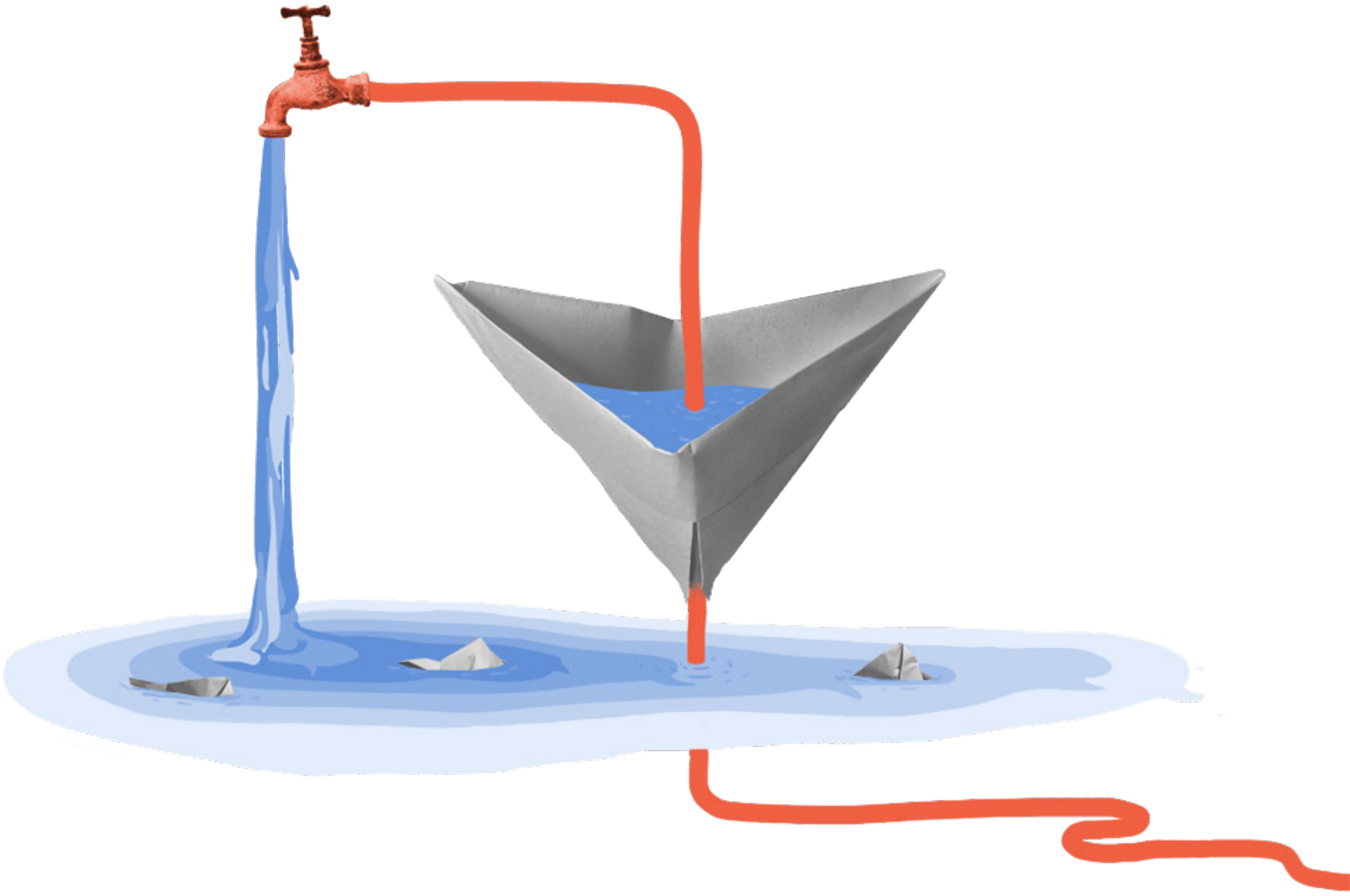


Malinformation: A Nuanced and Critical Concern for Civil Society

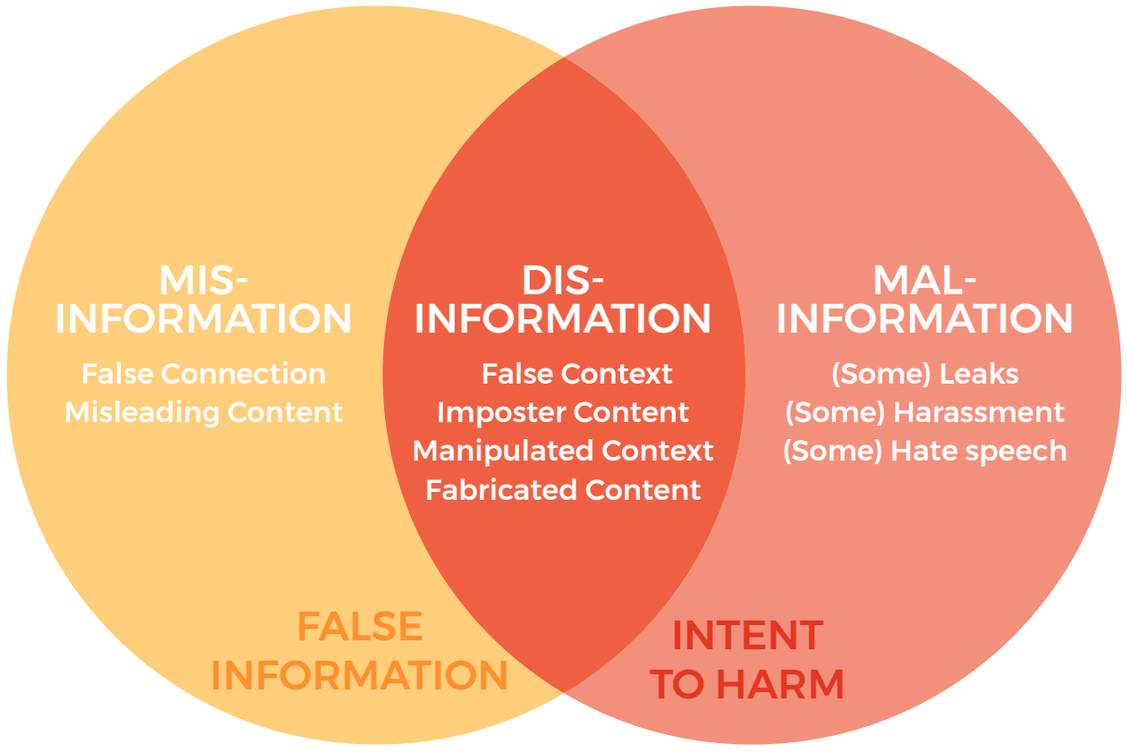
International
Civil Society Centre

Malinformation:
A Nuanced and Critical Concern for Civil Society

As our understanding of the threats digital technologies pose to civil society organisations (CSOs) continues to evolve, so too has the vocabulary with which we classify online harms. Modern CSOs are familiar with mis- and disinformation, and response toolkits and mitigation strategies for mis- and disinformation abound. Against this backdrop, experts are quickly acknowledging that malinformation, a relatively new term, constitutes a distinct information disorder. Malinformation is grounded in a frame of reference that is relevant to most CSOs – and may therefore appear familiar – but demands a unique set of considerations amidst the shrinking spaces CSOs navigate.

What is Malinformation?

Cornell University Communications Professor Clare Wardle and writer-researcher Hossein Derakhshan, who spent six years imprisoned in Iran for his writings an early web blogging, introduced the term 'malinformation' in 2017. Only in the past two years has the term begun to gain traction. A portmanteau of malware and information, malinformation is different from misinformation and disinformation in one key respect – its relationship to the truth. Wardle and Derakhshan write that malinformation is "Information that is based on reality, used to inflict harm on a person, organisation or country." In practice, malinformation is grounded in truth but exaggerated, stretched, or exposed in public to serve a particular agenda. As the non-profit Jewish Democracy describes, "For instance, the fact that a single polling location temporarily ran out of ballot paper might be used to argue for widespread election interference." While the underlying observation is true, it is twisted to promote a specific narrative.



A visual overview of Misinformation, Disinformation, and Malinformation from a report released by the Heinrich Böll Stiftung and originally adapted from a post by Prague-based journalist Temir Asanov.

To be sure, malinformation remains a contentious term. Because it is grounded in truth, assessments of whether a given piece of information is simply information or malinformation – designed to sow chaos, to generate revenue, or to wield influence – is open to interpretation. As one senior editor of a prominent libertarian magazine in the United States asserted, this judgment call is "in the eye of the beholder." In a related vein, a journalist suggested in Discourse Magazine that because malinformation risks labelling uncomfortable realities as misleading, it may be used to dismiss marginalised perspectives and dissent – precisely the speech many CSOs endeavour to protect.

