**Digital
Defenders
Partnership**

Digital Defenders Partnership 2024–2027 Strategic Plan

Towards centring feminism
and decoloniality

From gender equity and diversity inclusion towards centring feminism and decoloniality

Digital Defenders Partnership (DDP) is an international programme that contributes to strengthening the resilience of human rights defenders by increasing their digital security through a holistic and sustainable approach. DDP's 2024-2027 Strategic Plan is shaped by its commitment to centre feminist and decolonial practices across all of its work through a holistic approach that goes beyond recognising and addressing surface-level issues to delve into the systemic injustices that threaten the digital safety of human rights defenders.

→ **"Taking a bold approach and commitment towards grounding feminist and decolonial practices and principles across the digital security space is the next step needed to advance efforts aimed at dismantling systemic injustices at their root, instead of the perpetual cycles of unsustainable short-term solutions."**

- DDP Partner

→ **"Contexts are so diverse and needs are constantly shifting. This is what makes listening to those at the forefront of war and efforts to defend human rights so important. This is what makes Digital Defenders Partnerships so unique, it listens and acts as an ally and partner."**

- DDP Partner

→ **"Digital security is intersectional. By this, I mean that the digital does not live in an abstract and siloed space. My physical, mental, and emotional well-being are intimately intertwined with the digital paradigms. Therefore, digital security must be supported through a holistic approach in order to be truly considered effective in seeking to strengthen our individual and collective digital security."**

- DDP Partner

Gratitude

DDP's 2024-2027 Strategic Plan was developed through a participatory and community-centric process that brought together the insight, reflections, and recommendations of DDP's team, partners, donors, and human rights defenders across the ecosystem. As DDP surpasses a decade since its establishment, these valuable contributions assume a key role in shaping the programme's trajectory, propelling it towards a transformative phase that seeks to centre feminism and decoloniality across all aspects of its work.

DDP acknowledges that technology and digital spaces have been used as tools of colonialism and white supremacy, perpetuating and deepening political, economic, and social domination. This has resulted in sharp increases in inequality, the expansion of state-corporate surveillance, the development of sophisticated artificial intelligence systems that further racism, repression, and censorship, as well as the deployment of police and military technologies that further oppression, to name just a few.

DDP is committed to working towards feminist and decolonial realities that seek to dismantle and transform these unjust tools, practices, structures and systems. Thus, it is critical for us to name that the language and narratives that have been used within the digital and technology space, including those across human rights spaces, are deeply entrenched in these very same systemic injustices and caused harm. Framings such as "free internet," "digital security," and "protection," among others, have historical roots that must be critically examined and reframed through a grounding in decoloniality and feminism.

We are committed to doing this work and have included our collective definitions that describe our framing and approach in our Shared Language.[1] We acknowledge there is no one-size-fits-all approach and firmly believe in engaging in ongoing dialogue to understand the diverse framings and language used by individuals, communities, and groups while acknowledging this to be a continual effort.

---
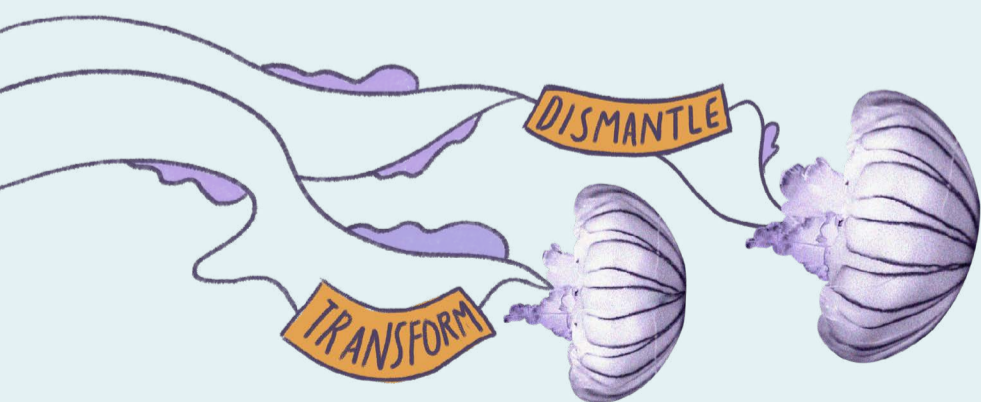
1   Shared Language: DDP developed a shared language glossary as a complementary component to its 2024-2027 Strategic Plan. For further details, refer to Appendix B.

Content

Executive Summary

Digital Defenders Partnership (DDP) is an international programme that contributes to strengthening the resilience of human rights defenders (HRDs) by increasing their digital security through a holistic and sustainable approach. Established in 2012 by the Freedom Online Coalition (FOC), DDP initially focused on supporting efforts to promote an open internet free from emerging threats. Originally conceived as a regranting mechanism primarily for urgent support to HRDs experiencing digital attacks, threats, or emergencies, DDP's programme has since evolved to better align with the specific needs and contexts of HRDs.

To date, DDP has positioned itself as a strong partner and ally supporting, through a holistic approach, the digital security of HRDs facing risks and threats. Since its inception, DDP has provided support to over 400 HRDs, encompassing both organisations and individuals, through funding and accompaniment. In 2013, DDP launched the Global Rapid Response Network (RareNet) to increase cooperation between responders and, the following year, co-developed the Digital First Aid Kit to support HRDs handle common digital security attacks. DDP is also an active member of CiviCERT, among other key digital security networks and communities. Additionally, DDP has played a crucial role in referring HRDs encountering digital threats to essential resources and responders and facilitates a global community of feminist helplines to provide support to women and LGTBQIA+ people facing gender-based violence online.

At the beginning of 2023, the DDP team launched the process to develop its 2023-2027 Strategic Plan, involving a core team and partnering with Sukuamis, a feminist collective focused on strengthening and supporting organisations, social movements, and political actors. This process was highly participatory and community-centric, incorporating the perspectives, recommendations, and experiences of DDP team members, partners, donors, and HRDs across the ecosystem.
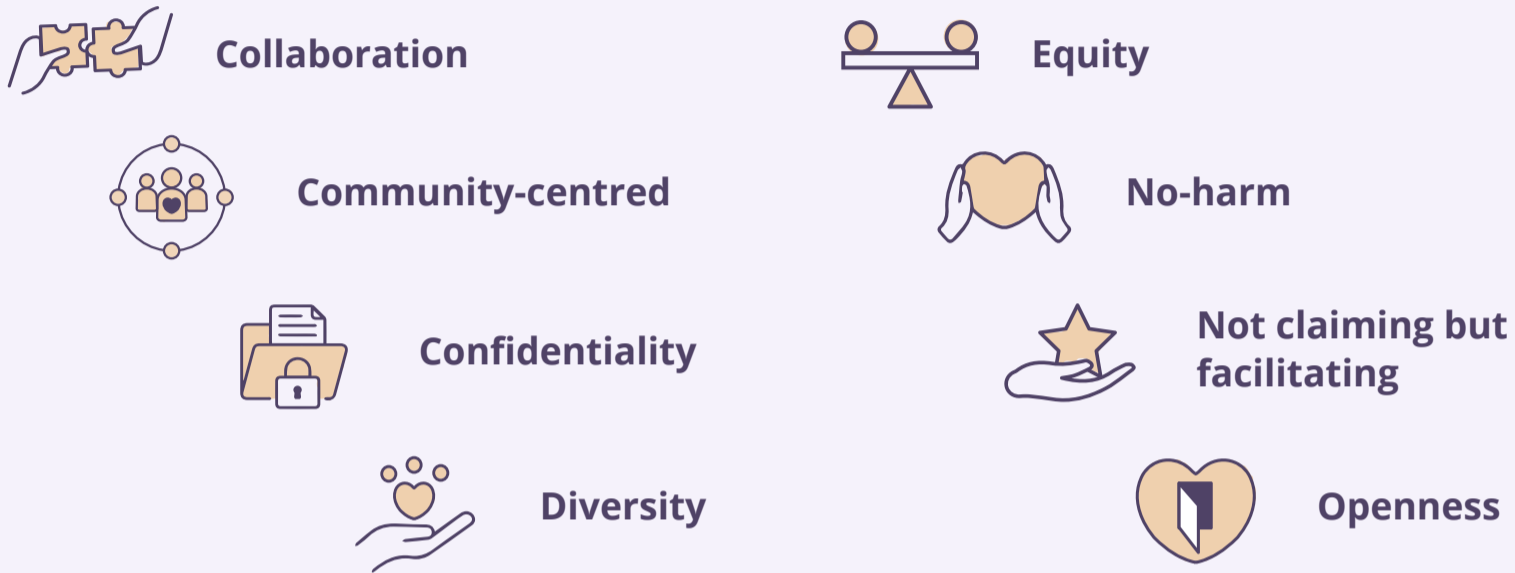
DDP's 2024-2027 Strategic Plan is shaped by its commitment to centre feminist and decolonial practices across all of its work through a holistic approach that goes beyond recognising and addressing surface-level issues to delve into the systemic injustices that threaten the digital security of HRDs. The strategy begins with a refreshed vision, mission, and guiding principles that steer DDP's endeavours and trajectory during this phase of its work.

Vision: envisions a world in which HRDs contribute to social justice while enjoying safety, well-being, freedom, and dignity.

Mission: DDP is an international programme that contributes to strengthening the resilience of HRDs by increasing their digital security through a holistic and sustainable approach.

Guiding principles:

Collaboration

Equity

Community-centred

No-harm

Confidentiality

Not claiming but facilitating

Diversity

Openness

To fulfil its mission, DDP supports HRDs working across movements and issues such as democracy, digital rights, disability justice, environmental and climate justice, feminism, freedom of expression, LGBTQIA+ rights, reproductive justice, and beyond. Aligned with our regionalisation approach that is grounded in the firm belief and understanding of local knowledge and expertise, each regional team identifies its priority populations based on the prevailing context.

Within the Journey of Change[2] of the 2024-2027 Strategic Plan, DDP's general objective is to contribute to strengthening HRDs' resilience by increasing their digital security from a holistic and sustainable approach.

This objective is pursued through four core Strategic Objectives, each supported by corresponding strategies, which will collectively guide DDP's efforts over the coming years.

Strategic objective 1: Increase flexible and relevant resources for holistic digital security for HRDs at risk (mitigate).

