Digital Democracy Initiative

TRAINER'S

Module

STRATEGIC COMMUNICATIONS

ADI SOUTH ASIA accountabilitylab

Table of Content

1. Introduction 3
2. Who this module is for 3
3. How to use this module alongside presentations 3
4. SESSION 0 — Opening and Framing: Advocacy, Communication, and Digital Safety 4
   4.1. Introduction 4
   4.2. Understanding the link between advocacy, communication, and digital safety 4
   4.3. Why communication choices generate digital risk 4
   4.4. Why digital safety enables sustained advocacy 5
   4.5. The South Asian risk environment 5
   4.6. Safety as a strategic condition for influence 6
   4.7. Practical implications for trainees 6
   4.8. Further reading and external resources 6
5. SESSION 1 — Opening and Framing: Advocacy, Communication, and Digital Safety 7
   5.1. Introduction 7
   5.2. Advocacy in high-risk environments 7
   5.3. The dual nature of visibility 7
   5.4. Strategic engagement as protection 8
   5.5. Constraints as structural conditions 8
   5.6. Advocacy as deliberate practice 8
   5.7. Further reading and external resources 8
6. SESSION 2 — Ethical and Strategic Digital Storytelling 9
   6.1. Introduction 9
   6.2. Why storytelling carries risk 9
   6.3. Consent as an ethical and strategic foundation 9
   6.4. Anonymity and representation 10
   6.5. Narrative choices as strategic decisions 10
   6.6. Storytelling and impact without harm 10
   6.7. The South Asian context 11
   6.8. Practical implications for trainees 11
   6.9. Further reading and external resources 11
7. SESSION 3 — Strategic Communication in Risky Digital Spaces 11
   7.1. Introduction 11
   7.2. Understanding how platform dynamics shape risk 12

7.3. Amplification and the mechanics of visibility 12
7.4. The strategic role of timing 12
7.5. Deliberate engagement over reflexive visibility 12
7.6. Operating within adversarial environments 13
7.7. Communication as a resilience practice 13
7.8. Further reading and external resources 13
8. SESSION 4 — Responding to Harassment and Digital Attacks 14
8.1. Introduction 14
8.2. Understanding escalation patterns 14
8.3. Anatomy of a digital attack 14
8.4. Psychological and organisational impact 15
8.5. Internal coordination and response planning 15
8.6. Managing visibility during harassment 15
8.7. Protecting organisational credibility 16
8.8. Building long-term resilience 16
8.9. Further reading and external resources 16

1. Introduction

This module is designed as a self-paced learning resource that complements the presentations used during the training. While the live sessions walked participants through the arguments, visuals, and real-world cases in an interactive format, this module provides a deeper narrative explanation of the concepts, helping learners revisit the ideas at their own pace and apply them in their organisational contexts. It brings together the themes of advocacy, communication, and digital safety, showing how each of these areas intersects when civil society operates in digital environments shaped by polarisation, surveillance, and the possibility of retaliation.

The purpose of this module is to give civil society workers, advocacy practitioners, communicators, and organisational leaders a clearer understanding of why digital communication decisions carry strategic consequences. The presentations demonstrate how narratives circulate, how visibility generates both opportunity and exposure, and how digital spaces can quickly shift from supportive to adversarial. This module expands on those insights by providing additional explanations, real-world examples, and external research that help readers understand the mechanics of digital risk and the conditions under which advocacy becomes vulnerable.

2. Who this module is for

The module is written for civil society actors who operate in politically sensitive or high-risk environments. This includes advocacy leads, communication teams, programme staff, and organisational leadership working on human rights, governance, gender equality, transparency, accountability, or community mobilisation. It is equally useful for individuals who regularly participate in online discourse or use digital channels to share stories, campaign for reform, or draw attention to rights-based issues. Anyone engaging with public narratives in digital spaces will find this module relevant, particularly those who are exposed to harassment, disinformation, surveillance, or politicised backlash.

3. How to use this module alongside presentations

The presentations provide visual clarity, case studies, diagrams, and examples that were discussed during the training. This module should be read as a companion that expands on those visuals and turns them into a comprehensive learning resource. Learners are encouraged to review the corresponding slides before or after each section of the module, placing the narrative explanations in context with the visuals. Where the presentations offer snapshots of real incidents or patterns of harassment, this module deepens those examples with additional research and external references. Where the slides outline concepts through diagrams, this module explains the logic behind them and demonstrates how they apply in real advocacy environments.