Even when considering some of the most straightforward cases of malinformation, civil society organisations will recognise distinct risks and needs that fall outside the scope of misinformation and disinformation.

Case Studies:
Malinformation and the Weaponisation of Personal Data

Doxing

After the government proposed a law in February 2019 permitting extradition to mainland China, Taiwan, and Macau, the largest protests in the history of Hong Kong – some exceeding 2 million people – took place. In a series of investigations, it was found that the police used excessive force against its people, and the government outlawed face masks to prevent protestors from demonstrating anonymously.

In conjunction with this effort emerged well-resourced campaigns online to identify protestors. An investigation by the CitizenLab, a group at the University of Toronto that studies digital security and human rights, found evidence that these online doxing operations – HKLEAKS – to unmask protestors, journalists, and others were likely coordinated in partnership with the Chinese government and were specifically designed to avoid attribution. One report alleges that a prominent doxing site is still online – two years after authorities were alerted. The site contains data of over 2,000 individuals from Hong Kong, with their "ID card numbers, headshots, home addresses and phone numbers."

Similarly, the Southeast Asia Freedom of Expression Network (SAFEnet), a civil society organisation based in Indonesia, has observed a spate of doxing-related incidents in recent years. Noting that doxing can happen to anyone online, the organisation emphasises that "journalists and activists have a higher vulnerability." After one journalist published an article assessing the veracity of a politically charged claim related to Indonesia's sensitive history of Communism, several Instagram accounts shared links to his home address and family pictures, including photos of his baby. Rolando Fransiscus, a photojournalist, discovered that his personal ID and press card hard been disseminated on Facebook and Instagram while documenting a rally. Human Rights Watch has revealed widespread human rights abuses in the Indonesian province West Papua. Veronica Koman, a Papuan human rights defender, noticed that her address had been shared on Twitter, and the offending account claimed that she was under observation.

Case Studies:
Malinformation and the Weaponisation of Personal Data

Figure 3: Promotion of the HKLeaks website (active at that time) via the #被摘下面罩香港暴徒名单# hashtag on Weibo in a post made by the official Weibo account for the People's Court of Shizhu Tujia Autonomous County, Chongqing, China, on September 21, 2019. Translation: "Share! Take note and recognize these faces! #listofHKriotersunmasked Lately, some internet friends have produced a website called HK Leaks, in it there is a list of various rioters and HK "separatists". The website is organized in three categories: "Poisonous fruit reporters" [a reference to Apple Daily reporters], *Hong Kong independence rioters, and those who want to see HK in chaos. They are all organized and sorted by family name, so it is convenient for all of you to see their evil faces. Take off their mask! Let's take action together! Share!".*

An image from"HKLEAKS Doxxing Explained: Role of Online Harassment Tactics to Repress 2019 Hong Kong Protests," a report published by CitizenLab in July 2023

Doxing, an act in which private information is made public with malicious intent, is a prime example of malinformation and a challenge with which many CSOs are well-acquainted. The published information is true, and it is therefore neither misinformation nor disinformation. However, in the cases above, the personal information of protestors was compiled and released to advance the political goals of the Chinese government, and the personal data of journalists and human rights defenders was shared presumably to serve the interests of those attempting to intimidate them.

Case Studies:
Malinformation and the Weaponisation of Personal Data

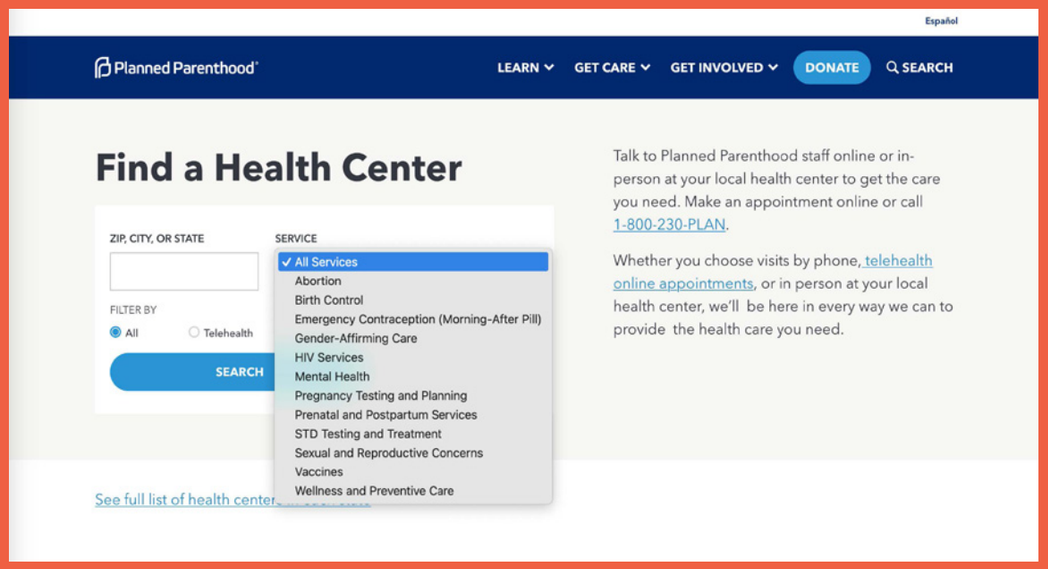
Calculated Misrepresentation and Potential Endangerment