Strategic objective 2: Strengthen and support HRDs' digital security knowledge, capabilities, and practices through a holistic approach (prevent).

Strategic objective 3: Support the strengthening of digital security knowledge, capacities, and practices within networks and communities at the local, regional, and global levels.

Strategic objective 4: Strengthen DDP's infrastructure, resilience and sustainability.

DDP employs the term Human Rights Defenders, but fully acknowledges that people may identify and understand this term in various ways. We aim to respect and honour these diverse identities and interpretations. When DDP utilises the term Human Rights Defenders, we are referring to "person(s) who, individually or with others, acts to promote or protect human rights". This includes activists, artists, journalists, lawyers, rapid responders, trainers, and actors who make information available to the public, especially those working collectively as part of a group, informal collective, organisation or network.

---

2   A Journey of Change is a framework that guides an organisation's efforts towards social justice by embracing an approach that acknowledges the inherently dynamic and non-linear nature of social change. It emphasises the imperative for adaptability, flexibility, and ongoing evolution in the pursuit of social justice.

Our story

Who We Are

DDP is an international programme[3] that contributes to strengthening the resilience of HRDs by increasing their digital security through a holistic and sustainable approach. With a diverse team across the world, DDP's strength lies in its holistic and community-centric approach that places HRDs at the very core of its mission and prioritises the expertise and lived experience of those closest to the context and realities.

DDP envisions a world in which HRDs not only contribute to social justice but also enjoy safety, well-being, freedom, and dignity. Its guiding principles include:[4]

- Collaboration
- Community-centred
- Confidentiality
- Diversity
- Equity
- No-harm
- Not claiming but facilitating
- Openness

With a commitment toward centring feminism and decoloniality, DDP approaches all of its work through a holistic approach that not only seeks to address surface-level issues but delves into the structural and systemic injustices that threaten the digital security of HRDs.

---

3   International programme: A global initiative within an organisation. DDP is an international programme hosted at Hivos. Centring a decolonial approach, DDP operates within a framework that prioritises the experience, knowledge, and autonomy of each region. We understand that those connected to the context, with the lived experiences, are best positioned to guide decision-making and contextually relevant strategies.

4   The definitions of the guiding principles can be found in Appendix B: Shared Language.

Where We Came From

DDP was established by the end of 2012, during the [second Freedom Online Conference in Kenya](#), by the Freedom Online Coalition (FOC) with the primary mission of providing rapid response to threats to internet freedom. At its inception, DDP concentrated on supporting efforts that focused on promoting an open internet that was free from emerging threats. The founding members of DDP comprised the governments of the Netherlands, the United States, the United Kingdom, and the Republic of Estonia.

Originally conceived as a regranting mechanism primarily focused on providing urgent support to HRDs experiencing digital attacks, threats, or emergencies, DDP's programme has since evolved to better align with the specific needs and contexts of HRDs. Lessons drawn from the program's initial implementation underscored that merely offering funding was insufficient for an effective response in supporting the digital security of HRDs.

Consequently, DDP's support has expanded to encompass a more comprehensive approach to address digital threats against HRDs. This approach now includes not only funding but also accompaniment and community building. The objective behind this holistic digital security approach, which was solidified in the last strategic plan (2020-2023), is to extend the programme's reach and to establish a more sustainable and systemic response to the equally systemic threats faced by HRDs within their contexts.

DDP's budget has experienced significant growth, increasing from 1.4 million in 2013 to 3.8 million in 2022. Additionally, the staff size has expanded from three team members primarily based in the Netherlands in 2013 to forty-four team members spread across five regions in 2023. DDP is hosted as an international programme at Hivos[5] and currently receives support from the Ministries of Foreign Affairs of Australia, Canada, Czech Republic, Denmark, Estonia, Finland, Germany, Latvia, the Netherlands, and the United Kingdom; along with the Swedish International Development Agency (SIDA) and the United States Department of State, all of whom are FOC members.
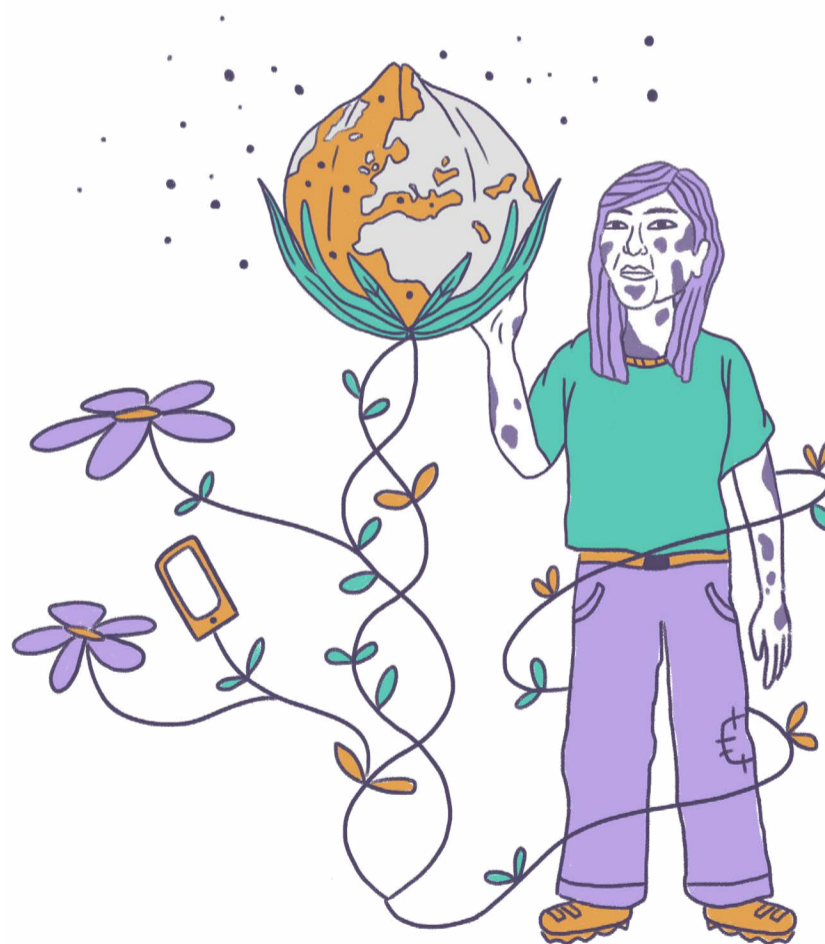
Where we are

DDP's 2020-2023 Strategic Plan objective was for HRDs in repressive and transitional environments to access improved capacities and networks so they can continue their work despite digital threats. The following strategic goals contributed toward the main objective:

Provide timely, flexible, and holistic emergency response resources to reduce the impact or risk of digital attacks against HRDs.

Strengthen awareness and capacities for sustainable and effective response to digital threats among HRDs at risk.

Develop and maintain accessible, collaborative, resilient, and responsive networks of expertise and support for HRDs under digital threats.

As a component of the 2020-2023 Strategic Plan, DDP developed a strategy to adopt and strengthen a structured approach to Gender Equality and Diversity and Inclusion (GEDI). This approach aligns with the requirements of HRDs, DDP's collaborators, partner organisations supporting HRDs, and DDP's internal operational framework.

Through the mentioned implementation period, DDP's main areas of work included: **Incident Emergency Response for providing flexible and holistic emergency support; Sustainable Protection Support for capacity building and increasing awareness; and Facilitation and Community Building for developing networks to support HRDs.** Within this period and aligned with the objectives within the GEDI strategy, DDP bore witness to significant growth, decentralisation and diversification of the team, which is more embedded than ever in the communities with whom it seeks to work with and for.

Through desk research of mid-term evaluations, as well as surveys and interviews with partners, donors and independent experts across the ecosystem, DDP was identified as a strategic and valuable partner that supported the digital security of HRDs through a holistic approach.

For many HRDs, DDP was among the only funders in the digital security space that they trusted and felt was a partner and ally rather than solely a funder.

"Most funders want more than they give, and this places us at higher risk. Think about being in a context where you are being surveilled and face serious threats. Trust and time are the most important. This is why DDP is so valuable to us. When we work with DDP we know we do not have to waste time convincing them of our work or explaining the context, they understand, respond to our needs, and ask us: 'how else can we support?.' This makes all the difference"

- DDP Partner

Additionally, DDP's accompaniment has been recognised as a vital cornerstone of its approach. DDP's partners have characterised it as fundamental support for strengthening their digital security, attaining greater autonomy and control, and increasing their awareness of the risks they face, along with the tools and practices available to mitigate them.

"After receiving the support, we realised how vulnerable we were in terms of safety in general and how we needed to start thinking about a strategy to deal with threats."