Taken together, the presentations and this module form a complete learning package. The slides illustrate how hostility, amplification, narrative distortion, and risk evolve in digital spaces, while the module gives the detailed understanding required to recognise these patterns and build safer, more deliberate advocacy practices. The goal is to help civil society practitioners engage effectively without

being overwhelmed by engineered hostility or unintended consequences of visibility, ensuring that their advocacy remains impactful, safe, and sustainable.

4. SESSION 0 — Opening and Framing: Advocacy, Communication, and Digital Safety

[Presentations attached: Session 0, Session 0.1]

4.1. Introduction

Advocacy in today's digital environment is shaped as much by communication choices as it is by political context. Civil society organisations increasingly operate in online spaces where visibility, narrative framing, and public engagement are inseparable from risk. This introductory session sets the conceptual foundation for the entire training by explaining why advocacy, communication, and digital safety form a single, interconnected system. The presentations used during the training highlight that exposure in digital spaces is not neutral; it creates pathways through which adversarial actors can intervene, distort narratives, silence individuals, and compromise organisational security. Digital safety, therefore, is not a restriction but the condition that allows advocacy to continue.

4.2. Understanding the link between advocacy, communication, and digital safety

Advocacy requires communication, and communication now takes place primarily through digital platforms. Because these platforms privilege virality, speed, and high-volume engagement, advocacy messages inevitably enter contested spaces where interpretation, mobilisation, and manipulation happen simultaneously. The presentation slides (attached) emphasise this dynamic visually. To summarise, online harassment is an engineered system, resembling a coordinated operation designed to overwhelm dissenting voices and distort public debate.

This framing helps learners understand that digital threats are not accidental incidents; they arise when adversarial actors deliberately respond to specific communication triggers.

The visual metaphor on page 4 reinforces this by portraying harassment as a swarm-like assault in which scattered individuals are surrounded and drowned out.

This demonstrates how the intensity of digital abuse often correlates with moments of heightened visibility, showing that communication choices, such as posting sensitive content without preparation or tagging polarising actors, can create direct risk exposure. This makes it clear that advocacy and digital safety cannot be separated: any public message has implications for the organisation's threat landscape.

4.3. Why communication choices generate digital risk

Communication in digital spaces involves decisions about timing, tone, audience, framing, tagging, and visibility. Each of these has risk implications. A message published at a politically sensitive moment may attract adversarial attention. Using charged language can provoke hostile mobilisation.

Tagging specific actors may expose the organisation to surveillance, trolling, or retaliatory targeting. The design of communication, including images, hashtags, and call-to-actions, may unintentionally escalate visibility to networks that seek to distort or weaponise the narrative.

The presentations illustrate this with clarity. Reference to 'When Hashtags Become Weapons' demonstrates that hostile networks strategically manipulate hashtags, amplify harmful narratives, and deploy coordinated harassment to silence civil society voices. Reference to the slides, "Engineered Manipulation of Discourse" shows how influence networks dominate political conversations by overwhelming organic engagement.

The structure of these attacks reveals that communication, not merely presence, can trigger risk. When organisations fail to account for how their messages may be intercepted or amplified by hostile actors, exposure increases.

4.4. Why digital safety enables sustained advocacy

Digital safety provides the foundation for long-term advocacy by protecting people, information, and organisational systems. Civil society cannot sustain public engagement if staff are routinely harassed, if accounts are compromised, if content is misrepresented, or if organisational data is breached. Safety practices ensure that advocacy does not collapse under pressure.

The example of the harassment campaign against journalist Gharidah Farooqi, referred to in the presentation, illustrates the stakes. The campaign lasted a week and involved 166,900 tweets at its peak, far beyond organic behaviour.

The analysis shows that most activity in such harassment campaigns comes from repetitive reposts rather than genuine conversation, indicating engineered amplification rather than organic engagement. The visuals also reveal the use of large volumes of altered or manipulated images, demonstrating how these campaigns escalate pressure, distort narratives, and intensify intimidation. This type of hostile engagement can easily overwhelm an individual or organisation, derail advocacy efforts, and induce long-term self-censorship unless safety strategies are already in place.