Civil society organisations, especially when critical of their home governments, risk being targeted and misrepresented as serving special interests. In May 2018, The Open Societies Foundations (OSF), the philanthropic organisation and international NGO funded by George Soros, announced its decision to leave Hungary and relocate to Germany because of pressure from the government. The year prior, as one example, a government spokesperson claimed that Soros wanted to "settle hundreds of thousands of illegal immigrants in Europe and Hungary." While OSF actively champions refugee rights and asylum assistance – presumably including the relocation of some number of refugees to Europe – the remarks of the spokesperson are based in truth yet partisan, ideologically driven, and seemingly exaggerated. As a statement from OSF released at the time noted, "The Foundations are taking appropriate steps regarding the safety and well-being of those affected by the office relocation." One month before the Foundations announced the move, a pro-government publication released a list of 200 names believed to be "mercenaries" of George Soros.

Case Studies:
Malinformation and the Weaponisation of Personal Data

Leaked Private Data

In August 2024, Planned Parenthood of Montana – a reproductive services organisation in the United States operating amidst a political crackdown on abortion rights – suffered from a cyber incident in which attackers claim to have stolen 93 GB worth of data, which they threatened to release. As of this writing, no patient data has been exposed from this breach, but the organisation has become a prime target in recent years. In October 2021, a hacker gained access to the names of 400,000 Planned Parenthood patients in Los Angeles, and in 2015, a hacking group claiming to be "social justice warriors" published the names of 300 Planned Parenthood employees from across the United States on a private website. As before, these exposures are not based on false information. Though the information contained within them is presumably true, they present a liability and an obstacle for CSOs. For instance, these Planned Parenthood disclosures complicate the work of reproductive rights groups in ensuring that women in their communities can access the medical care they require.

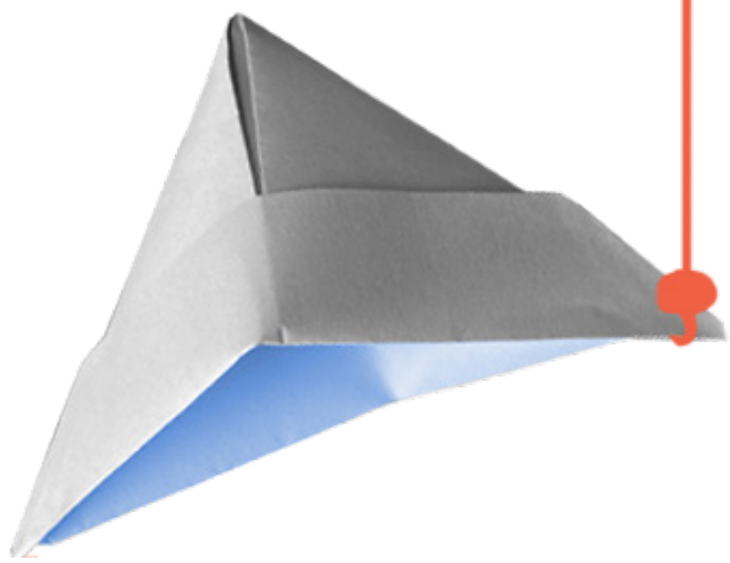


This image of a Planned Parenthood website shows a range of politicised medical services provided.