- DDP Partner

Amidst the COVID-19 pandemic, where HRDs faced heightened risks and threats, DDP's overall strategic plan and approach showed a high ability to adjust to the prevailing situation to support HRDs' digital security. One of DDP's partners succinctly described the impact: "DDP's support during the pandemic is essential. At the onset of the pandemic, we had many insecurities about how we were going to operate institutionally. We needed to structure a virtual office. Without [DDP], we would have done something else in an insecure way. In the midst of the uncertainty, we had the firmness of the facilitator's construction. Now, we have a secure virtual office that everyone uses to work, which allows us to continue our actions and collective work."
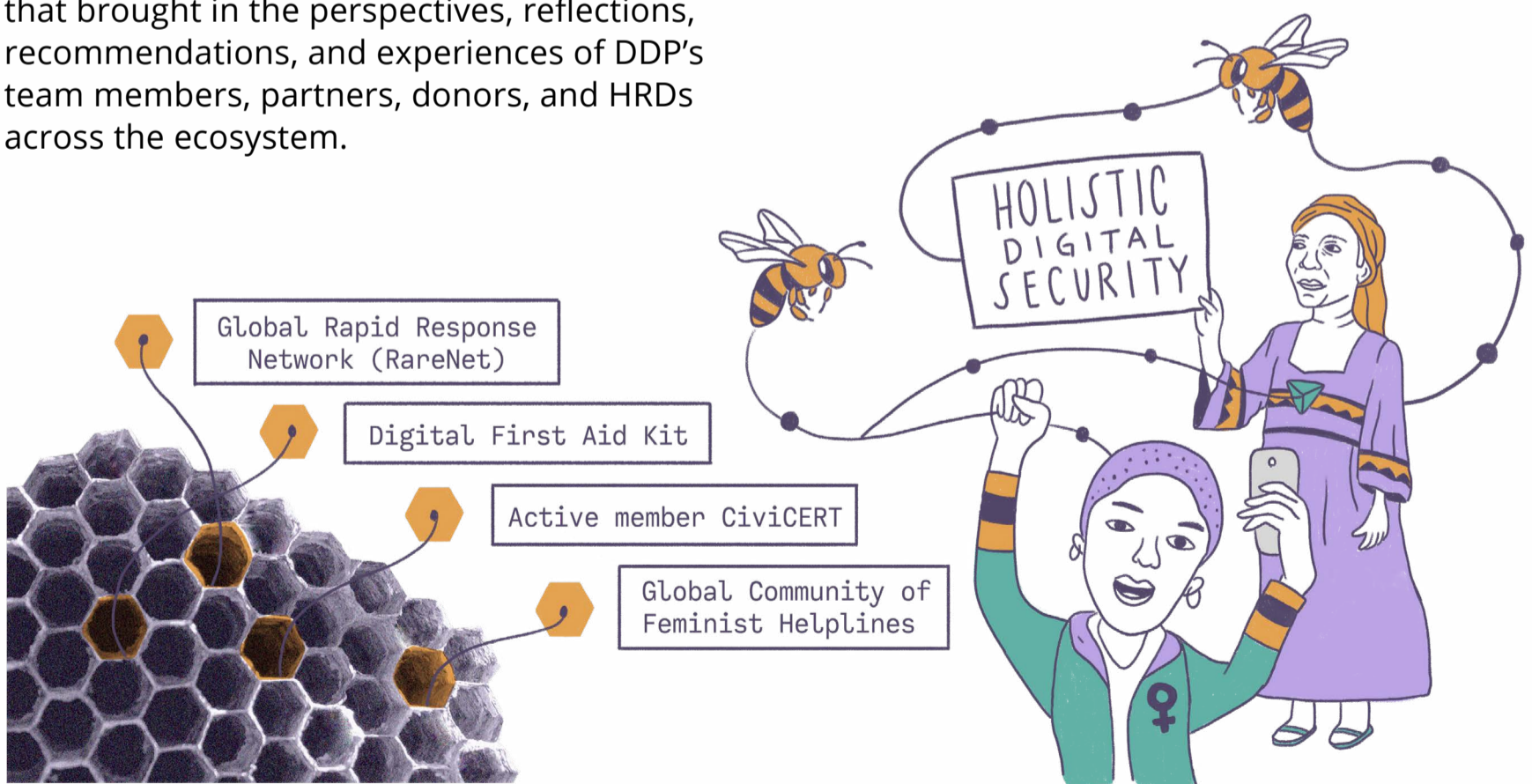
To date, DDP has positioned itself as a strong partner and ally supporting, through a holistic approach, the digital security of HRDs facing risks and threats. Since its inception, DDP has provided support to over 400 HRDs, encompassing both organisations and individuals, through funding and accompaniment. In 2013, DDP launched the Global Rapid Response Network (RareNet) to increase cooperation between responders and, the following year, co-developed the Digital First Aid Kit to support HRDs in handling common digital security attacks. DDP is an active member of CiviCERT, among other key digital security networks. Additionally, DDP has played a crucial role in referring HRDs encountering digital threats to essential resources and responders and facilitates a global community of feminist helplines to provide support to women and LGBTQIA+ people facing gender-based violence online.

Developing the 2024–2027 Strategic Plan

At the beginning of 2023, the DDP team launched the process to develop its 2024-2027 Strategic Plan. This included bringing together a core team to facilitate the process along with the accompaniment of Sukuamis, a feminist collective of activists working to strengthen and accompany the sustainability of organisations, social movements and political actors. The Strategic Plan process was led through a participatory and community-centric process that brought in the perspectives, reflections, recommendations, and experiences of DDP's team members, partners, donors, and HRDs across the ecosystem.

Sukuamis' approach was rooted in feminist, decolonial, collective wisdom, non-extractive, and collective care principles, with a strong emphasis on anti-ableist and creative values. The process employed a mixed-method approach, utilising diverse and complementary methodologies that prioritised open reflection, discussions, and allowed for constructive feedback and recommendations.

Global Rapid Response Network (RareNet)

Digital First Aid Kit

Active member CiviCERT

Global Community of Feminist Helplines

HOLISTIC DIGITAL SECURITY

This process, conducted from February to September, encompassed the following methods:

Document analysis: This involved a thorough review of programme documentation, including previous strategic plans, annual planning notes, mid-term evaluations, reports, policies, and related documentation.

Interviews: A total of thirty interviews were conducted, involving DDP team members, partners, donors, and HRDs across the ecosystem.

Surveys: Four surveys were conducted, resulting in 40 responses from DDP team members, partners, and HRDs across the ecosystem.
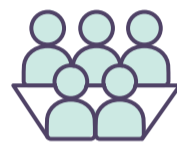
Group sessions: Twelve group discussions, reflection sessions, and analysis sessions were held with DDP team members.

In-person workshops: Two workshops were facilitated, one with the Latin American DDP team and another with a group of donors.
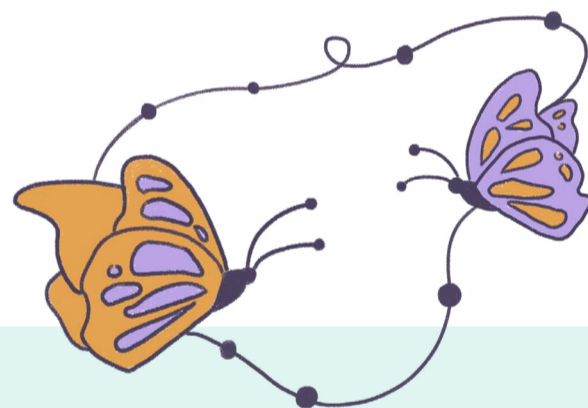
Throughout the co-creation of DDP's Strategic Plan, the DDP team played a pivotal role in offering essential guidance, reviewing, and validating each component. As part of this process, DDP collaboratively developed a Shared Language glossary, which serves as a complementary element to its 2024-2027 Strategic Plan. This Shared Language document provides collective definitions for key terms to create a clear understanding of the terminology and approach. This living document will undergo updates over time to reflect DDP's ongoing learning and evolution. **For reference, please see Appendix B to review the document.**

In the formulation of the Strategic Plan, DDP had a clear focus on implementing the lessons gained from the 2020-2023 Strategic Period. This required attention to look within to strengthen its internal capacity in response to its rapid growth during that period. The overarching goal was to deepen its efforts across all facets of its work and take a step forward by moving from gender equity and diversity inclusion, towards centring feminism and decoloniality across its strategy and work.

Current Context

Realities

HRDs are the bedrock of civic space, at the forefront of response to conflicts and humanitarian crises. HRDs meet the urgent needs of the present while pushing forward to dismantle systemic injustices to bring about transformational change, all while facing severe challenges, risks, and threats with little to no support, both in terms of access to vital resources and funding, with less than [1% of funds across the global human rights space reaching HRDs.](#)

The past few years alone have borne witness to a multitude of conflicts and crises that continue to exacerbate and compound existing injustices: the continuous devastating impact of the COVID-19 pandemic, which has strained healthcare systems and aggravated social inequalities by pushing millions of people to extreme poverty while "billionaires' wealth soared 70%"; the mounting threats and risks caused by climate change and the rise of climate refugees, MAPAs (Most Affected People and Areas) and the criminalisation of environmental justice activists, land defenders and indigenous communities; wars and armed conflicts that persist across the world, such as Israel and Palestine, Russia and Ukraine, Myanmar, Syria, Congo, Sudan, or Yemen, which are leading to humanitarian crisis and rights human violations; and escalating threats and violence against HRDs who are facing violence, harassment, and surveillance by governments, non-state actors, and extremist groups.

We are also in the midst of an unprecedented refugee and migratory crisis. According to UNHCR, by September 2023, over 114 million people – including refugees, internally displaced people, asylum-seekers and migrants – were forcibly displaced due to war, persecution, conflict, violence, human rights violations and humanitarian situations. Citizens from countries like Afghanistan, the Democratic Republic of Congo, the Central African Republic, El Salvador, Eritrea, Honduras, Mexico, Myanmar, Palestine, Somalia, Sudan, South Sudan, Syria, Ukraine, and Venezuela, to name some, were expelled to migration corridors that pose life-threatening conditions, even more so for women and girls who, in addition, suffer sexual violence.

Furthermore, governments across the world have been enacting oppressive laws aimed at cracking down on civic space and undermining the vital work of HRDs. These laws are designed to surveil, control, and punish those who advocate for human rights and social justice. The latest of these repressive laws was passed in Jordan in August, further restricting free expression, limiting access to information, and increasing censorship.

"States employ digital censorship, persecution, and surveillance to instil fear and silence us. This invisible yet profoundly felt force undermines our movements and endeavours, instilling fear for our safety. It not only targets our work but also takes a toll on our mental well-being, sowing doubt in our ability to trust one another. Ultimately, it aims to dismantle civil society, seeking to silence our voices."

- Human Rights Defender.

The deployment of cyber laws has increasingly become a favoured tool for repressive regimes to stifle civil society and undermine the essential work of HRDs. This concerning trend extends beyond Jordan, as countries like Cameroon, El Salvador, Indonesia, Israel, Libya, Malaysia, Malawi, Nicaragua, Russia, Syria, and Zimbabwe have also passed cyber laws. Such laws, while claiming to regulate online harassment, fake news, hate speech, and defamation, are being used to surveil, control, persecute dissent and curtail freedom of expression.

This restrictive regulatory trend takes place within the broader scenario of a highly concentrated and privatised technological sector, even more dominant since the COVID-19 pandemic when lockdown forced the digitalisation of most human activities.

A handful of Big Tech companies control global communications infrastructure, from internet backbone and other critical hardware to software, social media platforms and newer developments such as generative AI.

