]

2. Internet and digital communication restrictions:

Internet access, digital platforms, and social media are all under surveillance and, in some cases, restricted.[2] To

Figure 2: Challenges NGOs face while communicating online.

[1] https://www.hrw.org/news/2021/10/01/afghanistan-taliban-severely-restrict-media
[2] https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf

continue their operations without endangering their staff or beneficiaries, NGOs must carefully navigate these limitations.

3. Security and confidentiality:

NGOs operational communication is under severe surveillance by ITA.[3] NGOs have to prioritize the security and confidentiality of their communications to protect the identities and safety of their employees and the communities they serve. Under these circumstances, secure communication channels and encrypted messaging services become increasingly critical.

4. Limited public engagement:

The scope for public engagement and advocacy campaigns is significantly diminished in Afghanistan. NGOs are forced to limit their public communications and often rely on low-profile activities to avoid drawing attention.[4]

5. Risk of misinterpretation:

Communications that criticize ITA or advocate for rights contrary to their interpretation of Sharia law are especially risky. NGOs must carefully word their communications to ensure they do not inadvertently endanger their staff or operations.

6. Stakeholder engagement:

Engaging with international donors, partners, and the global community becomes more complex.[5] NGOs have to find ways to convey the realities on the ground, advocate for support, and demonstrate their impact without the usual avenues of open communication.

How to respond to communication challenges in Afghanistan?

1. How to address the challenges of (1) censorship and media control (2) internet and digital communication restrictions and (3) security and confidentiality:

[3] https://www.csis.org/analysis/talibans-increasing-restrictions-civil-society-and-aid-organizations
[4] https://press.un.org/en/2023/sc15222.doc.htm
[5] https://www.rferl.org/a/afghanistan-taliban-ban-swedish-ngo-humanitarian-crisis/32504979.html

Approach one - Use of Virtual Private Networks (VPNs):

Use of Virtual Private Networks (VPNs) to safely access the internet and bypass restrictions and censorship. This helps mask internet traffic and protect identities online. Keep in mind not to trust all VPN service providers. Some governments also employ VPN companies to access the data they require. Here are a few popular VPN service providers you may use:

Name	Service provider	Pros	Cons	Country located
ProtonVPN	Proton Technologies AG	Strong commitment to privacy and security, based in Switzerland with favorable privacy laws, no-logs policy, Secure Core feature for added security.	May have slower speeds due to heavy encryption.	Switzerland
	Website	https://protonvpn.com/		
Mullvad	Amagicom AB	Highly privacy-focused, no-logs policy, supports anonymous payments, WireGuard protocol support, bridge mode for bypassing censorship.	Interface may be less user-friendly for some users.	Sweden
	Website	https://mullvad.net/en		
ExpressVPN	Express VPN International Ltd	User-friendly interface, reliable speeds, strong encryption, TrustedServer technology for improved security.	Higher cost, based in a Five Eyes jurisdiction.	British Virgin Islands
	Website	https://www.expressvpn.com/		
NordVPN	Tefincom & Co., S.A	Extensive server network, strong encryption, specialty servers for added security and obfuscation, Double VPN for extra protection.	Had a security incident in 2018, based in a Fourteen Eyes country.	Panama
	Website	https://nordvpn.com/		
CyberGhost	Kape Technologies	User-friendly apps, strong encryption, supports multiple devices, dedicated servers for streaming and torrenting.	Privacy policy not as robust as some other providers, variable speeds on different servers.	Isle of Man
	Website	https://www.cyberghostvpn.com/		

Figure 3: popular VPN service providers.

Approach two – use encrypted communication apps and secure email services:

Leverage secure and encrypted communication apps and secure email services for internal and external communications. There are several secure and encrypted communication apps and secure email services (check figures 8 and 9).

Approach three – adopt low-profile:

Adopt a low-profile approach if you work in Afghanistan. Focus on maintaining a low profile in public communications and activities. Avoid appearing in social media and TV interviews. This could involve reducing the exposure of operations that the ITA might consider sensitive or controversial.

Approach four – avoid cultural sensitivity:

Ensure all communications and programs are not culturally sensitive by engaging Afghan experts in their design. This reduces the risk of negative attention.

Approach five – ensure regular training to staff on cyber security:

Offer regular training to staff on digital security, secure communication practices, and how to navigate restrictive environments safely. *If your organization is not capable of providing such training,* partner with organizations and individuals who specialize in digital security and counter-surveillance measures. They can provide up-to-date advice, technological solutions, and support to navigate digital challenges. There are so many organizations that can help you, including RTC. Check our website for the latest update at https://righttoconnect.org/online-resources/.

Approach six – check for digital security practices update:

Regularly update digital security practices. Digital surveillance technologies are constantly evolving. Consequently, regularly review and update digital security measures to counter new threats and take advantage of emerging secure communication technologies.

Approach seven – develop a contingency plan:

Develop and maintain a clear contingency plan for what to do in case of internet shutdowns, digital surveillance encounters, or the compromise of digital tools. Having such protocols in place ensures that staff know how to react swiftly and safely to protect information and the people involved.

Approach eight – ensure to store sensitive data in encrypted format:

Store sensitive data in encrypted formats, employing services that offer strong security measures. To ensure data integrity and protection against unauthorized access or loss, use access controls and secure backup solutions.

Approach nine – secure physical documents and communications:

Secure physical documents and communications. In addition to digital security, ensure that physical documents containing sensitive information are kept secure. Implement strict policies for accessing, handling, and disposing of sensitive physical materials.

Approach ten – require a policy for strong passwords and codes:

Implement policies requiring the use of strong, unique passwords for all accounts and services. While choosing a password:

- Write down a new, strong password rather than using a short, obvious one.
- Use symbols, capital letters, small letters, signs, and numbers in your password.
- Don't rely on Windows passwords. They are swiftly obliterated.
- Use passwords with a minimum of eight characters.
- Always use a new password if you change it.
- Use secure passwords that have nothing to do with your hobbies or personal life.
- Every month and every other month, modify passwords.
- Encourage employees to use password managers to help secure their passwords.

Here are some of the safest password managers for NGOs:

Name	Name of service provider	Suitability	Country located
Bitwarden:	8bit Solutions	Ideal for transparency and security-conscious users. It offers open-source, end-to-end encryption, and affordability.	United States
	Website	https://bitwarden.com/	
LastPass	LogMeIn, Inc	User-friendly with multi-factor authentication and secure sharing features. Suitable for those valuing convenience and collaboration.	United States

	Website	https://www.lastpass.com/	
1Password	AgileBits Inc	Strong security features, Travel Mode for added protection, and Watchtower for breach monitoring make it ideal for those seeking comprehensive security.	Canada
	Website	https://1password.com/	
Dashlane	Dashlane Inc	Offers dark web monitoring, VPN, and password changer. Beneficial for users looking for additional security beyond basic password management.	United States
	Website	https://www.dashlane.com/	
KeePassXC	KeePassXC Development Team	Best for users who prioritize control and privacy, providing free and open-source local password management.	Germany
	Website	https://keepassxc.org/	

Figure 4: best password managers for NGOs.

Approach eleven – utilize 2FA:

Implement Two-Factor Authentication (2FA) approach. Wherever possible, enable two-factor authentication for an added layer of security on accounts, especially for services critical to the organization's operations.

Approach twelve – Develop an incident response plan:

Develop a clear and actionable incident response plan to address potential security breaches or data leaks. The plan should include steps for containment, assessment, notification, and recovery. Be ready if your website is hacked or if your accounts' passwords are compromised. You should be ready for all these scenarios.