The Stakes for Civil Society Organisations

Beyond the cases presented above, malinformation presents CSOs with other threats involving unauthorised personal data disclosures, which can exact heavy psychological tolls on their targets partly because the disclosed information is based in truth. Amnesty International reports that 60% of human rights defenders aged between 13 and 24 across nearly 60 countries suffered from harassment in response to their activism. The analysis cites harassment in the form of trolling and hostile direct messages among the biggest culprits. Forty percent of the the four hundred respondents expressed that they “felt a sense of powerlessness and nervousness” as a result of the treatment they encountered. In fact, the problem is so acute that the young activists rank services to promote wellbeing ahead of improved reporting practices and legal assistance.

In addition to doxing, misrepresentation, leaked data, and harassment, related threats and sources of malinformation include forced outing, adversarial governments scrutinising the credibility of CSOs because they are not elected, funded by foreign entities and therefore allegedly serving foreign / special interests, and self-interested because their representatives earn fair salaries and occasionally travel internationally. Leaks of donor lists also present a special concern that warrants extra care as CSOs navigate increasingly surveilled digital spaces. Careless handling of malinformation could erode an organisation’s reputation as a result of distorted facts, invite harassment through leaks of personal data belonging to staff and stakeholders, exacerbate existing safety threats within an organisation, divert precious funds away from key priorities and toward reputational management, and ultimately jeopardise the trust of the public.



How CSOs Can Prepare and Respond to Malinformation

As with many challenges, prevention can preempt many downstream crises. First, unlike some efforts to respond to mis- and disinformation, labelling malinformation as such appears to be counterproductive, particularly because it is so open to interpretation.

Instead, in response to threats from hostile governments that CSOs are unelected and therefore uncommitted, organisations must "continuously work on demonstrating that they are rooted in the population" and highlight their impact through testimonials.

POTENTIAL MAINFORMATION	POSSIBLE SOLUTION
CSO legitimacy is challenged since CSO representatives are unelected	CSOs should "continuously work on demonstrating that they are rooted in the population" and highlight their impact through testimonials.
CSOs are accused of serving foreign agents or special interests because of international donors	CSOs can disclose funding sources and transparently explain the terms associatedwith grants. Releasing independent, thirdparty audits of the organisation is also encouraged. Organisations can also diversify their funding sources.
CSOs may be attacked for being selfserving because its employees are fairly paid and travel	CSOs ought to publish information regarding how funds are disbursed, spent, and disclosure partnerships when possible.
Adversarial governments claim that CSOs aid opposition parties	CSOs must invest in the political literacy of the population being served, foster relationships with independent media, and build alliances with likeminded organisations.
CSO staff members and stakeholders become victims of doxing, blatant misrepresentation, or private data disclosures	CSOs can prioritise investments in digital security and privacy.

This table previews some forms of malinformation with which CSOs may have to contend. Several of these recommendations are adapted from Leila Turčilo and Mladen Obrenovič in report released by the Heinrich Böll Stiftung.

How CSOs Can Prepare and Respond to Malinformation

Transparency regarding funding sources and spending can preempt allegations of serving special interests and of skepticism regarding employees' salaries and commitments. To limit the possibility of sensitive personal data being leaked, CSOs ought to prioritise basic digital hygiene and security practices. Some related suggestions are referenced below, and further digital security resources are available here.

- Reduce digital footprints through digital security training for staff.
- Enable automatic updates to digital services
- Communicate over end-to-end encrypted channels (e.g., Signal)
- Enable two-factor authentication where possible
- Use a password manager
- Keep highly sensitive conversations in-person when possible
- Communicate to staff how personal and professional online threats are connected. All stakeholders should be mindful about what information they share online and how.
- Share sector-specific trends
- Develop information management protocols
- Backup important data securely
- Auto-delete data regularly
- Implement access control measures (so only authorised individuals can access resources relevant to them)

In the event in which a CSO becomes a victim of malinformation, a crisis management team – comprised of legal counsel, data security experts, and communications professionals – can help weather the storm. Of course, legal recourse can be expensive and time-consuming, particularly when few jurisdictions designate protections specific to disclosures like doxing. Still, other legal mechanisms including defamation, invasion of privacy, electronic communications protections, or injunctive relief may provide additional legal cover.

Without engaging directly with the malinformation with which the organisation has been targeted, the most resilient defence against malinformation is simply acknowledging the distinct threat malinformation poses and showcasing the organisation's commitment to its unwavering mission and its proven track record in an effort to correct the record. By pairing this commitment to practices designed to mitigate mis-/disinformation, civil society organisations will be best equipped to continue their work unhampered by modern information disorders.

Written by Varoon Bashyakarla
Illustrations Karen Eckert

International Civil Society Centre