The current hegemonic technological development model, conceived in the centres of power, is only possible through neo-colonial practices such as the extraction of natural resources, the violation of labour rights, epistemological domination, anti-competitive practices, and lobbying to stop or shape regulation. All this at a high ecological cost due to increased energy and water consumption to keep data centres running, and an accelerated device consumption cycle.
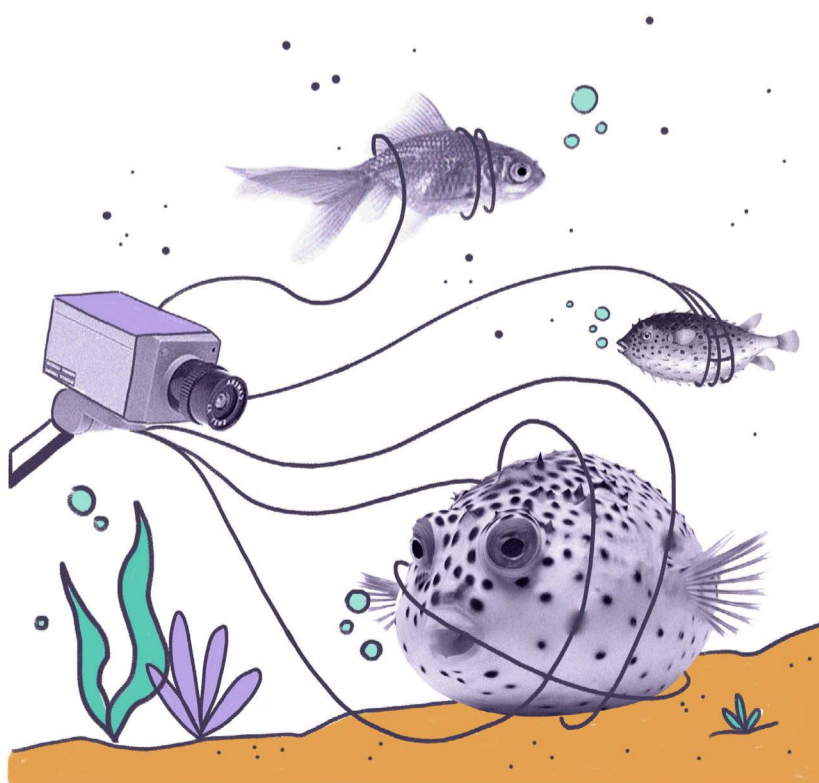
Moreover, Big Tech's algorithmic social media platforms and their monetisation schemes undermine democratic discussion, foster the dissemination of dis- and misinformation, reward the dissemination of hate speech and political violence, favour and endorse gender-based violence online, lead to behavioural disorders in children and adolescents, threaten privacy and facilitate tracking and surveillance.

HRDs, specifically, grapple with an escalating array of threats across physical, digital, and socio-emotional dimensions. Front Line Defenders 2022 Global Analysis and the European Union Agency for Fundamental Rights have documented 400 confirmed cases of HRDs who have been killed, underscoring the gravity of the dangers they face. Additionally, the United Nations has reported a rise in surveillance, control, and oppression, fuelled by tools like the Pegasus spyware developed by an Israeli cyber-arms company.

→ **"Most, if not all, of our work occurs at the intersection of physical and digital realms. In today's world, this is the reality. The digital security of our activism is paramount, as these dimensions are interdependent. Should we become targets of digital threats, our physical safety is consequently compromised."**

- Human Rights Defender

In the midst of this precarious context, the lack of funding for HRDs poses additional risks to their safety and security. With limited resources, they often struggle to implement adequate security measures, leaving them vulnerable to threats, harassment, and violence. This funding deficit also contributes to the erosion of civil society space, impeding their capacity to engage in critical social justice work. As a result, repressive governments and non-state actors can operate with greater impunity, perpetuating human rights abuses unchecked.

→ **"Funders must grasp the interconnected nature of all elements within the system, acknowledging that threats and risks to HRDs are not standalone issues but are intricately linked with broader injustices. Funding should adopt an approach that takes into account our comprehensive needs, remains adaptable, and acknowledges our unique insight into the challenges we confront. Your role should be to use your influence to secure additional resources and support for human rights work. Rather than expecting us to navigate bureaucratic hurdles while our lives are at risk."**

- Human Rights Defender

The realities confronted by women, Indigenous people, individuals with disabilities, and Black and LGBTQIA+ communities who engage in human rights defence are characterised by uniquely daunting challenges, pervasive discrimination, and structural injustices. These HRDs operate within a complex web of intersecting threats and risks that are inextricably linked to the broader systemic injustices they strive to address. As described in DDP's 2020 Annual Report, the groups most severely affected by violent attacks and killings include environmental, land, and Indigenous rights defenders, anti-corruption activists and women's rights defenders.
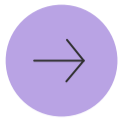
"I have taken a leading role in documenting State abuses, which is why I am subjected to surveillance and continual threats. As an Indigenous woman and feminist activist, I am acutely aware that my life is at risk every time I speak out. In this challenging journey, I have three guns pointing at me: the patriarchy, the coloniser, and the State. Yet, I know I must continue my work."

- Human Rights Defender

During the reflection and insight-gathering phase of the strategic planning process, HRDs shared the primary digital threats they encountered. While numerous threats were context-specific, six prominent threats emerged consistently across all responses. These include digital surveillance, phishing, account intrusion and control, internet blackouts, doxxing, and online violence and hate speech.

Human Rights Defenders' Needs to Improve their Digital Security

Through conversations and discussions with HRDs across the world, who are engaged in a wide array of efforts and work at the intersection of various movements, we have compiled a synthesised list of key needs that they have highlighted to support their digital security and efforts.[6]

Systemic change: Focus on systemic change rather than project-focused or isolated approaches. They stressed the importance of addressing the root causes of issues to create lasting impact. This entails recognising that digital threats and risks are often symptomatic of deeper structural problems.

Centre HRDs: It is crucial to centre the voices, ideas, and leadership of HRDs in all efforts related to their digital security. This means acknowledging their expertise and experiences in navigating the challenges they face. By actively involving HRDs in decision-making processes and resource allocation, organisations and funders can ensure that their support is responsive and relevant to their unique needs and perspectives.

---

6   These key needs have been listed in the cumulative order in which they were named by the HRDs who contributed to this process.

Holistic digital security: Recognise the interconnected nature of the digital realm with the physical and socio-emotional aspects of human rights defence. HRDs emphasise that digital security should encompass multiple dimensions, including psychological well-being, protection against online harassment, and safeguarding personal data. It goes beyond mere technical measures as it includes holistically all aspects that interconnect with digital security. This includes an in-depth analysis, through a feminist and decolonial framing, of the risks faced by HRDs, taking into account the interconnected and intersecting ways in which injustices and oppression impact individuals and collectives based on their individual and collective identities.

Flexible, trust-based, and long-term funding: HRDs underscore the critical importance of adequate and sustainable funding for their work. Many operate with little to no support, placing them at higher risk. Conventional project-based and short-term funding practices are often ineffective, hindering their ability to respond to evolving needs and mitigate risks. Flexible, trust-based, and long-term funding allows defenders to adapt swiftly to emerging challenges, share real-time information without fear of repercussions, and develop comprehensive long-term strategies to address and prevent risks and threats effectively.

Accompaniment: Funding alone is insufficient. HRDs described accompaniment in the form of technical skills sharing, guidance, and resources to identify and manage risks and threats effectively as vitally important. Learning about risk assessment and connecting with others within the ecosystem are essential components of this support.

Community building: HRDs emphasised the critical need for secure spaces where they can convene to establish connections, build networks, exchange insights and knowledge, and engage in collaborative resource-sharing and capacity-building. These community spaces provide defenders with invaluable support, fostering cooperation and the dissemination of best practices.

Advocacy and strategic communications: HRDs stressed the need for enhanced support in effectively conveying their experiences and raising awareness about the digital threats and risks they face. As well as support from those in positions of power to bring more and better funding to their efforts.

Our Future

The 2024-2027 strategy begins with a refreshed vision, mission, and guiding principles that steer DDP's endeavours and trajectory during this phase of its work.

Refreshed Vision, Mission, and Guiding Principles

Vision: DDP envisions a world in which HRDs contribute to social justice while enjoying safety, well-being, freedom, and dignity.

As we are acutely aware, the unwavering efforts of HRDs in their daily work play an indispensable role in reshaping our world and combating oppression resulting from systemic injustices. However, it is these very HRDs who often face heightened political violence, exposing them to serious risks on physical, mental, psychosocial, and digital fronts. Throughout the strategic planning process, a critical consensus was reached regarding DDP's vision for change: **a deliberate shift away from the concept of a "free internet" – as articulated since its inception and within the previous Strategic Plan – towards a heightened focus on the well-being of HRDs**. This shift entailed a deep reflection on the conditions envisioned for HRDs to sustain their essential work and efforts, with an unwavering priority placed on their security and overall well-being.

Another aspect that emerged during the refreshed vision process was the significance of presenting a positive vision of change – one that is proactive rather than reactive to threats and effectively communicates the intention to transform the current context faced by HRDs, all while maintaining a framing rooted in a feasible reality.

Mission: DDP is an international programme that contributes to strengthening the resilience of HRDs by increasing their digital security through a holistic and sustainable approach. We do this through: [7]
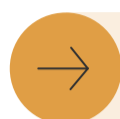
→ **Funding:** Providing financial resources for holistic digital security.

→ **Community Building:** Facilitating and supporting the strengthening of digital security networks and communities at local, regional and global levels.

→ **Accompaniment:** Providing support and knowledge resources to contribute to the sustainability of holistic digital security practices and habits.

DDP's complementary approach of funding, accompaniment, and community building has evolved over the years since its establishment. Each approach is listed in this order intentionally to represent and document DDP's history, learning, and evolution. Initially, DDP functioned primarily as a funding mechanism. Through intentional listening and work with HRDs, DDP learned that funding alone was insufficient, leading to the development of an accompaniment strategy. Most recently, in response to HRDs' requests and the growing importance of collaboration and strengthening networks and communities, DDP has taken on a role in facilitating and supporting community building at local, regional, and global levels.

Throughout the discussions and reflective spaces with DDP's partners and HRDs across the ecosystem, it became evident there was a lack of clarity regarding DDP's identity and role.