Approach thirteen – utilize TOR:

For situations requiring anonymity, consider using tools designed for anonymous communication, such as TOR (The Onion Router), for accessing the internet or transmitting sensitive information. Here are some of the of the most suitable TORs:

Name	Name of service provider	Suitability	Country located

Tor Browser	The Tor Project	The most well-known and widely used tool for accessing the TOR network. It's ideal for users who require strong anonymity and privacy protections while browsing the web.	Global (Headquartered in the United States)
	Website	https://support.torproject.org/tbb/	
Brave Browser with TOR	Brave Software	Combined with TOR, provides enhanced privacy features and built-in ad-blocking capabilities. It is suitable for users who want an alternative browser with Tor integration.	United States
	Website	https://community.brave.com/	
Whonix	Whonix Project	Whonix is a privacy-focused operating system that runs inside a virtual machine and directs all internet traffic through the TOR network. It's suitable for those seeking a more comprehensive privacy solution beyond just browser anonymity.	Global
	Website	https://www.whonix.org/	
Tails (The Amnesic Incognito Live System)	Tails Project	Tails is a live operating system designed to be booted from a USB stick or DVD and routes all internet traffic through TOR. It's suitable for users who want to maintain anonymity without leaving a trace on the host system.	Global
	Website	https://tails.net/	
Orbot/Orfox	The Guardian Project	Orbot is a proxy app that routes all your mobile device's traffic through the Tor network, while Orfox is the Tor Project's official web browser for Android. These are suitable for users who require TOR anonymity on their mobile devices.	United States
	Website	https://guardianproject.info/apps/info.guardianproject.orfox/	

Figure 5: some most suitable TORs.

2. How to respond to limited public engagement issue?

Responding to the problem of limited public engagement necessitates that NGOs adopt innovative approaches to continue their efforts discreetly and effectively. By adjusting strategies to focus on subtlety, security, and the leveraging of local networks, NGOs can continue to engage with the public and advocate for their causes. NGOs reach out to their beneficiaries and deliver their services, usually through local Shuras, Jirgas, and community leaders. There is a category of civil society organizations in Afghanistan called

Shuras and Jergas. They are traditional local councils that villages or tribes establish themselves, usually to represent a community's interests to other parts of society. Shuras and Jergas are local decision-making bodies that are arguably the most traditional building blocks of civil society in Afghanistan. They are generally composed of village elders and operate on an informal basis (i.e., as unregistered groups).

NGOs reach out to their beneficiaries directly, as well as through Shuras, Jergas, and community leaders. The beneficiaries of NGOs are various segments of society, including:

Women and girls	NGOs often focus on women's rights, empowerment, education, healthcare, and protection from violence and discrimination.
Children	NGOs work to improve access to education, healthcare, nutrition, and protection for children.
Internally displaced persons (IDPs)	NGOs provide assistance, shelter, healthcare, and livelihood support to individuals and families internally displaced due to conflict and natural disasters.
Refugees	NGOs offer services and support to refugees and returnees in Afghanistan, including assistance with resettlement, education, healthcare, and livelihood opportunities.
Marginalized communities	NGOs target marginalized groups, such as ethnic minorities, people with disabilities, and those living in remote or conflict-affected areas, with various programs and services.
Victims of natural disasters	NGOs provide relief and support to communities affected by natural disasters like floods, droughts, earthquakes, and avalanches.
Healthcare recipients	NGOs support healthcare systems, provide medical services, build infrastructure, and promote health education and awareness campaigns.

Figure 6: common beneficiaries of NGOs in Afghanistan.

To reach out to these beneficiaries, NGOs need to communicate with local Shuras and Jergas, as well as religious, community and neighborhood leaders. These categories of CSOs and individuals can play a significant role in disseminating information and advocating for change in a way that is culturally sensitive and less likely to attract unwanted attention.

Religious Leaders (Mulla Imams):	This group includes individuals who hold positions as mosque prayer leaders, religious instructors in schools, and experts in Shari'a law. The Mulla Imams are resourceful individuals in the whole community.

	They know the whole community, depending on the years of their service within the community mosque. If NGOs want to reach out to the right beneficiaries, they have to build a working relationship with these religious leaders.
Community leaders (Malik, Arbab):	In suburban and rural areas, maliks, or arbabs, serve as local village representatives, representing the village's interests both within the community and externally. These individuals are well-connected and resourceful for all residents in their village. NGOs seeking to deliver services to specific parts of the village will find that maliks and arbabs can be instrumental in facilitating connections and communications.
Neighborhood leader (Wakil Guzar):	Wakil guzar is a neighborhood leader elected for a specific term by each neighborhood within a municipality. These resourceful individuals play a key role in assisting NGOs by connecting them with the appropriate beneficiaries.

Figure 7: Key individuals to reach out the right beneficiaries in Afghanistan.

Note: Keep in mind that their helpfulness may vary based on their individual attitudes.

Meanwhile NGOs should:

- utilize small-scale, community-based interventions. Instead of large public campaigns, focus on smaller, community-based interventions that can fly under the radar. Workshops, discussion groups, and training sessions held in private settings can foster engagement and awareness without drawing attention.
- adopt indirect communication and advocacy tactics. Use storytelling, art, and cultural events as indirect ways to communicate messages and foster discussions around critical issues. These methods can be less confrontational and more acceptable to restrictive authorities.
- enhance private communication channels with beneficiaries and, for direct engagement with beneficiaries, maintain strong, secure lines of communication. Encrypted messaging apps and hotlines can facilitate private interactions, offering support, information, and resources without public exposure.

3. How to deal with the risk of misinterpretation?

Dealing with the risk of misinterpretation in Afghanistan, especially concerning communications potentially seen as critical of the ITA or advocating for rights contrary to their interpretation of Shari'a law, requires a strategic and cautious approach. NGOs must navigate this sensitive situation to continue their work without compromising their safety or operations. By employing these strategic

approaches, NGOs can navigate the complex and risky environment of operating in Afghanistan, minimizing the risk of misinterpretation and potential repercussions while still striving to achieve their mission and support the communities they serve.

Approach one – contextual knowledge and sensitivity awareness:

Contextual knowledge and sensitivity awareness are key steps in developing a deep understanding of the cultural and political context. This knowledge and awareness can guide the framing of messages in a way that resonates positively with the local community while still promoting the NGO's objectives. Review all decrees, directives, orders, and decisions issued by ITA after August 2021 that are relevant to your work to stay informed about the latest context and sensitivities in Afghanistan. To find out the decrees, directives, orders, and decisions relevant to your work, you need to contact the relevant ITA's ministries or directorates. ITA didn't publicize any of the decrees, directives, orders, and decisions on a website.

Approach two – careful use of language:

Careful use of language is another key factor in crafting communications with neutral, non-confrontational language that focuses on common human values and goals. In addition, NGOs operating inside Afghanistan should avoid directly challenging or criticizing any decisions and policies in public forums, social media, and mass media. Being professional is much safer than being an activist if you want to see changes in a country like Afghanistan. Criticizing any decisions and policies in public forums, social media, and mass media is considered opposing the ITA's mandate, which is interpreted as Shari'a among the ITA's authorities.

Approach three – engagement with religious leaders (mulla imams):

Engagement with religious leaders (mulla imams) is also a helpful step if they share a common vision for humanitarian issues. Their endorsement or involvement can lend credibility and culturally appropriate framing to the NGO's initiatives, reducing the risk of adverse interpretations.

Approach four – promoting universal human rights under local context:

Promoting human rights in a local context is also helpful to reduce the level of misinterpretation. NGOs should frame discussions around human rights and development goals within the context of local values and traditions. Highlight how these initiatives align with the betterment of the community, focusing on common ground rather than differences.

Approach five – localized messaging:

Localized messaging is also a key factor. Tailor your messages to local narratives and perspectives. Use stories and examples that reflect local experiences and aspirations, making the message more relatable and reducing the likelihood of misinterpretation.

Approach six – distinguish between private and public communication:

Distinguish between private and public communication, which may need to be more generalized and carefully worded, and private communications, where more direct and specific discussions can take place within safe, closed groups.

Approach seven – regular monitoring:

Monitor the reception of your communications among various segments of the Afghan population regularly, and adjust your strategies based on feedback to ensure the intended interpretation of your messages.

Approach eight – social media control:

When posting anything on social media, be cautious. Consider all the dimensions of a post on social media. Never let the employees post anything without approval from the SMT. Hire a social media and communication expert if your budget allows.

Note: You possess a deeper understanding of your mandate, project, and beneficiaries than we do. As a result, you can find the best possible solution to avoid any misinterpretation in the event that these strategies are insufficient.