4.5. The South Asian risk environment

Civil society in South Asia operates in politically tense digital ecosystems. Harassment networks, organised trolling, surveillance actors, and political influence machines frequently intervene in online narrative spaces. This makes communication highly sensitive. The presentation frames this environment through visual references to narrative flooding, showing how saturation of a hashtag or coordinated repetition can drown out authentic voices.

Across Pakistan, India, Bangladesh, Nepal, and Sri Lanka, online discourse is shaped by algorithmic prioritisation, polarisation, and the collapse of fact-based narratives under the weight of viral misinformation. Civil society organisations advocating on issues like human rights, women's rights, civic accountability, and transparency face digital risks not because of their organisational structures but because visibility puts them in the crosshairs of actors seeking to delegitimise or intimidate them.

This regional context reinforces why communication, advocacy, and safety must be treated as a single unit of practice rather than as siloed technical areas.

4.6. Safety as a strategic condition for influence

Effective advocacy requires credibility, continuity, and resilience. None of these is possible when digital risks are unmanaged. When organisations view safety only as a technical checklist, they miss its strategic function. A secure communication environment allows organisations to speak without fear, maintain narrative consistency, protect their staff and communities, and build long-term advocacy momentum. Digital safety enables narrative intervention and public engagement without exposing individuals to avoidable harm.

This is especially important because digital hostility produces psychological consequences. The visual metaphor symbolises the fear-driven withdrawal many activists experience after witnessing targeted harassment. Research from Media Matters for Democracy documents widespread self-censorship among women journalists in Pakistan for exactly this reason. Without safety, the people who are most essential to public-interest advocacy are pushed out of the digital sphere, shrinking civic space.

4.7. Practical implications for trainees

For trainees, the core lesson of this opening module is that advocacy does not begin with messaging; it begins with safety. Every decision about what to say, when to say it, who to involve, how much visibility to generate, and which communities to spotlight must be guided by an understanding of digital risk. When communication choices are deliberate and safety-informed, civil society can participate in digital democracy with greater confidence, resilience, and strategic effectiveness.

4.8. Further reading and external resources

- Access Now – Digital rights, incident response, and global documentation of harassment against activists
  https://www.accessnow.org/keepiton/
- EFF – Guides and analysis on privacy, surveillance, and digital protection for vulnerable groups
  https://eff.org/issues
- Citizen Lab – Research on targeted digital repression, spyware, and coordinated online attacks
  https://citizenlab.ca/research/
- Tactical Tech – Influence operations, political manipulation, and civic-space interference
  https://tacticaltech.org/projects/the-influence-industry/
- CIVICUS Monitor – Country profiles on civic space restrictions and digital repression
  https://monitor.civicus.org/
- UN Special Rapporteur on Freedom of Expression – Reports on digital repression, online harassment, and state pressure on civic actors
  https://www.ohchr.org/en/special-procedures/sr-freedom-of-expression
- Media Matters for Democracy – Research on online violence against women journalists in Pakistan
  https://mediamatters.pk/media-matters-for-democracy-launches-a-new-study-examining-the-impact-of-online-harassment-on-women-journalists/

5. SESSION 1 — Opening and Framing: Advocacy, Communication, and Digital Safety

[Presentations attached: Session 1]

5.1. Introduction

Advocacy in high-risk digital environments requires civil society actors to operate with a clear understanding of how visibility, narrative exposure, and platform dynamics shape both opportunity and threat. In politically sensitive contexts such as Pakistan, advocacy is never simply about raising a voice and it is about navigating power, surveillance, and hostility while still finding ways to mobilise communities and influence public discourse.

This session builds on the framing introduced earlier by examining how advocacy must adapt when the very act of speaking publicly can trigger backlash, distortion, or targeted pressure. It helps trainees understand how visibility can be empowering, but also how uncontrolled visibility can undermine the very goals an organisation is trying to pursue.