This ambiguity led to confusion about whether DDP was an organisation, a programme, or funding entity, and so forth. To provide clarity and bolster DDP's efforts, it was deemed imperative to clarify DDP's identity and role as an **international programme**, within the space through its refreshed mission statement.

DDP's commitment to **strengthening the resilience of HRDs** is rooted in its vision of change, which envisions a context where HRDs have the essential digital security required as they lead their efforts to promote social justice. Within this perspective, resilience is comprehensively understood, encompassing collective, individual, and systemic dimensions. Within this framework, the capacity to respond, rebuild, and adapt forms integral components of the way resilience is both understood and put into practice.

---

7   This component of the mission is also referred to as the approaches used to fulfil the mission.

As defined throughout this process, DDP's central work proposal revolves around the **digital security of HRDs from a holistic and sustainable approach**. This approach involves a comprehensive analysis, framed within a feminist and decolonial perspective, of the risks faced by HRDs. It considers the interconnected and intersecting nature of injustices and oppression that affect both individuals and collectives based on their unique and shared identities. This perspective enables a more effective understanding of the appropriate responses and mitigation measures to address digital security threats. **This means that:**
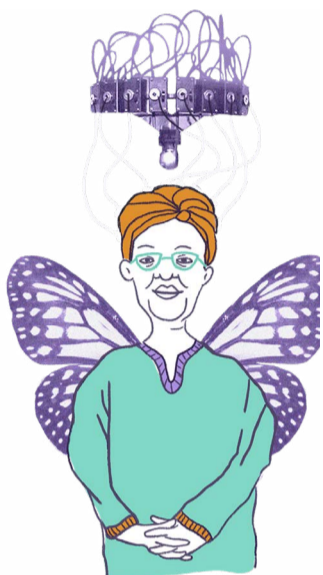
Recognizing the importance of an interdisciplinary comprehension of the threats, risks, and violence encountered by HRDs is essential, as are the strategies necessary to minimise their impact. The DDP team underscored the significance of understanding that these threats emanate not solely from the digital sphere but also have extensive repercussions across multiple facets of HRDs' lives. A comprehensive approach encompasses considerations related to physical security, digital and information security, legal measures, self-care, and overall well-being.

Sustainability is a core commitment centred on strengthening and supporting processes that can continue over a long period, while maintaining balance with its environment and resources (which includes human, environmental, and financial). In the context of DDP, this entails the efforts to strengthen the digital security practices and systems of HRDs in a manner that becomes integrated throughout their work, thereby contributing to the overall sustainability of their strategies.

With this framing, DDP provides financial resources, accompaniment support, and facilitates community-building strategies that work toward strengthening the digital security of HRDs through a holistic approach. This includes safeguarding computer systems, networks, and communication channels against malicious attacks, while taking into account physical and psycho-emotional security, legal measures, self-care, and overall well-being of HRDs.

Lastly, it is paramount for DDP to convey its role as a facilitator in strengthening networks, communities, and practices. This role revolves around recognising the wealth of wisdom and expertise within and across HRDs' communities. DDP serves as a partner and ally in weaving and connecting these networks, promoting exchanges among them, and supporting their co-creation and development.

Guiding Principles

DDP's founding principles have evolved over the years to align with its ongoing learning and approach. The programme's current guiding principles have been revised through a participatory process involving DDP's team members. **These updates are designed to better align with the refreshed vision and mission, as well as DDP's focus on centring feminism and decoloniality across all of its work. DDP's guiding principles include:**
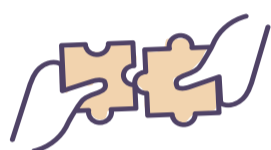
Collaboration: A strong commitment towards fostering solidarity, connection, cooperation and a sense of community in convening spaces. DDP understands that epistemic violence and injustice are barriers to true collaboration. We value different knowledge, aim to decentre dominant discourses and encourage the inclusion of marginal modes of knowledge production and consumption.

Community-Centred: The well-being, autonomy, empowerment and dignity of the people we work for and with are of the utmost importance. In all our activities and engagements, we want to create safe and respectful spaces where people can engage the personal and the political and feel safe and empowered.
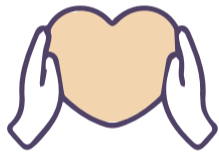
Confidentiality: A commitment to handling all incoming information responsibly and protecting it against inadvertent disclosure to unauthorised parties. In any remote coordination or online initiatives, secure and encrypted channels running on free and open-source software are a priority. Commercial or proprietary tools will be avoided as much as possible, especially if they have a history of violating users' privacy.

Diversity: Encompassing individual uniqueness and distinctions within communities and groups, diversity spans attributes such as race, ethnicity, gender, age, disability, sexual orientation, socio-economic status, education, and every facet that contributes to one's identity, values, and experiences. DDP believes in the importance of diversity and inclusivity, in our networks, teams, ideas and approaches. We work in a way that fosters non-discrimination, free expression, participation, and equity.
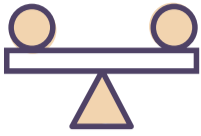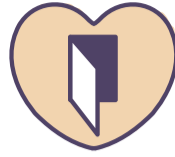
Equity: As a measure of justice, it refers to the fair treatment, access, opportunity, and protection of all people. DDP is committed to a feminist and intersectional approach as the epistemological basis for our analyses and the development of our programmes. Our approach to digital security and the overall protection of HRDs is developed through a lens which seeks to make visible the various layers of structural and discursive discrimination based on gender identity and expression, sexual orientation, race identity, ethnicity, geography, language, culture, religion, caste, socioeconomic status, employment, age, dis/ability, and neuro(a)typicality, among other things.

No-Harm: The understanding that our programmes are not neutral in the contexts within which they are implemented, which are invariably characterised by injustice and conflict in various forms. Our goal is to prevent or limit unintended negative outcomes through a decolonial approach that, through DDP's regionalisation, centres and prioritises the knowledge and solutions of the communities we work for and with.

Not claiming but facilitating: Encouraging individuals, organisations and networks to have and take ownership of their own interventions and activities while supporting their strategies and efforts.

Openness: Attitude of curiosity, innovation, reflective, and transparent learning in our individual and collective work. It is a position against the extraction, exploitation, privatisation, control and restriction of resources and knowledge, emphasising the political dimension of making information accessible to the public and of adopting, developing and maintaining free/libre and open-source tools that adapt and align with the evolving needs of the communities utilising them.

DDP is committed to working towards centring feminist and decolonial approaches These approaches seek to highlight both the relations of patriarchal and colonial domination and their direct effects on contemporary social configurations, in order to mitigate their consequences. Adopting these approaches entails active efforts to avoid reproducing misogyny, racism, colonialism and xenophobia and simultaneously working to dismantle them throughout the tools, practices, and systems within DDP and beyond: in project implementation, budget allocation, team management, decision-making structures, training, knowledge production, etc.

Throughout our previous strategic period (2020-2023), we paid a great deal of attention to including a feminist perspective in our projects and activities. We developed a specific GEDI strategy - now merged into this general strategy - and launched recommendations to guide our partners in mainstreaming gender into their activities. We also supported feminist organisations and collectives, and feminist infrastructure initiatives, and facilitated a community of feminist helplines for people facing gender-based violence online. We also began to host internal debates on decolonisation with seminars and content production that would allow us to reach a common understanding of what decolonisation meant for an organisation like DDP.

For this strategic period, our focus is to continue to deepen the feminist and decolonial approaches in our programme's implementation. However, we must complement it with an environmental justice approach from a political ecology perspective.

The climate crisis, the struggle for access to and control over nature, the extractivist model and the persecution of environmental activists and Indigenous peoples compel us to include this perspective in our programme. We understand that capitalism is only possible by the exploitation of nature, an exploitative international division of labour, and the subjugation of women and LGBTQIA+ people. Establishing connections between feminist and decolonial approaches, including an ecological and environmental justice perspective, is imperative. [8]

Operations-wise, we are fully aware that centring feminism and decolonisation in a programme hosted by an international organisation based in Europe and funded by State departments and agencies is challenging in many ways. We also acknowledge that we need to learn to deal with power, both collectively and individually, and explore and adopt institutional arrangements that mitigate the impacts of the different structural oppressions in which we are embedded.
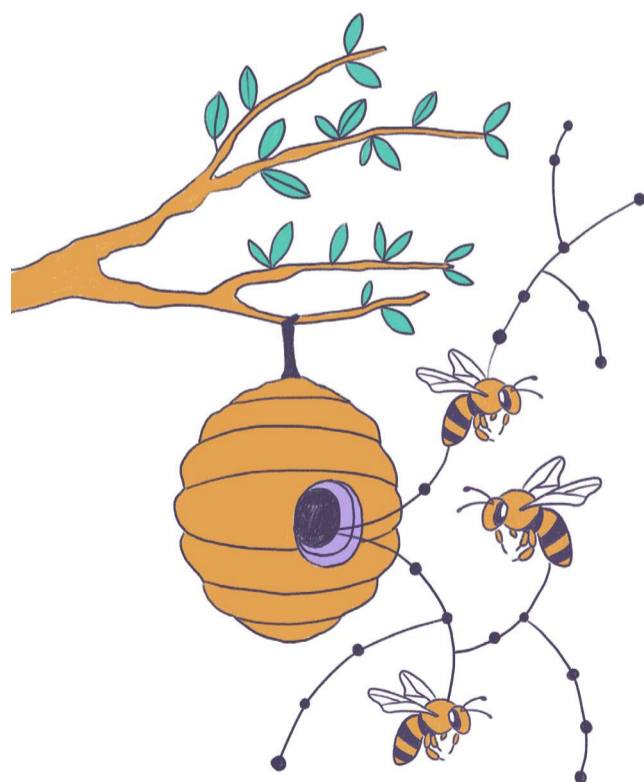
Nevertheless, we have started to move in that direction in recent years, and we are committed to making further progress in our 2024-2027 strategic period. We will look to achieve this not only by strengthening the knowledge and capacities of the DDP team in areas of feminism and decoloniality but also by adopting a labour justice framework, institutionalising multilingual working practices, strengthening decentralised decision-making, constantly reviewing our granting procedures to be culturally and context-sensitive, and improving internal complaints mechanisms, among other measures. **We have included Strategic Objective 4 to address this issue.**

---

8   To further explore this topic, read Mies, M. (2014). Patriarchy and accumulation on a world scale: Women in the international division of labour. Zed Books.