4. How to deal with the challenges of stakeholder engagement in Afghanistan?

Dealing with the complexities of stakeholder engagement in Afghanistan, especially under conditions that hinder open communication, requires NGOs to adopt innovative and strategic approaches. These strategic approaches must effectively communicate the ground realities, mobilize support, and demonstrate the impact of their work to international donors, partners, and the global community.

Approach one - Leverage technology for secure and safe communication:

Utilize secure and encrypted communication tools to share updates and reports with international stakeholders. Tools like Signal or secure email services can facilitate confidential correspondence and ensure sensitive information is not compromised. (Please refer to figures 8 and 9 for more information about the safest communication tools and email services.)

Approach two – use multimedia wisely:

Use multimedia to document activities, but do not publish them in your account. Compelling visuals and stories can bridge communication gaps. But be careful; creating impactful videos, photo essays, and infographics that highlight the ground realities, the NGO's efforts, and the communities' narratives can expose all beneficiaries to a major risk. Even if they are shared through the safest communication tools directly with stakeholders who may use them to create a global advocacy tool.

Approach three – virtual engagement:

While it is not probable to meet in person, engage through virtual platforms, but use the safest ones. Organize virtual meetings, webinars, and conferences to connect with international donors and partners. These platforms can also be used to host panels with on-the-ground activists, beneficiaries, and staff, providing firsthand insights into the situation in Afghanistan. (Please refer to figures 8 and 10 for more information about the safest platform.)

Approach four - international networks and partnerships:

Utilize international networks and partnerships, but do not expose them. Any exposure can pose a major risk to your staff, beneficiaries, and the communities you serve. Leverage partnerships with international NGOs, advocacy groups, and UN agencies to amplify the NGO's voice. Collaboration can result in joint advocacy efforts, shared platforms, and increased visibility among a broader audience of potential supporters.

Approach five – employ intermediaries outside Afghanistan:

Employ trusted intermediaries outside Afghanistan. There are thousands of Afghan civil society activists and HRDs in exile who can help you. Utilize intermediaries and liaisons who can travel or communicate more freely between Afghanistan's local NGOs and the international community and organizations. These individuals can serve as messengers and advocates, providing updates and facilitating dialogues on behalf of the NGO.

What are the safest communication tools for NGOs?

Apart from a few, none of these communication tools are completely secure. Select them based on your communication sensitivity.

Tools	Encryption	Data Privacy	Security Features
Signal	Uses end-to-end encryption by default for all messages, calls, and media shared, utilizing its own open-source Signal Protocol.	Collects minimal user data, with a focus on maintaining user privacy. It doesn't store messages on its servers once they've been delivered.	Offers self-destructing messages, screen security (prevents screenshotting), and registration lock (PIN to protect account).
Wire	Utilizes end-to-end encryption for text, voice, video, and files using the Proteus protocol, built on the Signal Protocol.	Collects some user information, including user ID, phone number (if provided), and email address (if provided), for account management purposes.	Supports features like timed messages, which automatically delete after a set period, enhancing privacy. Additionally, it offers user verification to prevent man-in-the-middle attacks.
Threema	Provides end-to-end encryptions for all communications, including messages, calls, and files. It uses the NaCl cryptography library, ensuring that only the communicating users can read the messages.	Designed for maximum data economy, not requiring an email or phone number to sign up. It generates a random Threema ID for each user, enhancing anonymity. Contact lists and group information are stored only on user devices, not on servers.	Includes a unique feature allowing users to verify contacts with QR codes, adding an extra layer of security against potential impersonation or man-in-the-middle attacks. It also offers encrypted backups and a poll feature within chats, maintaining encryption.
Session	Employs end-to-end encryption based on the Signal Protocol for messages. What sets Session apart is its onion routing protocol, which obscures metadata, making it difficult to determine who is communicating with whom.	Does not collect any personally identifiable information (PII) upon registration, using only session IDs for user identification. This approach maximizes privacy by not associating accounts with phone numbers or email addresses. It’s designed to leave minimal digital footprints, significantly enhancing user anonymity.	The decentralized architecture and onion routing not only provide strong data privacy but also resilience against network surveillance and censorship. Session's lack of central servers means there are no central points where user data could be requested or hacked.

Viber	Provides end-to-end encryption by default for messages and calls.	Collects limited data compared to others, like WhatsApp or Messenger, and focuses on user privacy, requires a phone number.	Offers self-destructing messages and requires a PIN for accessing the app on a new device.
WhatsApp	Implements end-to-end encryption by default for messages and calls, using the Signal Protocol.	Leading to concerns about data sharing between WhatsApp and other Meta-owned platforms, despite encryption. A phone number required.	Offers two-step verification but has faced scrutiny over Meta's data handling practices.
Telegram	Provides end-to-end encryption in "Secret Chats" only, not in regular messages. Regular messages use client-server/server-client encryption.	Stores data on its servers to allow for syncing across devices. Has access to metadata. Phone number required.	Offers self-destructing messages in Secret Chats and has an open API for third-party apps, which might pose additional security considerations.
IMO	Offers encryption for voice and video calls but lacks transparency about the type of encryption for messages.	Data collection practices are not as clear-cut, raising some concerns about user privacy. Phone number required.	Provides fewer privacy controls compared to its competitors.
Messenger (Facebook Messenger)	Offers end-to-end encryption in "Secret Conversations" only. Regular messages and calls use encryption in transit but can be accessed by Facebook.	Part of the Facebook ecosystem, sharing data across platforms for targeted advertising and other purposes.	Offers optional Secret Conversations, but by default, conversations are not end-to-end encrypted.
Delta Chat	Uses Autocrypt to automatically encrypt emails when communicating with other Autocrypt-enabled users.	Relies on email protocols, providing a decentralized system. Messages are stored on email servers but are encrypted.	No central servers, decentralized design, predominantly focuses on email communication security.
Element (formerly Riot)	Utilizes end-to-end encryption for chats and calls through the Matrix protocol.	Participants can self-host servers, increasing privacy control. However, this depends on server settings.	Supports encrypted group messaging, a variety of integrations, and customization options.

Figure 8: the safest communication tools for NGOs.

What are the safest email service providers for NGOs?

Apart from a few, none of these emails are completely secure. Select them based on your communication sensitivity.

Tools	Encryption	Data Privacy	Security Features
Riseup	Riseup focuses on providing secure communication tools for activists and movements, with a commitment to user anonymity.	Committed to protecting user anonymity and privacy, Riseup does not log any personal information that can be tied to their users and removes logs regularly. They are known for their strong stance on not sharing data with third parties unless legally compelled.	Includes VPN services to further protect the privacy of its users online. Riseup also provides 2FA for its services, adding an extra layer of security for account access.
	Website	https://riseup.net/en/email	
Autistici/Inventati (A/I)	Recommends the use of PGP for end-to-end encrypted email communication. Their services, inclusive of email and web hosting, support SSL/TLS encryption for data in transit.	Highly committed to user privacy, not tracking or profiling its users. They offer services with the intention of minimal data retention and ensuring user anonymity, aligning with their activism and community support principles.	Services are tailored for activists and those concerned about privacy, providing anonymous browsing services through VPN and TOR integration.
	Website	https://www.autistici.org	
ProtonMail	Offers end-to-end encryption for emails, ensuring that only the sender and recipient can read the content.	Utilizes zero-access encryption, meaning even ProtonMail cannot access the contents of your emails.	Operating under Swiss privacy laws, ProtonMail's servers are located in Switzerland, known for its strong privacy protections.
	Website	https://proton.me/mail	

Tutanota	Automatically encrypts emails and attachments end-to-end, securing communication.	Collects minimal personal information and offers anonymous payment options for premium features.	Based in Germany, Tutanota is subject to strict European GDPR regulations, emphasizing user privacy.
	Website	https://tuta.com	
Disroot	A privacy-focused platform providing email, cloud storage, and other services for activists and non-profit organizations.	Emphasizes encryption and security practices to protect user data and communication from surveillance.	As a community-driven platform, Disroot values transparency, privacy, and freedom of speech, catering to activist needs.
	Website	https://disroot.org/en	

Figure 9: the safest email service providers for NGOs.

What are the safest video conferencing tools for NGOs?

Apart from a few, none of these video conferencing tools are completely secure. Select them based on your communication sensitivity.