5.2. Advocacy in high-risk environments

The presentation for this session illustrates, visually and conceptually, that advocacy in constrained environments is shaped by the twin forces of political sensitivity and digital amplification. One of the early slides shows a spectrum of risk where seemingly routine acts of communication, such as naming a stakeholder or sharing a field image, can escalate when hostile networks pick them up.

The session emphasises that high-risk advocacy is not defined only by the issue at hand but by the digital terrain in which it unfolds: polarised publics, misinformation ecosystems, surveillance actors, and adversarial networks capable of reshaping narratives in minutes. In such environments, advocacy must be carefully calibrated to avoid unnecessary exposure while still achieving strategic goals.

5.3. The dual nature of visibility

Much of civil society advocacy relies on visibility. Public pressure, storytelling, evidence sharing, and mobilising audiences demand attention. But visibility has a dual nature. It is a tool for influence and also a point of vulnerability.

When organisations become highly visible without preparation, their messages may be twisted, their staff may be targeted, and their work may be reframed in ways that shrink their operational space. High visibility can attract public support, but it can also attract organised backlash, politicised misrepresentation, or hostile scrutiny, especially when dealing with sensitive themes such as governance, transparency, or human rights.

The core lesson is that visibility is not inherently good or bad; it is an exposure that must be intentionally shaped. The right visibility, at the right moment, with the right safeguards, strengthens advocacy. The wrong visibility, too early, too loud, or poorly framed, can harm the organisation, derail the issue, or endanger vulnerable communities.

5.4. Strategic engagement as protection

Strategic advocacy means organisations do not speak simply because a moment demands it; they speak with clarity on who the message is for, how far it is likely to spread, how hostile actors might respond, and what internal preparations are required if the communication escalates.

This requires understanding how algorithms reward polarisation, how hashtags evolve, and how digital conversations can be hijacked. It also requires operational awareness inside the organisation: who has access to accounts, who approves messaging during sensitive moments, how crisis escalation is handled, and what safeguards exist to protect staff or communities featured in advocacy content. Strategic engagement, therefore, becomes a risk-management practice and an influence practice at the same time.

5.5. Constraints as structural conditions

The session also shows that civil society actors operate under structural constraints that are far larger than individual organisations. The slides point to moments where platform manipulation, targeted harassment, politicised reporting, and pressure from powerful actors shape what CSOs can safely say online.

These constraints are not hypothetical, they shape everyday advocacy. When a hostile group can weaponise a hashtag, when a political actor can mobilise trolling networks, when a campaign can be derailed through misinformation, or when a narrative can be reframed overnight, advocacy becomes a high-stakes exercise.

Yet constraints do not mean silence. The session emphasises that CSOs can and must continue to advocate, but they must do so with a clearer sense of timing, phrasing, and exposure. This allows organisations to identify safe windows for communication, limit unnecessary provocation, protect vulnerable groups, and maintain long-term credibility even in politically tense environments.

5.6. Advocacy as deliberate practice

The central message of Session 1 is that advocacy cannot be improvised. It is a deliberate practice shaped by risk awareness, narrative discipline, and strategic visibility. Effective advocacy under constraint requires organisations to understand the digital field they operate in, anticipate amplification dynamics, and prepare for backlash before it happens. This transforms advocacy into a form of resilience, allowing civil society to speak confidently without exposing itself to harm.

5.7. Further reading and external resources

- Access Now – How digital threats affect activists and advocacy work https://www.accessnow.org/keepiton/
- ARTICLE 19 – Global analysis on freedom of expression under digital repression https://www.article19.org/resources/
- Chatham House – Strategic communication in civic conflict zones https://www.chathamhouse.org/

- UN OHCHR – Reports on reprisals and intimidation against human rights defenders https://www.ohchr.org/en/issues/sr-human-rights-defenders
- The Carnegie Endowment – Research on digital authoritarianism and shrinking civic space https://carnegieendowment.org/specialprojects/digitaldemocracy/

6. SESSION 2 — Ethical and Strategic Digital Storytelling

[Presentation attached: Session 2]

6.1. Introduction

Storytelling is at the heart of civil society work, but in today's digital environment, it is also one of the most sensitive and high-risk components of advocacy. The stories CSOs publish shape public narratives, influence power, mobilise communities, and challenge dominant discourses. They also expose real people to real dangers. This session helps trainees understand that digital storytelling is not merely a creative exercise; it is an ethical and strategic practice that requires careful attention to consent, anonymity, representation, and platform behaviour. The goal is to show how stories can generate impact while reducing the harm that often accompanies visibility in volatile digital spaces.