Who We Work With

To fulfil its mission, DDP supports HRDs working across movements and issues. This is because the foundation of HRDs' work is not isolated but rather intersectional and interconnected, since it seeks to dismantle and transform systemic injustices. Aligned with our regionalisation efforts that are grounded in the firm belief and understanding of local knowledge and expertise, each regional team identifies its priority populations based on the prevailing context. This enumeration aims to establish a standardised set of options that facilitate streamlined communication about each region's priorities. The list should remain open to edits and amendments to reflect varying priority populations across regions while maintaining a consistent wording approach to ensure clarity and understanding across all regions. It's important to note that each region maintains autonomy regarding the population they prioritise. **Priority population list*:**

→ **Actors who make information available to the public**

→ **Afro-descendant communities**

→ **Communities with disabilities**

→ **Environmental activists and land defenders**

→ **Feminist and women's rights activists**

→ **LGTBQIA+ activists**

→ **Indigenous communities**

→ **Rapid responders and holistic security trainers**

During this strategic planning process, a crucial insight emerged regarding the influence that the definition of priority populations and institutional priorities can exert on the agendas of local organisations and movements. Therefore, it is of paramount importance to effectively communicate that DDP's prioritisation process is designed to be responsive to the needs and realities of the contexts rather than imposing a predetermined agenda of populations and issues.

Journey of Change

A Journey of Change is a framework that guides an organisation's efforts towards social justice by embracing an approach that acknowledges the inherently dynamic and non-linear nature of social change. It emphasises the imperative for adaptability, flexibility, and ongoing evolution in the pursuit of social justice. The Journey of Change is purposefully crafted to underpin a shared political vision of justice, ensuring its resonance and malleability while offering a clear collective roadmap. A Journey of Change is composed of a General Objective, Specific Objectives and the necessary and sufficient strategies to achieve them. Collectively, these elements constitute the foundational framework of a Strategic Plan. For reference, please see **Appendix A to review the Journey of Change map.**

* Note: We understand the interconnectedness and intersectionality that exists among communities. This list does not seek to place any community in a silo or create any generalisations.

General Objective

Contribute to strengthening the resilience of HRDs by increasing their digital security from a holistic and sustainable approach. The General Objective is in alignment with the organisation's mission and actively **contributes to the realisation of its vision for social change. The DDP's Journey of Change encompasses four specific objectives along with their corresponding strategies, detailed below.**

SO1 | **Strategic Objective 1: Increase flexible and relevant resources for holistic digital security for HRDs at risk (mitigate).**

Providing resources to support HRDs to mitigate threats and prevent security incidents from escalating, thereby minimising harm, is a key priority of our work. As a result, we will remain committed to our original mandate, providing funding to respond to the digital security needs of HRDs, recognising their individual contexts and realities. We see knowledge as a critical resource to respond effectively to attacks or security incidents. That is why we will continue to develop and disseminate valuable resources in the form of manuals and guides.

When working with HRDs, it is imperative to acknowledge their multifaceted needs, many of which extend beyond our mandate. In such instances, we will continue to facilitate referrals to partner organisations and networks specialising in areas such as physical and psycho-emotional security. In the digital realm, we will continue to address specific needs through prompt guidance offered by our team of local experts.
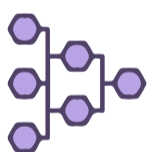
Strategies:

1.1. Provide funding that supports the security needs of HRDs in the event of security incidents with digital impacts.

1.2. Facilitate the provision of resources for the identification of risk factors and the development of mitigation strategies (Digital First Aid Kit, Tech Care, Feminist Security and Feminist Holistic Protection, etc.).

1.3. Respond to *ad-hoc* requests from HRDs facing security risks and threats, ensuring context-specific and relevant support (1:1, referrals, etc.).

1.4. Provide funding for national, regional or global initiatives that support the digital security of HRDs at risk.[9]

---

9   Currently, DDP employs two mechanisms to support this effort: the Regional Partnership Fund (RPF) and the Global Partnership Fund (GPF). Based on evaluations and learning, the RPF has proved to be an effective and relevant funding mechanism and will continue as established. The GPF will undergo a review and analysis during the current strategic planning period to assess its future trajectory.

This objective highlights a central topic of discussion within DDP related to its response to threats and attacks faced by HRDs. There has been significant reflection on whether the DDP has the capacity to respond effectively to emergencies. It was observed that regional teams are under substantial pressure to provide rapid responses, but this expectation does not align with the actual operational processes of the programme, including the review of proposals and fund allocation. As a result, the primary value of this funding is not necessarily speed but rather its flexibility and relevance in providing digital security support through a holistic approach. Additionally, it underscores the trust that HRDs place in the DDP and its understanding of the context.

Another important reflection was to acknowledge that security incidents are not exclusively digital; DDP – in line with its mandate and the expertise of its team – primarily focuses on digital responses. An example was provided of an environmental incident with a digital impact, clarifying that the digital realm is not the cause but rather the effect. DDP addresses this aspect by allocating funds to deal with such situations.

This objective and its strategies also emphasise the importance of responding to risks and threats effectively with complementary resources such as manuals and procedures. The aim is to reduce the repercussions of attacks or pre-empt their escalation, thereby preventing further damage. In this context, another integral strategy entails the provision of support and guidance by Digital Protection Facilitators and the DDP team at large. Leveraging their extensive networks, both personal and professional, they extend invaluable support to HRDs when facing specific instances of attacks or threats.

Moreover, when confronted with needs beyond the scope of DDP's expertise, the teams refer HRDs to resources and people specialising in various domains such as physical security, psychological or psychosocial support, legal counsel, and more. This holistic approach ensures that HRDs receive comprehensive support tailored to their unique circumstances, ultimately enhancing their capacity to navigate and mitigate the multifaceted risks and threats they encounter.

| **SO2** | **Strategic Objective 2: Strengthen and support HRDs' digital security knowledge, capabilities, and practices through a holistic approach (prevent).** |

Central to our approach is providing resources, in funding as well as tools, that support HRDs to identify and implement prevention practices that become ingrained throughout their work. We will also continue to implement

our Digital Protection Accompaniment Model, which consists of a comprehensive strategy focused on improving HRDs organisations' and collectives' digital (and overall) security.[10]

---

10   Read DDP's Digital Protection Accompaniment Model manual to gain further insight.
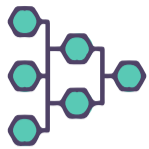
Strategies:

2.1. Grant Sustainable Protection Funds to HRDs aligned with the regional priorities.

2.2. Provide accompaniment to strengthen HRDs' digital security through a holistic approach that fosters the internalisation of knowledge, practices, and habits.

2.3. Facilitate the provision of resources to strengthen HRDs' digital security as well as their infrastructure and use of free and open-source software through a holistic approach (includes the resources developed/documented/gathered through the accompaniment process, prevention clinics, etc.).

2.4. Strengthen HRDs' knowledge and access to free and open-source software and resources.

The sustainability criterion embedded within DDP's Mission entails strengthening existing digital security systems and practices, while also incorporating knowledge designed to prevent digital security risks and incidents. This knowledge and practice are fundamental components of the DDP's approach and what they aim to support HRDs in embedding throughout their practices and work. To achieve this objective, DDP provides funding, accompaniment, and resources that prioritise the long-term strengthening of HRDs' digital security.

DDP's Accompaniment model, identified as a foundational and crucial resource by partners, offers a holistic and sustainable response to digital threats. The model has a dedicated focus on improving HRDs organisations' and collectives' digital (and overall) security.

During the development of the strategic plan, the distinction between "Protection" and "Security" was carefully considered. The regional teams pointed out that "protection" encompasses or implies elements like evacuation procedures and the temporary relocation of individuals, as well as addressing needs such as protection from diseases, contagion, hunger, or cold, among others. These are areas that are clearly beyond the scope of DDP's coverage. It is for these reasons that the Journey of Change focuses on "security" rather than "protection."

In alignment with DDP's principles of Openness, the strategy to strengthen HRDs' knowledge and access to free and open-source software and resources was proposed and prioritised. DDP has already been spearheading this initiative, albeit with limited visibility and documentation. Therefore, incorporating it as a formal strategy is an endeavour to ensure that this work is acknowledged and recognised.

SO3

Strategic Objective 3: Support the strengthening of digital security knowledge, capacities, and practices within networks and communities at the local, regional, and global levels.[11]

We will maintain our efforts to facilitate and support the creation and expansion of rapid response networks supporting HRDs' digital security, while upholding, honouring, and promoting local knowledge and expertise in the regions where we work.
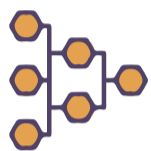
Strategies:

3.1. Provide support (financial and technical) as well as capacity-building to members of rapid response networks.

3.2. Develop a strategy for DDP's participation and engagement in rapid response networks.

3.3. Provide funding for collaboration, knowledge exchange, research, and the dissemination of learnings.

In this third objective, DDP's role as a facilitator to strengthen rapid response networks while simultaneously respecting, honouring, and promoting local knowledge and expertise within different regions is central to its approach. To be more specific, DDP extends its support to the Rapid Response Network (RaReNet), CiviCERT, digital security helpdesks for civil society and the global community of feminist helplines oriented at people facing gender-based violence online.

One evident need that surfaced during the strategic planning process is to formulate a strategic approach in which DDP and its team actively participate in existing networks that contribute to the strengthening of HRDs' digital security. This clarity is essential for the purpose of formalising and refining the structure of DDP's engagement in these networks. It will empower DDP to operate with greater strategic precision, ensuring that key opportunities for collaboration are not missed.

In general, the funds allocated by DDP in this area of work are used for training members of the rapid response networks, and funding self-organised activities or meetings among network members. These funds can also support the dissemination of research findings and lessons learned by the networks themselves, thereby enhancing and broadening their impact and outreach. This extends to other communities and networks that are working to strengthen HRDs' digital security, whether directly or indirectly connected to DDP. DDP humbly acknowledges that it is part of a broader ecosystem, and its goal is to contribute to the overall strengthening of HRDs' digital security.

---

11 DDP recognises the importance of local, regional, and global levels without assigning specific priorities, as they are all interconnected and interrelated. A critical aspect of our work is to ensure that our efforts do not perpetuate silos that reinforce the same injustices and practices that cause harm.