Tools	Encryption	Data Privacy	Security Features
Jitsi Meet	Provides end-to-end encryption for video conferences and ensures secure communication channels.	Open-source platform with no cost, and users can self-host servers for added privacy.	Password-protected rooms, same-room participants visibility control, and user password authentication.
	Website	https://meet.jit.si	
BigBlueButton	Supports encrypted web traffic and includes security features for maintaining confidentiality.	Designed for educational contexts, it provides controlled access to recordings and features.	Selective access permissions, moderation controls, and virtual whiteboard collaboration tools.
	Website	https://demo.bigbluebutton.org	
Whereby	Offers end-to-end encryption for calls and meetings conducted on the platform.	Provides the ability to set passwords for meetings and control access to them.	Secure, password-protected virtual meeting rooms and waiting room features.

	Website	https://whereby.com	
Blue Jeans	Provides encryption at rest and in transit to secure user data during calls and conferences.	Offers privacy features like data masking and controlled participant permissions.	Secure join features, privacy controls, and moderator controls for meeting security.
	Website	https://www.bluejeans.com	
GoToMeeting	Uses strong encryption protocols to secure data during calls and conferencing.	Compliance with data protection regulations, but user data may be collected for service improvement.	Meeting lock feature, screen sharing restrictions, and attendee access permissions.
	Website	https://www.goto.com/meeting	
Facetime/iMessage (Apple)	End-to-end encryption for texts, calls, and video chats within the Apple ecosystem.	Strong privacy protections due to Apple's encryption standards and commitment to user privacy.	Blocked contacts, Face ID/Touch ID authentication for apps, and automatically expiring iMessages.
	Website	https://support.apple.com/en-ca/guide/deployment/dep154cd083a/web	
Google Meet	Provides secure video conferencing with end-to-end encryption in transit and at rest for all G Suite users.	Google's security standards ensure data protection, but user privacy might be impacted by data collection for personalized ads.	Meeting lock, privacy controls, and measures to prevent unauthorized access.
	Website	https://meet.google.com	
Duo (Google)	Uses end-to-end encryption for calls and video chats, securing communication from third-party access.	User data collection for service improvement might impact privacy, alongside meeting Google's security standards.	Encrypted video calls that prevent the interception of communication, Face Match for authentication.
	Website	https://meet.google.com/calling/	
Microsoft Teams	Secure transmission and storage of data with comprehensive encryption protocols.	Complies with strict data privacy regulations with advanced privacy settings and controls for users.	Encrypted communications, multi-factor authentication, secure channels, and compliance standards.
	Website	https://www.microsoft.com/en-ca/microsoft-teams/log-in	
Xspace	Xspace provides end-to-end encryption for video calls and ensures secure data transmission	Highlights user data protection and ensures compliance with data privacy regulations.	Implements password-protected meeting rooms, admin controls for

	during private space communication.		access permissions, and secure document sharing features.
	Website	https://twitter.com/	
Clubhouse	Clubhouse faced criticism for its lack of end-to-end encryption, leading to privacy concerns regarding the security of audio chats on the platform.	Users have raised privacy concerns due to data retention practices and previous security incidents involving uninvited listeners joining private conversations.	Limited tools for moderation and control over conversations compared to traditional conference platforms, which could impact user safety.
	Website	https://www.clubhouse.com/	
Zoom	Faced initial encryption controversies but has since upgraded its security protocols to provide end-to-end encryption for all meetings and messaging.	Improved data privacy practices and transparency following scrutiny, offering options for users to control data sharing and security settings. Offers a range of security features like password protection, waiting rooms, host controls, and end-to-end encryption to safeguard user communication.	
	Website	https://zoom.us/	

Figure 10: the safest video conferencing tools for NGOs.

What terminology should NGOs avoid while communicating?

When NGOs communicate, especially in environments where content surveillance is prevalent, avoiding certain terminology can help minimize the risk of their communications being flagged or monitored. Several countries have adopted advanced technologies to enhance their surveillance capabilities. Since 2014, the issue has expanded with the advancement of technology, allowing for more pervasive and complex surveillance methods. Notably, the use of artificial intelligence in monitoring online activities has raised new privacy concerns.

Surveillance and monitoring methods have evolved from being the purview of intelligence operatives to being embedded within both commercial and governmental hardware and software systems. Previously, surveillance was reserved for individuals perceived as national security risks. Now, due to government-implemented monitoring and filtering systems on the Internet, we are all treated as potential suspects.

The technology employed does not always differentiate among users; it scans our emails, messages, and web searches for certain keywords. Upon detecting these, it either alerts surveillance teams or cuts off our communications. Encryption stands as one of the last bastions of online privacy, enabling us to secure our communications so that only the intended recipients can decipher them. Even the Internet's structure incorporates encryption, such as the Secure Sockets Layer (SSL), to facilitate secure financial dealings.

NGOs around the world face significant risks in their home countries, including surveillance and various restrictions that limit their communication and often result in harsh consequences for continuing their advocacy. Additionally, the security of their digital tools is increasingly compromised; emails go undelivered; social media accounts are compromised; internet connections are unreliable; communications are closely monitored; devices are confiscated; and malware destroys important work.

These challenges, including the authorities' intensified scrutiny of online content and swift retaliation against "undesirable" communication by NGOs, are well-documented issues. NGOs are constantly monitored across digital platforms such as news sites, social media, and blogs. They confront numerous hurdles, like the digital divide, repression enabled by digital tools, rights violations under the guise of security, widespread cyber vulnerabilities, and general digital insecurity. By gaining proficiency in using computers, smartphones, and understanding the internet, activists and human rights defenders can better safeguard their initiatives, effectively defending their rights and those of the people they aim to support.

China's "Golden Shield" serves as an advanced technology, operating on a national internet infrastructure separate from the global web to enhance national security through centralized user databases and comprehensive surveillance. Integrating surveillance capabilities extensively into the network, the Golden Shield extends content filtration to diverse public and private information devices, utilizing intricate technology for effective surveillance control.

According to a Freedom House social media surveillance report, governments around the world, ranging from authoritarian regimes to smaller states, are increasingly investing in advanced technology for mass surveillance of citizens on social media. This practice,

which expands beyond the capabilities of traditional spyware, involves the automated collection, organization, and analysis of vast amounts of data from digital communication platforms. Given the widespread use of these platforms for personal and political expression, people view social media surveillance as particularly invasive. In countries like Iran and China, authorities have mobilized thousands to monitor online activities and report dissent. Furthermore, advancements in artificial intelligence (AI) have enhanced the ability of these surveillance systems to analyze relationships, sentiments, and even predict locations of users, revealing patterns and information beyond human detection capabilities.[6]

In Afghanistan, ITA faces obstacles in controlling external communications, a task that would be challenging without external support and the progression of time. Comparable to practices in Iran, China, and Russia, surveillance over social media has become a strategic tool for ITA in asserting control and monitoring dissenting voices. Currently, ITA is using their own strategy, employing social media surveillance to reinforce their authority and embracing tactics akin to regional norms. According to the representatives of NGOs and activists we interviewed in the field, ITA follows the same strategy as Iran and China by hiring hundreds of people to monitor and surveil Afghan social media account holders in Afghanistan and abroad. As an NGO operating in this climate, increased social media activity or vocal advocacy on civil society matters could make you a target for ITA monitoring. Speaking at public forums, defending human rights, or drawing attention to corruption raises the likelihood of scrutiny. Importantly, targeted surveillance does not necessitate criminal activity, with governments worldwide employing sophisticated cyber algorithms to surveil professionals across sectors, including activists, journalists, and NGOs. Surveillance tools have leveraged the acquired data to vilify activists, implicate them in fabricated charges, and orchestrate their arrest, highlighting the pervasive threat of unwarranted intrusion and interference in legitimate civil society initiatives. Therefore, when communicating in Afghanistan, NGOs should be mindful of using terminology that may unintentionally cause offense or misinterpretation. Remember that adopting a professional approach is safer than acting as an activist if you aim to effect positive changes in Afghanistan.

Is using social media platforms safe for NGOs?