6.2. Why storytelling carries risk

The Sesssion emphasises that storytelling decisions directly influence risk exposure. Many of the visuals highlight how narrative elements, photos, quotes, location details, and hashtags can unintentionally reveal identities or contexts that adversarial actors may exploit. The presentation attached outlines how digital stories travel far beyond intended audiences, often stripped of context as they circulate.

When a story moves through networked platforms, it becomes vulnerable to misinterpretation, politicisation, and targeted harassment, especially when it deals with marginalised communities, sensitive rights violations, or politically charged subjects.

This means that ethical storytelling is not only about accuracy and dignity; it is about anticipating how a story behaves once it enters an environment shaped by algorithms and adversarial actors. The risk does not lie in the content alone, but in the journey the content takes.

6.3. Consent as an ethical and strategic foundation

Consent is the cornerstone of ethical storytelling, but in a digital context, it must go far beyond basic permission. This includes understanding how audiences may react, how far the content may spread, whether it could trigger reputational or security harm, and whether the story might later be reinterpreted in a politicised environment.

For civil society, this means reframing consent as a strategic conversation, and considering asking the following questions:

- Does the individual understand the risks of going public?
- Is the story being shared in a way that protects them if public sentiment turns hostile?
- Is the organisation prepared to manage backlash if the story becomes the target of narrative manipulation?

The presentation's emphasis on informed, continuous, and opt-out consent surfaces the idea that safety is not a single decision but an ongoing process.

6.4. Anonymity and representation

The slides also highlight the role of anonymity in safeguarding individuals, particularly in contexts of political repression, gendered harassment, or social stigma. The presentation maps different levels of anonymisation, from altering names to removing visual identifiers, showing how strategic anonymisation can preserve impact without exposing identities.

Representation, similarly, carries ethical weight. A story is not neutral; it frames a person or community in a particular light and invites the audience to react. Misrepresentation can fuel stereotypes, reinforce harmful narratives, or be used by adversarial actors to delegitimise the organisation. Ethical representation, therefore, means portraying individuals and communities with dignity, accuracy, and agency, while remaining aware that adversaries actively seek missteps to weaponise.

6.5. Narrative choices as strategic decisions

The presentation reinforces that narrative choices shape how content is interpreted and how it circulates. The presentations attached explain how narrative framing, whether a story is told through a lens of vulnerability, resilience, rights, injustice, or solidarity, affects the kind of attention it attracts.

In sensitive contexts, certain framings may provoke backlash or be hijacked by politicised actors seeking to reshape the narrative for their own purposes.

This is why digital storytelling must be deliberate. Storytellers must consider:

- How might adversaries react?
- Could the narrative escalate into digital harassment?
- Does the framing unintentionally expose beneficiaries to scrutiny?
- Does the story need to be paced, contextualised, or anonymised differently?

Strategic storytelling means acknowledging that stories do not exist in isolation; they exist in contested digital spaces where multiple actors compete for narrative dominance.

6.6. Storytelling and impact without harm

Impactful storytelling requires visibility, but ethical storytelling requires moderation of that visibility. The Session slides emphasise that stories can still achieve influence, mobilisation, and awareness without putting people at risk. For instance, the "framing spectrum" that ranges from fully identified storytelling to fully anonymised documentation, each suited for different levels of risk.

Many powerful advocacy stories have achieved scale precisely because they were carefully anonymised, contextually framed, or disseminated in phases to manage exposure.

The goal is to produce stories that resonate deeply but do not create unintended digital footprints that adversaries can weaponise. Ethical storytelling prioritises human dignity; strategic storytelling adds the layer of anticipating how hostile actors might distort the narrative.

6.7. The South Asian context

Digital storytelling in South Asia takes place within a politically charged, polarised, and surveillance-heavy environment. Narratives around human rights, gender, minorities, governance, corruption, or political dissent are routinely hijacked by organised networks. Hostile actors use manipulated visuals, miscontextualised screenshots, and selective amplification to discredit individuals and groups.