SO4   Strategic Objective 4: Strengthen DDP's infrastructure, resilience, and sustainability.

We are deepening our work by recognising the importance of looking within to strengthen our resilience and sustainability. By prioritising our foundations, we enhance our capacity and ability to provide robust support to HRDs.

Guided by feminist and decolonial approaches, we will work to develop policies and processes that bolster our internal practices, structure, and culture.
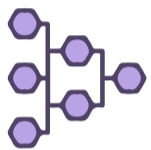
Strategies:

4.1. Develop DDP's feminist and decolonial approaches and incorporate them into DDP's internal operations and project implementation through an intersectional lens (policies, procedures, etc.).

4.2. Develop and implement a labour justice framework that guides DDP's practices (including fair compensation and human resources management).

4.3. Develop and implement collective care practices (including workload management, institutionalising multilingual work practices, project management approaches, mental health support, etc.).

4.4. Strengthen the knowledge and capacities of DDP team members in areas of feminism, decoloniality, digital security, collective care, learning, and evaluation.

4.5. Develop clear decision-making and leadership models and procedures (including a review and update of DDP structure, roles and functions, etc.).

4.6. Strengthen the institutional capacity for innovation and creativity by creating dedicated team spaces and practices designed to support learning, strategic planning, and reflection.

This objective emphasises the urgent need to strengthen DDP internally, recognising the dedicated efforts of numerous team members over the years that have propelled DDP's substantial and strategic growth. Notably, for the first time since DDP's establishment, internal strengthening takes precedence as a strategic objective. With this goal in mind, it is time to embark on the path of sustaining all that has been achieved from a sustainable, decolonial, feminist, and intersectional perspective. This entails advocating for a culture that prioritises the well-being and care of its members, with the allocation of necessary resources, funding, and time to support this effort.

As it is important to highlight, these aspirations extend beyond good intentions; they must be underpinned by processes, mechanisms, policies, and agreements that ensure the necessary conditions for their implementation in daily work. Throughout this process, two primary tensions were identified within the team:

The absence of clarity concerning decision-making, levels of responsibility, and the accurate definition of roles/positions.

The lack of transparency and a perception of "injustice" regarding the compensation structure and the assurance of labour rights.

Additionally, there were concerns about evident cases of burnout occurring among team members, with uncertainties about the appropriate institutional response.

Considering the above, DPP formulated strategies to prioritise enhancing clarity and establishing a robust infrastructure in the mentioned areas. These strategies aim to foster greater institutionalisation of effective practices for managing and resolving these tensions. Addressing these issues presents a significant opportunity to strengthen DDP as a whole.

Lastly, it was also highlighted, particularly in one region, that investing in open-source systems was imperative to contribute to DDP's sustainability and resilience. Similarly, in another region, there was a strong desire for DDP to evolve into a more multilingual organisation and enhance accessibility. The discussion on how to address these suggestions is yet to take place, but there is a clear emphasis to prioritise multilingual work practices within the collective care objective.

"Strengthening DDP's infrastructure, resilience, and sustainability aims to foster a greater institutionalisation of effective practices for managing and resolving tensions and presents a significant opportunity to strengthen DDP as a whole."

APPENDIX A

Journey of Change Map

General Objective	Strategic Objectives	Strategies
Contribute to strengthening the resilience of human rights defenders (HRDs) by increasing their digital security from a holistic and sustainable approach.	1. Increase flexible and relevant resources for holistic digital security for HRDs at risk (mitigate).	**1.1. Provide** funding that supports the security needs of HRDs in the event of security incidents with digital impacts. **1.2. Facilitate** the provision of resources for the identification of risk factors and the development of mitigation strategies (Digital First Aid Kit, Tech Care, Feminist Security and Feminist Holistic Protection, etc.). **1.3. Respond** to ad-hoc requests from HRDs facing security risks and threats, ensuring context-specific and relevant support (1:1, referrals, etc.) **1.4. Provide** funding for national, regional or global initiatives that support the digital security of HRDs at risk.
	2. Strengthen and support HRDs' digital security knowledge, capabilities, and practices through a holistic approach (prevent).	**2.1. Grant Sustainable Protection Funds** to HRDs aligned with the regional priorities. **2.2. Provide** accompaniment to strengthen HRDs' digital security through a holistic approach that fosters the internalisation of knowledge, practices, and habits. **2.3. Facilitate** the provision of resources to strengthen HRDs' digital security as well as their infrastructure and use of free and open-source software through a holistic approach (includes the resources developed/documented/gathered through the accompaniment process, prevention clinics, etc.). **2.4. Strengthen** HRDs' knowledge and access to free and open-source software and resources.

General Objective	Strategic Objectives	Strategies
	3. Support the strengthening of digital security knowledge, capacities, and practices within networks and communities at the local, regional, and global levels.	**3.1. Provide** support (financial and technical) as well as capacity-building to members of rapid response networks. **3.2. Develop** a strategy for DDP's participation and engagement in rapid response networks. **3.3. Provide** funding for collaboration, knowledge exchange, research, and the dissemination of learnings.
	4. Strengthen DDP's infrastructure, resilience, and sustainability. *We are deepening our work by recognising the importance of looking within to strengthen our resilience and sustainability. By prioritising our foundations, we enhance our capacity and ability to provide robust support to HRDs. Guided by feminist and decolonial approaches, we will work to develop policies and processes that bolster our internal practices, structure, and culture.*	**4.1. Develop** DDP's feminist and decolonial approaches and incorporate them into DDP's internal operations and project implementation through an intersectional lens (policies, procedures, etc.). **4.2. Develop and implement** a labour justice framework that guides DDP's practices (including fair compensation and human resources management). **4.3.Develop and implement** collective care practices (including workload management, institutionalising multilingual work practices, project management approaches, mental health support, etc.). **4.4. Strengthen** the knowledge and capacities of DDP team members in areas of feminism, decoloniality, digital security, collective care, learning, and evaluation. **4.5 Develop** clear decision-making and leadership models and procedures (including a review and update of DDP structure, roles and functions, etc.). **4.6 Strengthen** the institutional capacity for innovation and creativity by creating dedicated team spaces and practices designed to support learning, strategic planning, and reflection.

APPENDIX B

Strategic Plan Shared Language

Why Language Matters?

The language we use and how we define it shapes our understanding and practices across organisations and communities, transcending contexts and moments. Committed to transparency, accountability, and constant evolution through learning, Digital Defenders Partnership (DDP) developed a shared language glossary as a complementary component to its 2024-2027 Strategic Plan. Through this document, DDP provides collective definitions for each term to create a clear understanding of the terminology and approach. This living document will be updated throughout time to reflect DDP's continuous learning and evolution.

Note: A comprehensive organisational glossary is also in development, encompassing terms in this Shared Language document accompanying the 2024-2027 Strategic Plan.

Table of Contents

H

- Hivos
- Holistic Approach
- Holistic Protection
- Human Rights Defender

I

- International Programme
- Intersectional Approach
- Integrity

J

- Journey of Change

L

- LGTBQIA+

M

- Mentoring

N

- Not Claiming but Facilitating
- No-harm

O

- Openness

P

- Physical Security
- Political Ecology
- Protection
- People-Centred

R

- Risk
- Regions
- Regionalisation
- Resilience

S

- Safety
- Security
- Secure
- Self-care and Well-being
- Social Justice
- Sustainability

T

- Threat

V

- Vulnerability

A

Accessibility: The approach or extent to which a person or community can access resources, information and spaces. This includes physical and virtual realms, emphasising the collective responsibility to address systemic barriers to ensure accessibility rather than burden the individual or community experiencing a lack of access due to systems of oppression.[1]

Accompaniment: Mentoring civil society organisations to build sustainable digital protection practices.[2]

Accompanied Organisation: Organisation, collective or network engaged in a Digital Protection Accompaniment process.

Attack: Attempts "to close the socio-political space" in which human rights defenders work, including "literal physical spaces, as well as economic, social, technological, legal or environmental space, among others."[3]

C

Capacity: "Strengths and resources a group or defender can access to achieve a reasonable degree of security."[4]

Crisis: Profound and detrimental change in a political, economic or social process. DDP understands crisis as an event that: (1) poses a serious threat to the DDP team members or Hivos/DDP reputation; (2) severely disrupts normal operations, including physical and psychosocial events; (3) requires a quick or immediate intervention and response; (4) requires coordinated and efficient management of procedures and resources, whether human, material or logistical, that is beyond the capability of the local office/programme where the event has occurred.[5]

Civil Society Computer Incident Response Center (CiviCERT): Launched in 2015, CiviCERT is a network of Computer Emergency Response Teams (CERTs), rapid responders, and independent Internet Content and Service Providers (ICSPs) who support civil society in preventing and addressing digital security incidents. DDP is a member of CiviCERT.

---

1   Definition drafted by Sukuamis.
2   Definition sourced from DDP's Digital Protection Accompaniment Model manual.
3   Definition by Higson Smith, Ò Cluanaigh, Ravi & Steudner, 2016: 20.
4   Definition by Eguren & Caraj, 2009: 29.
5   Definition sourced from DDP's Crisis Manual.

Collaboration: A strong commitment towards fostering solidarity, connection, cooperation and a sense of community in convening spaces. DDP understands that epistemic violence and injustice are barriers to true collaboration. We value different knowledge, aim to decentre dominant discourses and encourage the inclusion of marginal modes of knowledge production and consumption.[6]

Confidentiality: A commitment to handling all incoming information responsibly and protecting it against inadvertent disclosure to unauthorised parties. In any remote coordination or online initiatives, secure and encrypted channels running on free and open-source software are a priority. Commercial or proprietary tools will be avoided as much as possible, especially if they have a history of violating users' privacy.[7]

Community Building: Set of practices aimed at creating, strengthening or facilitating communities of individuals or collectives gathered under a common need or interest or within a geographical area.

Climate Justice Approach: A political, social, and ethical framework which understands that the climate crisis results from capitalism and its compounding and intersecting systemic injustices. According to this framework, overcoming the climate crisis requires an intersectional social justice approach that puts the leadership, solutions and needs of those most affected at the centre.[8]

D

Decolonial Approach: Political and epistemological positioning that seeks to highlight the ongoing legacy of colonial domination and direct effects on contemporary social systems and structures, all while developing strategies to overcome its consequences and dismantle it.[9] Adopting this approach entails active efforts to not reproduce racism, colonialism and xenophobia in project implementation, budget allocation, team management, decision-making structures, training, knowledge production, etc.