Using social media platforms can be both beneficial and challenging for NGOs operating in Afghanistan. To mitigate risks and maximize the benefits of using social media, NGOs should develop clear social media policies, establish security protocols, train staff on digital safety, and engage with communities thoughtfully and responsibly on these platforms. Here are some pros and cons to keep in mind regarding the safety of using social media while communicating in Afghanistan.

[6] https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance

1. Pros

Pro one – reach and engagement:

Social media platforms offer NGOs an invaluable tool to expand their reach, engage directly with global communities, and elevate awareness around their causes. By leveraging the extensive reach and interactive nature of social media, NGOs can effectively communicate their missions, share impactful stories, and mobilize support across diverse audiences. This digital approach not only amplifies their message but also fosters a sense of connectedness and participation among supporters, enabling real-time interaction and feedback. Consequently, social media serves as a dynamic catalyst for NGOs looking to drive change and garner widespread attention for their initiatives.

Pro two – advocacy and networking:

Social media platforms provide NGOs with a multifaceted toolset to advocate for societal transformation, rally backing for their causes, and establish connections with like-minded organizations, funders, and stakeholders. By harnessing the communicative power of social media, NGOs can effectively raise awareness about critical issues, galvanize grassroots support for campaigns, and forge partnerships that amplify their impact. This digital landscape not only serves as a platform for broadcasting messages but also cultivates a networked community dedicated to driving positive change and advancing collective goals in the realm of social impact.

Pro three – direct communication:

Engaging directly with your audience plays a crucial role in achieving your objectives. Unlike websites that often communicate to visitors, social media facilitates a two-way interaction with supporters and donors, allowing for immediate and proactive communication rather than relying on them to reach out after visiting your website. Equipped with customized information, this direct line of communication can effectively accelerate the process from raising awareness to eliciting the intended action.

Pro four – fundraising:

Social media stands as a crucial avenue for facilitating fundraising initiatives, engaging donors, and coordinating crowdfunding campaigns to bolster NGO projects in Afghanistan. Utilizing these platforms allows NGOs to harness their expansive reach, interactive

features, and storytelling capabilities to appeal to potential supporters, cultivate donor relationships, and efficiently mobilize financial resources for their humanitarian endeavors.

Pro five – information dissemination:

Incorporating social media into their outreach strategies enables NGOs to efficiently disseminate time-sensitive updates, valuable resources, educational content, and crucial emergency notifications to the public. By harnessing the immediacy and broad reach of social platforms, NGOs can swiftly distribute vital information, engage with their audience, and respond effectively to unfolding events, ensuring that their communications are not only timely but also impactful and far-reaching.

Pros six – maximizing awareness and connection:

Social media serves as a potent means of connection, acting as an effective platform for raising awareness. It enables organizations to reach out to the millions seeking to connect with individuals, brands, and causes that match their interests. By sharing information and visuals instantly, social media offers insights into an organization's character, complementing the carefully crafted messages that exist on its website.

2. Cons

Con one – security risks:

Implementing social media strategies in conflict areas such as Afghanistan can introduce security challenges, encompassing risks to the well-being of personnel, recipients of aid, and assets belonging to organizations operating in these regions. By engaging with social platforms, NGOs must navigate concerns related to the exposure of sensitive information, potential targeting of staff or beneficiaries, and the safeguarding of vital resources in environments fraught with instability and security risks.

Con two – censorship and surveillance:

NGOs operating in Afghanistan encounter obstacles tied to internet censorship, surveillance practices, and limitations on free expression while utilizing social media channels. Negotiating these hurdles involves navigating stringent controls on online content, heightened surveillance measures that threaten privacy and security, and constraints on the freedom to communicate openly across digital platforms. These challenges underscore the complex landscape within which NGOs must operate when engaging with social media in Afghanistan, necessitating careful consideration and adaptation to ensure effective and secure communication strategies.

Con three – misinformation and disinformation:

Social media platforms serve as conduits for the dissemination of misinformation, propaganda, and false narratives, posing a risk to the credibility and standing of NGOs. The proliferation of misleading content through these channels can tarnish the reputation of NGOs, undermining public trust and distorting the accurate portrayal of their missions and activities. As a result, NGOs must remain vigilant in navigating the landscape of social media to effectively combat misinformation and safeguard their digital integrity.

Con four – privacy concerns:

NGOs must exercise prudence regarding data privacy, cyber vulnerabilities, and information security threats when disclosing sensitive data on social media platforms. The act of sharing such information opens up potential risks related to data breaches, unauthorized access, and exploitation by malicious actors, underscoring the importance of implementing robust safeguards and protocols to protect sensitive information and maintain the integrity of their operations in the digital realm.

Con five – data security risks and obligations:

When using third-party social media services, control over data management and security often shifts away from your organization. These vendors gain access to both internal organization data and information gathered from external sources, such as images shared on platforms like Facebook or sensitive personal and financial details. It's crucial for organizations to remember their obligation to adhere to global laws and regulations concerning the handling of personal data. By providing a social media site with access, organizations relinquish a degree of control, underscoring the importance of vigilance in data protection practices.

Con six – navigating security challenges in donations:

Financial transactions on social media platforms pose security challenges for organizations collecting donations. While platforms like Facebook provide donation tools, they necessitate sharing sensitive financial data, have donation thresholds for payouts, and rely on user trust in platform security. In contrast, websites with SSL certificates offer a more secure and controllable environment for donors, ensuring enhanced data protection and management of funds across desktop and mobile versions.

Con seven – fostering trust:

Social media platforms do not provide the same level of inherent trust as recognized website domain extensions do. A key benefit of having a website lies in the association with trusted domain extensions, such as .org, which is widely recognized for bringing together

organizations, companies, and individuals around common interests or causes, fostering efforts to enact positive change. This level of trust and awareness, critical to brand perception, is something social media channels simply cannot match.

How should NGOs use social media safe?

NGOs can utilize social media safely and effectively by implementing some practices to harness the power of social media while safeguarding their data, protecting their online presence, and minimizing potential risks associated with online communication and engagement.

Approach one – data protection measures:

NGOs have to prioritize the security of sensitive information they share on social media. By employing robust measures such as creating strong, unique passwords, activating two-factor authentication for added protection, and limiting access to official accounts to authorized personnel exclusively, NGOs can effectively mitigate the risk of unauthorized access, data breaches, and potential misuse of confidential data, safeguarding their digital presence and maintaining the trust of their audience.

Approach two – privacy settings:

Utilizing the privacy settings offered by social media platforms is crucial for NGOs to maintain control over their online presence. By conscientiously configuring these settings to manage the visibility of posts, messages, and profile details, NGOs can safeguard sensitive information and conversations from being publicly accessible. This proactive approach helps NGOs maintain confidentiality, protect sensitive data, and uphold the integrity of their communication channels across social media platforms.

Approach three – training and education:

Equipping staff members with comprehensive training on data security, privacy protocols, and social media guidelines is essential for NGOs to effectively mitigate risks in their online interactions and communications. By educating employees on recognizing and responding to potential threats, NGOs bolster their defenses against cybersecurity breaches, privacy infringements, and misinformation dissemination. This proactive measure ensures that staff are well-prepared to navigate digital platforms securely, safeguard sensitive data, and uphold the organization's reputation in the online sphere.

Approach four – monitoring and response plan:

Establishing vigilant monitoring protocols for social media accounts is vital for non-NGOs to promptly detect unauthorized access, identify suspicious activities, and address inappropriate content. By conducting regular assessments and swiftly responding to security incidents or breaches, NGOs can effectively safeguard their online presence, maintain the integrity of their communication channels, and uphold trust with their audience. Having a well-defined response plan ensures that NGOs can mitigate risks, limit potential damages, and uphold a secure and reputable digital environment for their stakeholders.