The earlier presentation provides clear evidence of this. The visuals on coordinated harassment campaigns show how adversarial networks repurpose narrative elements, images, quotes, or hashtags to distort public meaning and escalate attacks.

This underscores the need for careful narrative design, especially when dealing with vulnerable communities whose stories may be twisted into disinformation.

6.8. Practical implications for trainees

For civil society professionals, this session reinforces that storytelling must be grounded in ethical responsibility and strategic foresight. Decisions about what details to include, what identifiers to remove, how to frame a narrative, and when to publish are integral to protecting communities. Ethical storytelling protects dignity; strategic storytelling protects safety. Together, they allow organisations to produce impactful narratives that advance advocacy goals without exposing individuals to harm.

6.9. Further reading and external resources

- Tactical Tech – Guide on the ethics of digital storytelling and the risks of data exposure https://tacticaltech.org/projects/data-and-activism/
- UN OHCHR – Principles on human dignity, representation, and protection in human rights documentation https://www.ohchr.org/
- WITNESS – Resources on ethical video, anonymity, and safeguarding vulnerable subjects https://www.witness.org/resources/
- Access Now – Digital security guidance for activists managing sensitive stories https://www.accessnow.org/keepiton/
- CIVICUS – Case studies on storytelling in restrictive civic environments https://monitor.civicus.org/

7. SESSION 3 — Strategic Communication in Risky Digital Spaces

[Presentation attached: Session 3]

7.1. Introduction

Digital spaces have become central to how civil society communicates, mobilises, and influences public narratives. But these spaces are also unpredictable, polarised, and shaped by algorithms that privilege speed and outrage over nuance. This session helps trainees understand that communication in digital environments is never neutral; it is shaped by platform incentives, adversarial behaviour, and the unpredictable pathways content takes. Strategic communication, therefore, becomes a protective

discipline. It enables organisations to engage deliberately rather than reactively, ensuring that their messages generate impact without exposing staff or communities to unnecessary risk.

7.2. Understanding how platform dynamics shape risk

Early slides show that visibility is primarily determined by algorithmic signals such as engagement spikes, emotional intensity, timing, network behaviour, and audience clustering.

In high-risk contexts, these signals can work against civil society: a post intended for awareness-raising may suddenly become hyper-visible due to algorithmic amplification, attracting hostility that the organisation did not anticipate.

Later visuals reinforce that platforms reward content that polarises, provokes, or emotionally engages, while more nuanced advocacy messages may gain slower traction. This means organisations must understand the digital ecosystem before entering it. Without this awareness, communication decisions can escalate into unwanted exposure that compromises safety.

7.3. Amplification and the mechanics of visibility

Amplification is one of the most important dynamics shaping risk in digital environments. The presentation highlights how posts can quickly jump from small, controlled audience groups to wider, adversarial networks through retweets, quote tweets, duets, stitches, dupe videos, and stitched commentary. The Session discusses how content spreads beyond the original audience once it enters the "public amplification layer," a zone where coordinated actors, political proxies, or troll networks intervene.

This amplification is not always organic. Influential actors, political groups, state-aligned clusters, and interest networks can deliberately boost content to distort narratives, overwhelm CSO messaging, or provoke harassment. Civil society organisations must therefore treat amplification not as a measure of success but as a potential vector of risk. In short, the moment a story begins gaining traction is the moment safety protocols must activate.

7.4. The strategic role of timing

Timing is presented in the module as one of the most decisive factors in determining whether communication will remain safe or become weaponised. The presentation visually outlines how the same message can have different consequences depending on when it is posted, during a political controversy, a sensitive national moment, or peak hours of online mobilisation.

Timing determines who sees the message first, how quickly it spreads, and whether adversarial networks are active enough to hijack the narrative. In Pakistan, for instance, majoritarian groups, hyper-partisan influencers, and political digital teams operate in predictable cycles. Strategic communication requires aligning messaging with calmer windows, avoiding moments of mass political agitation, and anticipating periods when disinformation actors are most active.