Digital Rights: "Human rights and legal rights that allow individuals to access, use, create, and publish digital media or to access and use computers, other electronic devices, and telecommunications networks."[10]

---

6   One of DDP's organisational principles.

7   One of DDP's organisational principles. To gain further insights, read the Traffic Light Protocol and DDP's organisational policies and approaches around confidentiality.

8   Definition drafted by Sukuamis.

9   Read the Digital Protection Accompaniment Model manual to gain further insight into how we practise a decolonial approach in our accompaniment.

10   Definition sourced from Wikipedia.

Digital Attack: Actions or interventions of malicious actors to constrict or otherwise negatively impact the work, physical or psychological well-being of others through digital technologies. This can include: intimidation in either offline or online spaces due to the nature of one's work; gender-based violence online; unauthorised access to emails, websites, social media, etc.; targeted censorship, phishing and malware attacks; confiscation or destruction of devices during protests or raids; identity fraud or theft; and internet shutdowns.[11]

Digital Security: "Protection of computer systems and networks from attack by malicious actors that may result in unauthorised information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide."[12] [13]

Digital Protection Accompaniment Model: In response to the trend of "box-checking" digital security trainings for human rights defenders, DDP developed a Digital Security Accompaniment Model. The model consists of a comprehensive programme of activities, including sustainable responses to threats, facilitation, and community building within the broader ecosystem of support to human rights defenders under digital siege.[14]

Digital Security Incident: "Any fact or event which you think could affect your personal or organisational security. Security incidents can be incidental or provoked intentionally or unintentionally."[15]

Disability Justice: "Path and goal of Collective Liberation, in which we hold the question "How do we move together" - as people with mixed abilities, multiracial, multi-gendered, mixed class, across the orientation spectrum - where no body/mind is left behind."[16] (Sins Invalid)

Diversity: Encompassing individual uniqueness and distinctions within communities and groups, diversity spans attributes such as race, ethnicity, gender, age, disability, sexual orientation, socioeconomic status, education, and every facet that contributes to one's identity, values, and experiences.[17] DDP believes in the importance of diversity and inclusivity, in our networks, teams, ideas and approaches. We work in a way that fosters non-discrimination, free expression, participation and equity.

---

11   Revised definition sourced from DDP's 2020-2023 Strategy.

12   Definition sourced from Wikipedia.

13   Read DDP's Digital Protection Accompaniment Model manual to gain further insight around digital security.

14   Read the Digital Protection Accompaniment Model manual to learn more.

15   Definition by Eguren & Caraj, 2009: 45-46.

16   Definition by Sins Invalid.

17   One of DDP's organisational principles. Definition drafted by Sukuamis.

E

Ecosystem: Multitude of activists, collectives, organisations and networks with which we share common values, goals, and objectives. This includes those with a focus on digital rights, emergency response, Internet freedom, privacy rights, protection of human rights defenders, technological autonomy, and many more.[18]

Emergency: Sudden, unexpected and dangerous event that requires fast action with resources available to avoid harmful results.

Equity: As a measure of justice, it refers to the fair treatment, access, opportunity, and protection of all people. DDP is committed to a feminist and intersectional approach as the epistemological basis for our analyses and the development of our programmes. Our approach to digital security and the overall protection of human rights defenders is developed through a lens which seeks to make visible the various layers of structural and discursive discrimination based on gender identity and expression, sexual orientation, race identity, ethnicity, geography, language, culture, religion, caste, socioeconomic status, employment, age, dis/ability, and neuro(a)typicality, among other things.[19]

F

Fund: Amount of money devoted to financially supporting DDP's incident emergency mechanism, strengthening of organisational sustainable security practices and rapid response community building.

Feminist Approach: The political and epistemological positioning that seeks to highlight relations of patriarchal domination and their direct effects on contemporary social configurations and to mitigate its consequences.

G

Grassroots: Organisations, networks or movements in direct relation to local communities.

H

Hivos: The Humanist Institute for Development Cooperation is an international cooperation organisation based in The Hague aimed at amplifying and connecting voices that promote social and environmental justice and challenge power imbalances. Hivos, a member of the Freedom Online Coalition, has hosted DDP since its creation in 2012.

---

18   Revised definition sourced from DDP's 2020-2023 Strategy.

19   One of DDP's organisational principles.

Holistic Approach: A positioning for security and protection of human rights defenders that recognises the need for, and promotes, an interdisciplinary understanding of political violence and the strategies needed to reduce it. This includes physical security, digital and information security, legal responses, and self-care and well-being.

Holistic Protection: Protection strategies developed with a holistic approach.

Human Rights Defender: "Person who, individually or with others, acts to promote or protect human rights."[20] This can include activists, artists, journalists, lawyers, teachers, and actors who make information available to the public, among others, both as an individual or within a group, collective, and/or organisation.

I

International Programme: A global initiative within an organisation. DDP is an international programme hosted at Hivos. Centring a decolonial approach, DDP operates within a framework that prioritises the experience, knowledge, and autonomy of each region. We understand that those connected to the context, with the lived experiences, are best positioned to guide decision-making and contextually relevant strategies.

Intersectional Approach: A feminist method of analysis which seeks to visibilise overlapping forms of discrimination based on a person's social and political identities (including those related to race, disability, ethnicity, gender identity, religion, sexual orientation, etc.) to discern and address the fundamental causes underlying injustices.[21]

Integrity: Commitment to transparency and accountability in all projects, outcomes, and decision-making processes. This entails documenting and sharing useful information with others and striving to establish fair and just processes in all relationships with donors, partners, grantees, consultants, and all other members across the ecosystem.

J

Journey of Change: A framework that guides an organisation's efforts towards social justice by embracing an approach that acknowledges the inherently dynamic and non-linear nature of social change. It emphasises the imperative for adaptability, flexibility, and ongoing evolution in the pursuit of social justice. The Journey of Change is purposefully crafted to underpin a shared political vision of justice, ensuring its resonance and malleability while offering a clear collective roadmap.[22]

---

20   Revised definition sourced from DDP's 2020-2023 Strategy.

21   Definition developed based on Kimberlé Crenshaw's concept of intersectionality.

22   Definition provided by Sukuamis.

L

LGTBQIA+: Lesbian, Gay, Trans, Bisexual, Queer, Intersexual, Asexual, and + to "recognize the limitless sexual orientations and gender identities across the community."[23]

M

Mentoring: Process through which DPFs accompany, train and coach focal points to become protection agents within their organisations.

N

Not Claiming but Facilitating: Encouraging individuals, organisations and networks to have and take ownership of their own interventions and activities while supporting their strategies and efforts. [24]

No-Harm: The understanding that our programmes are not neutral in the contexts within which they are implemented, which are invariably characterised by injustice and conflict in various forms. Our goal is to prevent or limit unintended negative outcomes through a decolonial approach that, through DDP's regionalisation, centres and prioritises the knowledge and solutions of the communities we work for and with. [25]

O

Openness: Attitude of curiosity, innovation, reflective, and transparent learning in our individual and collective work. It is a position against the extraction, exploitation, privatisation, control and restriction of resources and knowledge, emphasising the political dimension of making information accessible to the public and of adopting, developing and maintaining free/libre and open-source tools that adapt and align with the evolving needs of the communities utilising them.

P

Physical Security: Protection of the physical integrity of the organisation and its staff, including protection of the building, hardware, and physical files and documentation. Travel and other forms of logistical security for events and workshops also fall under this category.[26]

---

23   Definition sourced from The Human Rights Campaign.

24   One of DDP's organisational principles.

25   One of DDP's organisational principles.

26   Definition from DDP's Accompaniment Manual, article 'What do we understand by a holistic, community-based and intersectional approach?'

Political Ecology: Critical field of knowledge that examines how power relations and economical structure shape nature-society relations.

Protection: "Condition or state of being kept safe from injury, damage, or loss." (Cambridge Dictionary).

People-Centred: The well-being, autonomy, empowerment and dignity of the people we work for and with are of the utmost importance. In all our activities and engagements, we want to create safe and respectful spaces where people can engage the personal and the political and feel safe and empowered. [27]

R

Risk: Possibility of negative events happening.

Regions: Each of the geographical areas in which DDP operates. Currently: Asia, Anglophone Africa, East Europe, Caucasus and Central Asia, Francophone Africa and Latin America.

Regionalisation: Decentralisation process of DDP operations through which regions gain autonomy in decision-making.

Resilience: A profound response system encompassing social, community, individual, and systemic elements that enable a group to rebound, reconstruct, or adapt in the face of challenges, while also acquiring knowledge and capabilities that empower it to confront contextual adversities with increased strength. [28]

S

Safety: Feeling of not being in danger. In contrast to security, it is a personal sensation of having under control all elements that could harm us.

Security: Protection against threats and attacks.

Secure: State of being protected against threats and attacks.

---

27   One of DDP's organisational principles.
28   Definition provided by Sukuamis.

Self-care and Well-being: The recognition of, and strategies for, the psychological and psychosocial impacts of the risks which team members of human rights organisations face related to the work they carry out. Indeed, the risks of burnout, unhealthy internal conflicts, and staff turnover as a result of untreated institutional conflicts are even more of a risk to human rights organisations, as these organisations are often understaffed, underfunded, and working in dangerous environments. [29]

Social Justice: A long-term collective political vision of achieving a just society by dismantling systemic oppression and injustices. [30]

Sustainability: Quality of being able to continue a process over time in balance with the environment's resources (economic, human, ecological, etc.).

T

Threat: "Declaration or indication of an intention to inflict damage, punish, or hurt."[31]

V

Vulnerability: "Any factor which makes it more likely for harm to materialise or result in greater damage."[32]

---

29   Definition sourced from DDP's Accompaniment Manual, article 'What do we understand by a holistic, community-based and intersectional approach?'

30   Definition provided by Sukuamis.

31   Definition by Frontline Defenders.

32   Definition by Frontline Defenders.

Digital Defenders Partnership 2024-2027 Strategic Plan

Towards centring feminism and decoloniality