Approach five – Regular updates and patches:

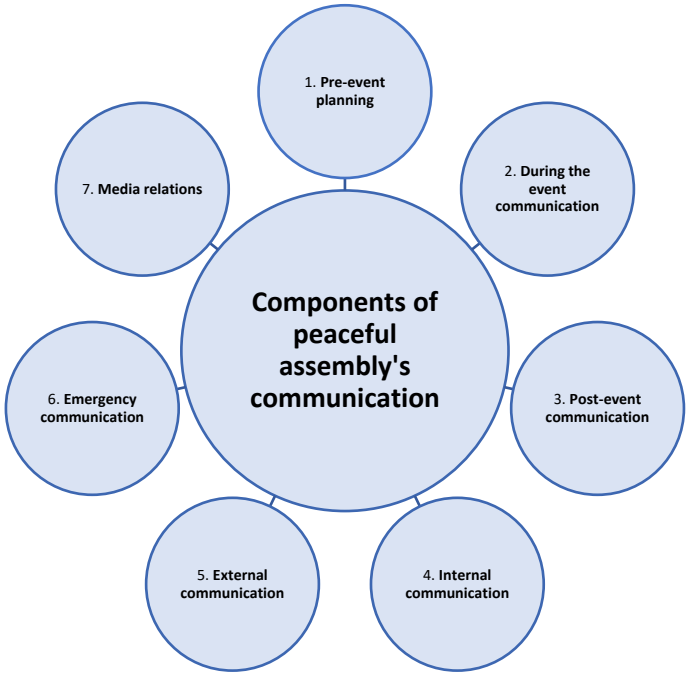
Maintaining the commonality of social media accounts with the latest security patches and software updates is critical for NGOs to preempt potential vulnerabilities exploitable by cyber attackers. By staying abreast of security enhancements and promptly implementing updates, NGOs can fortify the resilience of their digital assets, reduce the risk of security breaches, and enhance the overall protection of sensitive data and communications shared on social media platforms.

Approach six – verification of links and messages:

NGOs must prioritize verifying the legitimacy of links, messages, and requests received through social media channels to mitigate the risk of phishing scams or fraudulent activities. By promoting a culture of caution among staff members, emphasizing the importance of scrutinizing unknown links, and refraining from sharing personal information, NGOs can enhance their defenses against cyber threats and potential data breaches. This proactive approach ensures that NGOs uphold cybersecurity vigilance, protect sensitive information, and mitigate the impact of malicious attempts to compromise their digital security.

Section Two: Peaceful Assemblies' Communication

What is a peaceful assembly's communication?



A peaceful assembly's communication refers to the ways and methods used by organizers and participants to share information, logistics, and messages during a peaceful assembly, such as a protest, rally, or demonstration. Such communications are necessary to effectively coordinate peaceful activities and keep all participants safe and informed about everything. In this context, communication includes pre-event planning, during-event planning, and post-event planning.

What are the components of a peaceful assembly communication?

Figure 11: Components of peaceful assembly communication.

1. Pre-event planning:

Utilizing digital platforms like social media, emails, and websites to spread awareness, gather support, and share details about the event's time, location, and objectives.

2. During the Event:

Employing various means, such as loudspeakers, signs, and personal devices, to communicate messages to participants and to direct the crowd effectively. Group messaging apps or social media can also facilitate real-time updates to manage logistics dynamically and respond to any unforeseen circumstances.

3. Post-event communication:

To maintain engagement and momentum, participants should be contacted through announcements, debriefs, or publications that summarize the event's outcomes, express gratitude to attendees, and outline next steps or follow-up actions.

4. Internal communication:

The internal communication component of a peaceful assembly encompasses all strategies and tools used to coordinate communication among the organizers, volunteers, and any key stakeholders directly involved in executing the event. Effective internal communication is crucial to maintaining organization, ensuring safety, and adapting to situational changes during the assembly.

5. External communication:

Engaging with media and other external entities to broadcast the assembly's message more widely and portray the event accurately and favorably.

6. Emergency communication:

Emergency communication during a peaceful assembly refers to the predefined strategies and methods used to quickly relay information about urgent situations and coordinate responses among organizers, security personnel, volunteers, and participants. This form of communication is essential for managing potential crises and ensuring the safety of all individuals present.

7. Media relations:

Handling communication with the media to ensure the assembly’s objectives and narrative are correctly understood and reported. This could involve press releases, designated spokespersons, and media briefings before and after the event.

How to communicate before during and after a peaceful assembly?

Communicating effectively during a peaceful assembly in Afghanistan requires special considerations to ensure safety and compliance with the local laws and cultural norms. Here are some specific ways to communicate before, during, and after an assembly under such conditions:

Approach one – Legal compliance:

The ITA regulations prohibit organizing a peaceful assembly without authorization from the Ministry of Interior Affairs. Acquiring approval from the Ministry is incredibly challenging, bordering on unattainable. You should not take the risk or allocate any effort towards this endeavor. Attempting to establish a constructive dialogue with ITA representatives to secure approval for a peaceful assembly is unlikely to yield positive results.

Approach two – Monitor the situation:

Make sure to collect trustworthy information about any updates regarding public gatherings. Check news sources and reports from human rights organizations for up-to-date details.

Approach three – Develop an Internal communication strategy:

Develop a strategy and identify tools used to coordinate communication among the organizers, volunteers, and any key stakeholders involved directly in executing the event. Effective internal communication is crucial to maintaining organization, ensuring safety, and adapting to situational changes during the assembly. Please refer to figures 8, 9, and 10 to find the safest and best tools and platforms to communicate internally.

Approach four – Develop an external communication strategy:

Develop a strategy addressing how to engage with media and other external entities to broadcast the assembly's message more widely and to portray the event accurately and favorably. Please refer to figures 8, 9, and 10 to find the safest and best tools and platforms to communicate externally.

Approach five – Develop an emergency communication strategy:

Develop an emergency communication strategy before a peaceful assembly to quickly relay information about urgent situations and coordinate responses among organizers, security personnel, volunteers, and participants. This form of communication is essential for managing potential crises and ensuring the safety of all individuals present.

Approach six – Maintain your media relations:

Local media will never cover your event due to the safety of their reporters and outlets because they are prohibited from covering any assemblies. Maintain communication with the external media to ensure the assembly's objectives and narrative are correctly

understood and reported. This could involve press releases, designated spokespersons, and media briefings before and after the event. For safety measures, please check our *Peaceful Assembly Manual for Afghan Resilient Civil Society.*

Approach seven – Communication with participants:

Ensure that all participants in the assembly are aware of the safety guidelines. It's crucial to emphasize the significance of maintaining conduct, engaging in actions, and adhering to any agreed-upon codes of behavior. Additionally, encourage everyone to remain vigilant and report any activities they may notice during the assembly. For safety measures, please check our *Peaceful Assembly Manual for Afghan Resilient Civil Society*.

Approach eight – Coordinate with NGOs and HRDs:

If feasible, reach out to both international NGOs and HRDs in order to gain insights into the present circumstances. They possess precise knowledge about potential actions and necessary safety precautions.

Approach nine – Consider communication channels:

If you're planning to partake in or organize an assembly, think about secure ways to communicate. Encrypted messaging services can offer more privacy and security for organizers and participants. Never use your local phone number when you engage in an assembly. Please refer to figures 8, 9, and 10 to find the safest tools and platforms to communicate.

Approach ten – Engage international organizations and media:

Make sure that international human rights organizations and the media are aware of the assembly. Sometimes, in volatile environments, international observation can offer a degree of protection. Please refer to figures 8, 9, and 10 to find the safest and best tools and platforms to communicate externally.

Approach eleven – Think of a virtual assembly:

Evaluate if a physical assembly is not possible or if a virtual gathering through online platforms can achieve your goals without the associated risks. Please refer to figures 8 and 10 to find the safest and best tools and platforms for a virtual assembly.

Approach twelve – Display signs and symbols:

Consider using elements such as signs, banners, or symbols to express your message. These tools can play a role in conveying your cause or demands to observers, the media, and authorities.

Approach thirteen – Chant slogans:

Come together in slogan chants that reflect the gathering's purpose. This will foster a feeling of togetherness. Enhance the impact of your message but avoid any cultural sense-making words that ITA minds and shows reaction against them. However, a high percentage of words are sense-making when they end up organizing a peaceful assembly.

Approach fourteen – Engage in peaceful dialogue:

If you come across any situations with authorities and counter-protesters, try to engage in peaceful conversations with them and avoid any violence. Find a way to leave the area immediately.