7.5. Deliberate engagement over reflexive visibility

A central lesson of this session is that reflexive posting, publishing content simply because an issue is trending, often exposes organisations to harm. Strategic communication requires shifting from urgency-

driven behaviour to intentional engagement. The slides illustrate this on page 10 by showing two contrasting approaches: “reflexive visibility,” where content is posted impulsively and escalates unpredictably, and “deliberate visibility,” where communication is timed, contextualised, and internally prepared.

Deliberate communication also means choosing the right platform for the right purpose. Not every issue requires a public-facing post. Some narratives are safer in closed networks, newsletters, community groups, offline briefings, or controlled messaging channels. Strategic communication requires asking not just “What should we say?” but “Where and when should we say it, and what are the consequences?”

7.6. Operating within adversarial environments

The South Asian digital environment is shaped by organised influence operations, political propaganda networks, coordinated trolling groups, and state-linked actors that monitor civic narratives. Communication strategies must account for this adversarial terrain.

Earlier presentations (Session 0 and 0.1) showed how harassment networks weaponise hashtags, images, and partial context to target CSOs and journalists.

Strategic communication, therefore, means recognising that every public message exists within a contested space. Decisions around phrasing, visibility, tagging, and timing must factor in the possibility of misinterpretation, hostile response, or narrative hijacking.

In the Session 3 slides, the framing of “risk-aware communication flows” shows how organisations can build internal processes that guide message creation, approval, dissemination, and response protocols. This ensures that communication remains intentional even during charged or sensitive moments.

7.7. Communication as a resilience practice

This session positions strategic communication as a resilience tool. It shifts communication from being reactive and exposure-prone to being thoughtful and risk-informed. When organisations understand how digital ecosystems behave, they can plan messaging that maximises impact and minimises vulnerability. This involves aligning communication with advocacy goals, anticipating adversarial behaviour, adjusting timing, managing visibility, and preparing internally for possible backlash.

Ultimately, the session teaches that communication does not only tell stories, it also shapes risk. When done well, it strengthens advocacy by creating safe pathways through which organisations can engage with the public without exposing themselves or their communities to unnecessary harm.

7.8. Further reading and external resources

- Access Now – Guidance on navigating online threats and platform-driven risks https://www.accessnow.org/
- Tactical Tech – Influence operations and strategic communication research https://tacticaltech.org/projects/the-influence-industry/
- Oxford Internet Institute – Research on algorithmic amplification and content dynamics https://www.oii.ox.ac.uk/

- MIT Technology Review – Analysis on platform behaviour and disinformation flows https://www.technologyreview.com/
- Digital Forensic Research Lab – Monitoring influence operations and cross-platform narrative manipulation https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/

8. SESSION 4 — Responding to Harassment and Digital Attacks

[Presentation attached: Session 4]

8.1. Introduction

Online harassment and communication-driven attacks have become routine threats for civil society organisations working in politically sensitive environments. These attacks are not isolated or spontaneous; they follow clear escalation patterns, exploit platform dynamics, and deliberately target credibility, emotional stability, and operational continuity.

This Session helps trainees understand how to prepare for these threats before they happen, how to recognise the early signs of escalation, and how to coordinate internally to reduce harm. The goal is not to eliminate risk, that is impossible in adversarial digital spaces, but to manage it in a way that protects people, preserves organisational integrity, and ensures advocacy can continue even during periods of pressure.

8.2. Understanding escalation patterns

The Session 4 presentation opens by mapping the typical stages through which harassment campaigns evolve. The early visuals show how a single post or public statement can move within hours from organic engagement to politicised amplification, and then rapidly into coordinated harassment.

These stages are important because they demonstrate that harassment is rarely random. It usually begins with a trigger, a sensitive issue, a controversial claim, or a narrative challenge, and then spreads as actors mobilise their networks. By the time harassment becomes visible at scale, the attack is already well underway. Recognising these early indicators helps organisations intervene before escalation becomes overwhelming.

The presentation also highlights how digital platforms intensify harassment through algorithmic incentives. When content is polarising or emotionally charged, platforms push it further into public spaces, drawing in adversarial networks. This feedback loop means organisations must interpret harassment not merely as personal hostility but as a platform-enabled phenomenon that grows through structural incentives.

8.3. Anatomy of a digital attack

Several slides in the presentation illustrate the anatomy of a harassment campaign. The session shows how an initial wave of quote-tweets, hostile comments, and targeted tagging creates the first layer of pressure.

As engagement increases, the second layer usually emerges, which involves more coordinated behaviour such as synchronised messaging, repeated hashtags, and manipulated imagery. The third layer, displayed in later slides, shows attempts to shift the narrative entirely, reframing the target as illegitimate, immoral, or politically motivated.

These stages reveal why unprepared organisations often feel overwhelmed: harassment is not just abusive language, it is a deliberate attempt to control narrative space.

The presentations from Session 0.1 reinforce this through real examples of organised harassment in Pakistan, where manipulated visuals, repetitive posting, and targeted narratives are used to distort meaning and incite mobs. The documented volume of images and network coordination shows that these attacks function as influence operations rather than spontaneous reactions.

Understanding these tactics allows civil society organisations to design response strategies rooted in analysis rather than panic.

8.4. Psychological and organisational impact

Harassment is designed not only to punish but to silence. The slides emphasise how sustained attacks can lead to fear, emotional exhaustion, and self-censorship across teams. This psychological pressure is often the primary goal of adversarial actors: to make individuals retreat from public spaces and to force organisations to reduce their digital visibility. When staff members begin avoiding communication roles or when leadership becomes hesitant to speak, advocacy loses momentum. This makes internal preparedness as important as external response. Teams must be psychologically supported, decision-making must be clarified, and responsibilities must be distributed so that no one is isolated during crises.

8.5. Internal coordination and response planning

The attached presentation outlines that response planning must begin long before harassment occurs, and the concept of “internal coordination layers,” showing how responsibilities should be divided between communications teams, leadership, safety focal points, and support roles.

Preparedness requires organisations to define in advance who monitors platforms, who evaluates whether a response is necessary, who drafts statements, who supports affected staff, and who maintains communication with partners or media if the attack escalates. This prevents confusion during crises and ensures that no one person bears the emotional burden alone.

Strategic response does not always mean responding publicly. In many cases, silence, deprioritisation of the attack, or shifting communication to safer channels is more effective than engaging directly with hostile actors. The key is intentionality: organisations should respond only when the response contributes to strategic goals, not when adversaries attempt to provoke them into reactive visibility.

8.6. Managing visibility during harassment

Visibility must be reconsidered during harassment. When an attack escalates, certain narratives, posts, or individuals may need to be temporarily de-emphasised to avoid further targeting. This does not weaken advocacy; it strengthens resilience. Visibility can be reintroduced once the hostile wave

subsides and once the organisation has regained control over its narrative environment. The session encourages CSOs to treat visibility as a dial, not a switch, something to be managed and recalibrated depending on the level of risk.

8.7. Protecting organisational credibility

Harassment campaigns often aim to damage credibility by reframing motives, distorting messages, or associating the organisation with political agendas. The slides highlight how credibility can be protected through consistent messaging, pre-established values, and clarity about the organisation's advocacy goals.

Credibility also relies on not being drawn into hostile framing. When CSOs respond impulsively, their reactions can inadvertently validate the narratives that adversaries attempt to impose. Strategic communication and internal coordination ensure that responses reinforce credibility rather than undermine it.

8.8. Building long-term resilience

This Session ultimately reframes digital harassment as a recurring environment, not an exceptional crisis. Civil society organisations must develop long-term resilience by creating internal cultures of safety, conducting regular scenario planning, aligning communication strategies with risk awareness, and ensuring continuous staff support. Resilient organisations do not merely survive harassment; they adapt their operations so that harassment becomes less effective over time.

8.9. Further reading and external resources

- PEN America – Resources on online abuse, journalist safety, and strategies for resilience https://onlineharassmentfieldmanual.pen.org/
- Access Now – Digital Security Helpline and guidance for civil society facing coordinated attacks https://www.accessnow.org/help/
- WITNESS – Guidance on protecting identity and responding to manipulated visuals https://www.witness.org/resources/
- International Center for Not-for-Profit Law – Research on repression patterns and state pressure on CSOs https://www.icnl.org/
- UN Special Rapporteur on Human Rights Defenders, Reports on reprisals, intimidation and digital threats https://www.ohchr.org/en/special-procedures/sr-human-rights-defenders