Approach fifteen – Utilize social media:

During the assembly, do not live tweet or share updates on social media platforms. Posting photos, videos, and statements from the event will help engage an audience and increase awareness about your cause, but it puts everyone at risk. If you want to share anything, do it after the event. Meanwhile, be careful while posting videos and photos on social media platforms. It is highly recommended to use an anonymous account, blur participant faces, and use a VPN and TOR. Please refer to figures 3 and 5 to find the best VPN and TOR.

Approach sixteen – Emergency contacts:

Make sure to save emergency numbers on your phone or have them written down and kept with you. Meanwhile, providing an emergency contact could potentially put your loved ones at risk in the event of a phone seizure.

Approach seventeen – Low profile management:

Keep the event's profile low to avoid attracting unwanted attention. Avoid loudspeaker announcements and high-visibility banners.

Approach eighteen – Communication among organizers:

Maintain a discreet line of communication among organizers during the event to coordinate actions and respond to any unforeseen circumstances. If someone is monitoring electronic communication, use subtle signals.

Approach nineteen – Stay low-profile:

After you leave, make sure not to appear with the clothes you wore during assembly again, and do not carry any noticeable signs or materials from the gathering.

Approach twentieth – Check-in:

Reach out to your family or a friend through a safe social media communication tool that provides end-to-end encryption services. Inform them that you are safe. If you think you are not safe, do not share your location.

Approach twenty first – Debrief:

Do not gather with the participants at a venue to have a conversation about the event. While safe, plan any necessary actions moving forward. Use a social media communication tool like Signal, which offers 100% end-to-end encryption, for any arrangements. Do not speak over the phone number.

Approach twenty second – Social media caution:

It's important to be mindful of what you share on social media. Sometimes the information we post can pose potential risks to ourselves or those around us. If you have to share something on social media, use an anonymous account and a VPN.

Approach twenty third – Monitor the situation:

After completing the assembly, make sure to stay informed about the happenings in your area through news sources. This will help you stay informed about the assembly's consequences and any changes that may affect your safety.

Approach twenty fourth – Contingency plan:

Make sure you have a plan in case the peaceful gathering becomes chaotic or dispersed by security forces. It's best not to remain at your location and avoid traveling unless necessary. Find a place to stay. Only disclose your whereabouts if you are confident that no one will hand you over to ITA. Do not carry your mobile and registered phone number with you.

Approach twenty fifth – Quiet Debriefing after the event:

Conduct a low-key debriefing with key organizers to discuss the outcomes and any lessons learned. Make sure to conduct this in a secure and private manner. Instead of physically gathering, consider organizing a virtual gathering using the safest social media communication tool that offers encrypted messaging services. Please refer to figures 8, 9, and 10 to find the safest tools for your communication.

Approach twenty sixth – Careful Release of Information:

If sharing information about the event publicly (e.g., through social media or the press), be very cautious about what is shared to avoid potential repercussions. Highlights should focus on peaceful aspects and community involvement, without provoking authorities. Meanwhile, all participants have to cover their faces; if not, blur the faces of all participants exposed in a video or photo supposed to be publicized.

Approach twenty seventh – Follow-up support:

If there are any repercussions from the authorities, provide support to participants. Collaborate with domestic and international human rights organizations or community leaders to provide assistance where needed.

What communication terminology should be avoided during an assembly?

Before, during, and after an assembly in Afghanistan, it is important to avoid certain communication terminologies that may be considered sensitive or inappropriate. It is a bit difficult to introduce some specific terminologies, but anything related to topics that contradict the ITA's ideology would not be welcomed. It is crucial to be mindful of local customs, cultural norms, and the current political environment when communicating in such a setting. For additional details on how ITA monitors the use of these terminologies, please see What terminology should NGOs avoid while communicating?, which provides more information about the use of sensitive terminologies.

What are the safest communication tools and platforms to use in Afghanistan?

Please see figures 8, 9, and 10 for the safest communication tools and platforms.

What are the pros and cons of social media use in a peaceful assembly?

1. Pros:

Pro one – Awareness and Mobilization:

Social media platforms can be powerful tools for raising awareness and mobilizing participants quickly and effectively. Information about the assembly's time, location, and purpose can reach a wide audience in a short period of time.

Pro two – Information Sharing:

Social media allows for real-time updates and the sharing of information, which can be crucial for coordinating activities and responding to any changes or emergencies during the assembly.

Pro three – Community Building:

These platforms can help in building and sustaining communities of like-minded individuals who support the cause, fostering a sense of solidarity among participants.

Pro four – International Attention:

Through social media, the issues at the heart of the assembly can garner international attention, potentially leading to international support and pressure, which might influence outcomes positively.

Pro five – reach and engagement:

Social media platforms provide organizers with an essential resource to broaden their influence, connect directly with worldwide communities, and increase visibility for their causes. By utilizing the wide reach and interactive capabilities of social media, organizers can clearly convey their objectives, disseminate powerful narratives, and gather support from varied audiences. This digital strategy not only enhances their message but also cultivates a feeling of involvement and engagement among supporters, allowing for immediate interaction and feedback.

Pro six – advocacy y and networking:

Social media platforms offer organizers a versatile suite of tools to promote social change, garner support for their initiatives, and build relationships with allies and stakeholders. By leveraging the communicative capabilities of social media, organizers can effectively highlight important issues, energize community support for their efforts, and develop collaborations that enhance their influence. This digital environment not only acts as a medium for disseminating messages but also helps create a connected community committed to fostering positive social change and achieving shared objectives in the social impact sector.

Pro seven – direct communication:

Direct engagement with your audience is essential for reaching your goals. Social media enables interactive communication with your supporters, allowing for immediate and active exchanges. This direct channel of communication, enhanced with tailored information, can efficiently speed up the transition from increasing awareness to prompting the desired action.

Pros eight – information dissemination:

Incorporating social media into their outreach strategies enables organizers to efficiently disseminate time-sensitive updates, valuable resources, educational content, and crucial emergency notifications to the public. By harnessing the immediacy and broad reach of social platforms, organizers can swiftly distribute vital information, engage with their audience, and respond effectively to unfolding events, ensuring that their communications are not only timely but also impactful and far-reaching.

Pro nine – maximizing awareness and connection:

Social media acts as a powerful tool for connectivity, serving as a dynamic platform for increasing awareness. It allows organizers to engage with a vast audience looking to connect with like-minded individuals and causes they care about. Through instant sharing of information and visuals, social media provides a window into an assembly, enhancing the well-crafted messages that reflect its purpose.

2. Cons:

Con one – Government Surveillance and Repression:

There is a high risk of surveillance on social media in Afghanistan. The use of these platforms can expose organizers and participants to risks, including arrests or worse, if they are perceived as opposing policies.

Con tow - Misinformation and Disinformation:

The spread of misinformation and disinformation can occur rapidly on social media, potentially leading to confusion, spreading rumors, and weakening the assembly's objectives.

Con three – Incitement and Violence:

Social media posts can be taken out of context or manipulated to incite violence or aggressive actions, which could jeopardize the peace and legality of the assembly.

Con five – Fragmentation:

While social media can unify, it can also fragment groups. Differences in opinions and approaches can become more pronounced, leading to splinter groups and weakening the collective strength of the assembly's participants.

Con six – Security risks:

Integrating social media strategies in conflict zones like Afghanistan can present security hurdles, involving potential threats to the safety of organizers, security personnel, and volunteers. When utilizing social platforms, organizers must address concerns about the disclosure of sensitive information, the possible targeting of participants or volunteers, and the protection of essential resources in environments marked by instability and security challenges.

Con seven – Censorship and surveillance:

Organizers of peaceful assemblies in Afghanistan face challenges related to internet censorship, surveillance tactics, and restrictions on freedom of speech when utilizing social media platforms. To overcome these barriers, one must navigate tight digital content regulations, increased surveillance that poses risks to privacy and safety, and limitations on open communication through online channels. These obstacles highlight the intricate environment in which organizers have to work when utilizing social media in Afghanistan, emphasizing the need for thoughtful deliberation and adjustment to guarantee efficient and secure communication approaches.

Con eight – Misinformation and disinformation:

Social media platforms act as channels for spreading misinformation, propaganda, and inaccurate stories, presenting a threat to the reputation and credibility of the organizers of a peaceful assembly. The spread of false information via these platforms can tarnish the

image of a peaceful assembly, eroding public confidence and distorting the true representation of their goals and purpose. Therefore, organizers need to stay alert when maneuvering through the realm of social media to counter misinformation successfully and protect their integrity in the digital domain.

Con nine – Privacy concerns:

Organizers of a peaceful assembly should exercise caution when it comes to data privacy, cyber risks, and threats to information security while sharing sensitive data on social media channels. The decision to disclose such information exposes vulnerabilities to potential data breaches, illicit access, and misuse by malicious entities, highlighting the significance of establishing strong protections and procedures to safeguard sensitive data and uphold the credibility of their activities in the online sphere.

How to expose on media and social media during and after a peaceful assembly?

In Afghanistan, utilizing media and social media to expose or cover a peaceful assembly demands careful strategic planning due to the highly restrictive and monitored environment. Here are some guidelines and precautions to consider when using media and social platforms during and after an assembly:

Approach 0ne – Safety first:

Always prioritize the safety of participants. If exposing information is likely to lead to punitive measures against individuals, it might be necessary to withhold that information.

Approach tow – Anonymous reporting:

Ensure anonymity in reports to protect the identities of those involved. Use methods such as voice distortion and blurring faces in videos and photos to safeguard participants from reprisals.

Approach three – Secure networks:

Use secure and encrypted communication tools to disseminate information. This reduces the risk of surveillance and interception by authorities. Please refer to figures 8, 9, and 10.

Approach four – Selective sharing:

Be selective about what to share in real time. Avoid broadcasting strategic locations or movements that could be used against participants by adversaries.

Approach five – Real-time monitoring:

Continuously monitor the situation to address any misinterpretation or misuse of the shared information. Quick clarification or removal of posts might be necessary to prevent escalation.

Approach six – Domestic and international media engagement:

Engage with trusted local and international media that may cover the event more extensively, while also providing an additional layer of protection through their presence and interest.

Approach seven – Documented evidence:

Compile and archive visual and textual evidence of the assembly, ensuring it is stored safely and can be accessed for future advocacy without compromising the safety of individuals involved. But be careful that the documented evidence doesn't leak out.

Approach eight – Controlled exposure:

Control the narrative by releasing information in phases to keep the topic relevant and in public discourse while managing risks.

Approach nine – Use vetted channels:

Use channels and platforms that have established protocols for sensitive content to ensure that the shared information does not lead to harmful consequences.

Approach ten – feedback loop:

Establish a feedback loop with participants and supporters to assess the effectiveness of the media strategy and make adjustments for future activities.

Approach eleven – Data protection measures:

Securing sensitive information on social media is crucial for assemblies. Organizers can safeguard this information by implementing stringent security practices, such as generating strong, unique passwords, enabling two-factor authentication for enhanced security, and restricting access solely to organizers. Adopting these measures helps prevent unauthorized access, data breaches, and the misuse of confidential information, thereby protecting their digital presence and preserving their audience's trust.

Approach twelve – Privacy settings:

Organisers of a peaceful assembly must use the privacy settings provided by social media platforms to effectively manage their online presence. Carefully adjusting these settings to control who can see their posts, messages, and profile information allows organizers to protect sensitive data and private conversations from public exposure. This deliberate strategy helps maintain confidentiality, secures important information, and preserves the integrity of their communication channels on various social media platforms.

Approach thirteen - Training and education:

It is vital for organizers to provide security personnel and volunteers with thorough training in data security, privacy practices, and social media guidelines to effectively minimize risks during online interactions and communications. Educating these individuals on identifying and addressing potential threats strengthens their ability to combat cybersecurity violations, privacy breaches, and the spread of misinformation. By taking this proactive step, we equip security personnel and volunteers to securely navigate digital platforms, safeguard sensitive information, and uphold the integrity of the assembly's online reputation.

How to build a constructive dialogue with the ITA representatives?

ITA regulations explicitly prohibit initiating a peaceful assembly without prior authorization from the Ministry of Interior Affairs. Securing approval from the Ministry is exceptionally challenging, verging on the unfeasible. We strongly advise against taking any risks or investing effort in this pursuit. The likelihood of successfully engaging in a constructive dialogue with ITA representatives to obtain approval for a peaceful assembly is minimal.

Engaging in any communication with ITA representatives during an unauthorized peaceful assembly is expected to result in adverse consequences. We recommend leaving the premises immediately and not returning to the area after the assembly.

For further details, please refer to our Peaceful Assembly Manual for Afghan Resilient Civil Society.

What to communicate at the end of an assembly?

1. Conclusion:

Make a public announcement about the assembly's conclusion. Typically, this announcement aligns with the delivery of the message. At times, security concerns may necessitate concluding a peaceful assembly earlier than scheduled. Make sure to use an appropriate communication method to inform all participants about the conclusion. Prior to mobilizing, it is critical to communicate the planned conclusion time and procedures for ending the event.

2. Instructions:

Provide participants with clear instructions on how to disperse from the assembly. Encourage them to vacate the area peacefully and avoid any confrontations with authorities or counter-protesters. We recommend that participants take different routes to exit the area.

3. Facilitate a peaceful exit:

To ensure a safe departure, it is crucial to designate and communicate exit routes or points to all participants. Make sure to clearly mark, secure, and easily accessible these routes.

4. Monitor the situation:

As an organizer, remain vigilant for signs of tension or potential conflicts so that you can communicate effectively with participants and volunteers. It is essential to stay alert and swiftly tackle any issues that arise. Promote peaceful behavior and intervene if necessary to resolve any disputes or conflicts.

5. Post-assembly contacts:

Exercise caution when sharing post-assembly information with participants. This may involve updates on subsequent gatherings or events linked to the cause, ways to sustain advocacy efforts, or disengagement for security concerns. Offer a secure contact method for participants to remain connected, receive updates, or disconnect for safety reasons. Maintaining ongoing communication and involvement with all participants outside of the assembly is essential.

6. Document the assembly:

Ensure that someone is designated to document the assembly by capturing photos and videos, if it is deemed safe to do so. This documentation will act as proof of the event's nature and can be instrumental in countering any inaccurate narratives or allegations that might surface subsequently. Additionally, it is crucial to evaluate the gathering's effectiveness, pinpoint any challenges encountered, and highlight areas for enhancement in future events. Refrain from sharing the images and videos with any individuals. If you choose to post them on social media, consider using an anonymous account, VPN, or TOR for privacy and blurring the faces of all participants.

Reference

1. https://www.hrw.org/news/2021/10/01/afghanistan-taliban-severely-restrict-media
2. https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf
3. https://www.csis.org/analysis/talibans-increasing-restrictions-civil-society-and-aid-organizations
4. https://press.un.org/en/2023/sc15222.doc.htm
5. https://www.rferl.org/a/afghanistan-taliban-ban-swedish-ngo-humanitarian-crisis/32504979.html
6. https://protonvpn.com/
7. https://mullvad.net/en
8. https://www.expressvpn.com/
9. https://nordvpn.com/
10. https://www.cyberghostvpn.com/
11. https://righttoconnect.org/online-resources/
12. https://bitwarden.com/
13. https://www.lastpass.com/
14. https://1password.com/
15. https://www.dashlane.com/
16. https://keepassxc.org/
17. https://support.torproject.org/tbb/
18. https://community.brave.com/
19. https://www.whonix.org/
20. https://tails.net/
21. https://guardianproject.info/apps/info.guardianproject.orfox/
22. https://riseup.net/en/email
23. https://www.autistici.org
24. https://proton.me/mail
25. https://tuta.com
26. https://disroot.org/en
27. https://meet.jit.si

28. https://demo.bigbluebutton.org
29. https://whereby.com
30. https://www.bluejeans.com
31. https://www.goto.com/meeting
32. https://support.apple.com/en-ca/guide/deployment/dep154cd083a/web
33. https://meet.google.com
34. https://meet.google.com/calling/
35. https://www.microsoft.com/en-ca/microsoft-teams/log-in
36. https://twitter.com/
37. https://www.clubhouse.com/
38. https://zoom.us/
39. https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance