KALEIDOS
RESEARCH

MID-TERM EVALUATION OF THE DIGITAL DEFENDERS PARTNERSHIP

Marije van Gent
Ben Wagner
Evelien Boonstoppel

In collaboration with
Gabriela Martínez Sainz (Mexico)
Wairagala Wakabi (Uganda)
Oleg Kozlovsky (Russia)

Amsterdam, 6 June 2017

Kaleidos Research / Pakhuis De Zwijger / Piet Heinkade 181-H / 1019 HC Amsterdam
T +3188 7120360 / www.kaleidosresearch.nl / info@kaleidosresearch.nl / @KaleidosR
Kaleidos Research is part of NCDO Foundation

CONTENTS

EXECUTIVE SUMMARY

Introduction

In 2012, the Digital Defenders Partnership (DDP) was established by the Freedom Online Coalition (FOC) to protect critical internet users and to keep the internet open and free. The programme is implemented by the Dutch-based INGO Hivos, and funded by seven international donors: the US state department, the Ministries of Foreign Affairs of the Netherlands, Finland, Estonia, Latvia, the Swedish International Development Cooperation Agency (SIDA) and – since spring 2017 - the Department of Foreign Affairs Trade and Development Canada. This mid-term evaluation assessed the effects of DDPs approach on critical internet users and the digital emergency response ecosystem as executed from the start of the programme in 2012 until now.

Digital Defender Partnership

By means of providing support, expert advice and funding to individuals, DDP aims to increase safety for cyber activists under attack. In addition, DDP supports the capacity of the digital emergency response eco-system by investing in key responders who provide services to critical internet users. In the visual flow chart below, the theory of change of DDP is presented showing how DDPs outputs lead to the desired outcomes and impact. DDP comprises three different types of interventions, each type aiming for particular intermediate outcomes. The first group of interventions is focused on incidental emergency: tools like the incidental emergency grant, the support of three strategic partners and some of the advice & referrals DDP provides. The second group of interventions contains sustainable emergency support, such as the digital integrity fellowship, the sustainable emergency grants and tools like the Digital First Aid Kit. The third group of interventions aims to enhance the digital emergency response eco-system, in order to improve the quality of response towards critical internet users.

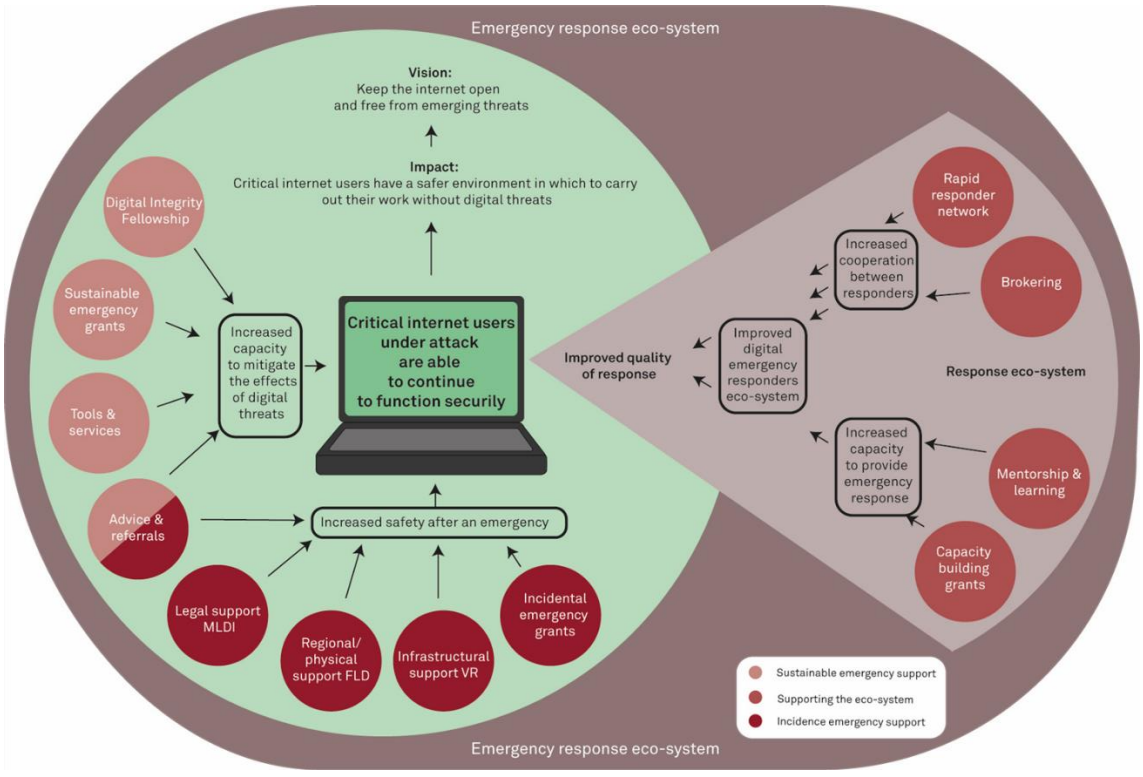

Figure 1.

Value of DDP for stakeholders

Almost all respondents supported through DDP feel that they have benefitted from the support. Critical internet users report an increased level of awareness of security threats and improved their digital safety practices, although in some cases adherence to digital safety procedures remains a bottle-neck. In half of the cases, critical internet users felt that the support given was not a quick fix, but led to sustainable changes. Organisations that received long term support (via the digital integrity fellowship or by receiving a sustainable emergency grant) report more behavioural and organisational changes compared to organisations receiving incidental support as they had time to adopt practices and develop protocols over time. In addition, the critical internet users more at-risk were more inclined to change their digital safety practises. The data also implied that the support not only impacted the beneficiaries, but in some cases also the people and organisations they collaborated with; beneficiaries shared their gained knowledge and skills in their community.

Although it is difficult to assess whether the capacity of the digital response eco-system has increased, responders feel that the quality of their response has improved through DDP support. Rapid response members of RaReNet are positive about the effect of this network on their work, although they agree that the benefits could be higher if the network was even more actively managed. Strategic partners value the trust DDP gives to them and the grants help them to sustain their work. Donors and outsiders also value the outcomes of DDP as positive. Outsiders appreciate the existence of DDP due to the sheer need for digital safety support in many countries but feel that the outreach of DDP is quite limited. They also stress the importance of long term support, like the digital integrity fellowship, to capacitate organisations to deal with digital safety issues themselves.

DDPs strategy

According to DDPs beneficiaries, all the different interventions have a certain impact and contribute to the goals of DDP. In general, the Theory of Change (see figure 1 above) seems confirmed by the data. However, when looking at the needs of the target group, DDPs interventions will never be sufficient and it is clear that DDPs budget is a limiting factor. It makes it even more important to be very strategic in the focus of the programme and who to support. There is a large group of critical internet users in need that is not reached by the programme. DDPs outreach and selection processes are assessed as somewhat weaker compared to other elements; because of the conscious choice to not undertake a strong outreach, there is a dependence on DDPs (elaborate) network to connect to organisations in need of support. Critical internet users that operate more locally and that experience a language barrier, might be less served then organisations with an international network.

With regards to DDPs approach, it is clear that DDPs values are very relevant in this field and that the right values are selected. Especially DDPs value of trust & confidentiality is deemed very important and it is acknowledged that the DDP staff strongly adheres to this principle. This give applicants the necessary trust to share personal information.

Conclusion

DDP stands out with a holistic approach which puts them “at the top of the pile” of present funders, as an expert framed. DDP seems to be trendsetting at two points. They played an important role in setting up a convening space, in particular for rapid responders. Second, DDPs acknowledgement that digital safety behaviour change of critical internet users is a lengthy process that takes time, and could be better addressed via a digital integrity fellowship was also innovative.

We can conclude that DDP has established a good portfolio of instruments to service both target groups of critical internet users and responders. Since DDP has rapidly grown from a grant facility to a portfolio with diverse interventions, our advice is to consolidate DDPs strategy and interventions, although some adaptions could be done to fit to existing needs.

1. INTRODUCTION

1.1. Introduction of Digital Defenders Partnership (DDP)

Internet freedom is under threat worldwide. Repressive governments across the world censor information of public interest, expand surveillance and crack down on privacy tools. Critical internet users such as bloggers, cyber-activists, journalists and human rights defenders are challenged in repressive environments. They face targeted hacking and DDoS attacks as well as mass surveillance and next generation censorship threats.

To protect these critical internet users and to keep the internet open and free, the Digital Defenders Partnership (DDP) was established in 2012 by the Freedom Online Coalition (FOC)[1]. By means of providing advice and (financial) support to individuals, DDP aims to increase safety for cyber activists under attack. In addition, DDP also aims to increase the capacity of the digital emergency response eco-system, referring to the combination of all the different players in this integrated mechanism of response. It does so by investing in key responders who provide services to critical internet users. Through that DDP aims to develop structural emergency response capacity, in order to provide rapid responses in case of (urgent) digital emergencies in repressive internet environments.

DDP's method of intervention is multifaceted: it invests in the safety of critical internet users not only by providing funds (granting), but also by providing services (linking & learning) (see Figure 1.1). It thereby differentiates between (short-term) responses in case of urgent emergencies, and structural (long-term) support by means of capacity building, such as the Digital Integrity Fellowship[2]. Since 2016, DDP has started a strategic partnership with three organisations, namely Media Legal Defence Initiative, Front Line Defenders and VirtualRoad. Each organisation fulfils a specific need within the digital emergency response ecosystem. A more elaborate description of the programme can be found in Chapter 3.

The programme is implemented by the Dutch-based INGO Hivos, and funded by six international donors: the US state department, the Ministries of Foreign Affairs of the Netherlands, Finland, Estonia, Latvia and the Swedish International Development Cooperation Agency (SIDA)[3].

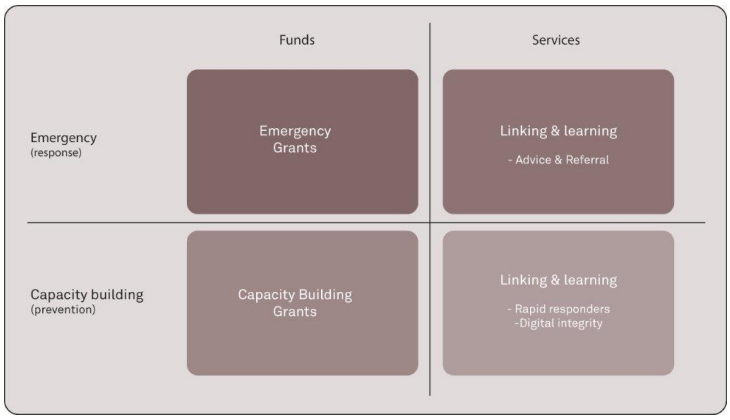

Figure 1.1. Types of investments in the safety of critical internet users by DDP

[1] The Freedom Online Coalition is a partnership of 30 governments, working to advance Internet freedom. Coalition members work closely together to coordinate their diplomatic efforts and engage with civil society and the private sector to support Internet freedom

[2] Digital security experts, called digital integrity fellows, provide comprehensive support to organisations under attack to build digital security expertise inside organization over the period of 6-8 months.

[3] In spring 2017, an additional donor, Department of Foreign Affairs Trade and Development Canada, started to support DDP.

1.2. Introduction of this study

DDP commissioned a mid-term evaluation to assess the effects of DDPs approach on critical internet users and the digital emergency response ecosystem as executed from the start of the programme in 2012 until now. This mid-term evaluation was conducted by evaluation experts of Kaleidos Research (the Netherlands) in collaboration with Dr. Ben Wagner, an expert on internet and human rights (Germany). Three local researchers assisted in conducting parts of the fieldwork: Gabriela Martínez Sainz (Mexico), Wairagala Wakabi (Uganda) and Oleg Kozlovsky (Russia).

The objective of this evaluation was two-sided, focussing on two key elements of creating greater accountability and fostering learning within the program. By doing so, the aim was to provide DDP with a knowledge base for identifying appropriate actions to address particular issues or problems in design, implementation and management of the programme, and to reinforce successful initiatives or approaches. Following these objectives, the leading question of this study was:

To what extent and how does DDPs multifaceted interventions and DDPs approach affect the digital emergency response ecosystem and critical internet users?

More specifically, the evaluation focused on five specific topics. An overview of all questions can be found in Table 1.1)

- The quality of the programme design
- Value of the programme according to participants
- Process
- Costs/benefits
- Learned lessons and recommendations

Table 1.1 Overview of sub research questions

1. Quality of programme design
How do the different DDP parts (granting and linking & learning interventions as described in ANNEX 3) interlink and contribute to increased safety & strengthened human rights for critical internet, and increased capacity of the global emergency response ecosystem?
How does DDPs approach contribute to increased safety & strengthened human rights for critical internet users and increased capacity of the global emergency response ecosystem?
How does DDP gear the work to actively include women? Is the target group defined enough?
To what extent are DDPs strategy, objectives, interventions, approach and choice of strategic partners still valid and appropriate to needs of critical internet users, emergency responders and the emergency response ecosystem? Are the activities and outputs of the programme consistent with the intended impacts and effects?
2. Value of outcomes to participants
How valuable were DDP outcomes to critical internet users, the emergency response ecosystem, the rapid response community, digital integrity organizations, donors, strategic partners? What has happened as a result of the program?
How do others (non-grantees, others in the response or internet freedom field) experience/recognize/value the DDP program, approach and interventions?
What are some of the stories that show the effects of the DDP program? What real difference has the activity made to the beneficiaries? What have beneficiaries done in terms of changing their behaviour so as to avoid or supersede the same threats after going through DDP or grantees interventions? And if they haven't changed anything, why is that?
3. Process
What enabled successful implementation and outcomes to occur? What barriers existed that led to less than successful implementation and outcomes?
4. Cost Benefit
Does the value of DDP outcomes outweigh the costs of implementation?
5. Lessons learned and recommendations
What are the lessons learned and recommendation regarding DDPs strategy, objectives, interventions, approach, choice of strategic partners and gender-dimension?
What are the recommendations regarding the DDPs log frame and monitoring of results?

2. METHODOLOGY

In this chapter, we will present the overall evaluation framework, which is based on a realist approach, as well as a mixed method approach that was used to answer the research questions.

Realist evaluation approach
This evaluation is theory-driven; we aimed to develop a programme theory that served as a base of this study. A good programme theory helps to capture the big, messy “real world” picture of a programme, with all the possible pathways leading to change, and the assumptions behind these pathways. A programme theory (Theory of Change) can be defined as a set of explicit assumptions about what action is required to solve the problem and why the problem will respond to this action. A clear view on the (assumed) causes of the problem and the underlying generative mechanisms, allows us to identify how DDP aims to intervene to address the problem. This information is essential to improve existing or future programs.

Mixed-method
To answer the research questions mentioned above, we opted for a mixed-method approach. By using a combination of different and complementary methods – including a documents analysis, an online survey and qualitative interviews - we were able to obtain a clear view of the functioning of the programme. Annex 1 provides an overview of all the research questions and the proposed research methods and provides insight in which research question is addressed by what method(s). It also shows the topics addressed per stakeholder.

- Document analysis

We started the evaluation with a desk study to gain insight into the set-up and implementation of the programme. We studied the available programme documentation, including programme plans, annual reports, programme documentation of grantees (like grantee plans and reports). The desk study also offered a starting point to identify topics and important stakeholders to be included in the study. The results were furthermore used for the development of research tools such as the online surveys and focus group discussions.

- Workshop with strategic partners

A full day workshop was held with the DDP team and strategic partners to collectively discuss a draft problem tree, a draft theory of change and to gain a better insight into the partners view of the programme and the collaboration between partners. Apart from four Hivos staff members, representatives of MLDI, Virtual Road and a Digital Integrity Fellow were present. The representative of Front Line Defenders was not able to join the workshop and was interviewed separately afterwards.

- Country studies

To get a good feeling of the impact of the programme and to study the effects of the DDP in local settings we conducted case studies in three countries: Mexico, Russia and Uganda. The countries were selected by Hivos and represent three different world regions where the programme is active. Apart from the region, another important selection criterium was the presence of different DDP interventions in that country.

Three local researchers familiar in digital safety and/or human rights conducted the fieldwork in the three countries. In Mexico, the local researcher with a background in human rights was supported by a local expert on digital safety in the research process. The local researchers conducted seven (and in one country eight) interviews in the local language for each country case study. In total 22 interviews were collected. The notes from each interview were written out in English. The interviewees represent three different types of stakeholders: direct DDP beneficiaries (critical internet users and responders),

indirect beneficiaries (for example human right activists who have been supported by DDPs strategic partners) and external stakeholders and/or experts on the local digital safety context and not connected to the programme. The selection of the interviewees was made with the help DDP staff members and DDPs strategic partners. The local experts were identified by the local researchers. Stories of change, authentic narratives that are told by beneficiaries about the change that has taken place due to the programme, were collected during the interviews with the beneficiaries. These stories gave insight into how beneficiaries perceive the effect and added value of the programme in their organisation or work. The stories provided a rich picture of the influencing factors and enabling conditions that have led to the described changes. A generic guideline for interviews with (indirect) beneficiaries and a guideline for the local expert interviews are presented in Annex 2 and Annex 3.

The findings of each country are presented in three confidential case study reports that illustrate how the programme effected critical internet users in that country and helped to identify enabling and constraining factors and strengths and weaknesses of the programme.

- Additional qualitative fieldwork

Apart from the 22 interviews by local researchers in the three case study countries, 6 additional interviews with donors, Digital Integrity Fellows and an expert were conducted by the evaluation team. In addition, the three DDP staff members were interviewed separately. Also, two focus group discussions were conducted. The first focus groups discussion included four members of the Rapid Response Network with the objective to discuss the design and value of the programme and the impact of the Rapid Response Network on their work. In the second focus group discussion, three experts/DDP outsiders gave their view on DDP. Most of the data was collected face-to-face during the Global Internet Freedom Festival March 2017 in Valencia, Spain. Other interviews were conducted face-to-face or through jitsi, that enables secure video calls. An overview of all the qualitative fieldwork can be found in table 2.1

Table 2.1 Overview qualitative fieldwork.

Types of stakeholders	In-depth interviews	FGD	Workshop
Full-day Workshop with strategic partners			1
Direct beneficiaries: Critical internet users (including organizations that received digital integrity support)	5*		
Direct beneficiaries: The emergency response ecosystem	3*		
Indirect beneficiaries: critical internet users who are served by strategic partners or responders (grantees of the program)	8*		
Local external stakeholders	7*		
Digital integrity fellows	2		
Donors	3		
The rapid response community		1	
External stakeholders and experts		1	
Interviews with DDP staff	3		

* Interviewed by a local researcher

- Online surveys

To obtain the opinion and feedback of beneficiaries in those countries that were not represented in the three selected country studies, two online surveys were developed for DDP grantees; one for critical internet users and one for responders. The questionnaires were to a large extent similar, so most of the results could be compared. To protect the safety of the respondents, all necessary security measures were taken into account. The self-hosted survey via Greenhost.nl used the open source web application Lime Survey and HTTPs encryption. The survey was completely anonymous and no questions were asked that could lead to the identification of the respondent. DDP supported 70

grantees between 2012 and 2016, but only 30 grantees were invited for the survey. The reason for this difference is multifold. Firstly, the DDP has given multiple grants to the same organisations; one survey was send to cover different grants. In some cases, there was no contact person to fill out the survey available: for example, in cases where the person responsible for the grant left the organisation and no other staff member could give the feedback needed. Also, some of the grants concerned technical projects, which are not supported anymore by DDP. These organisations were not invited for the survey, since the questions in the survey would not be relevant for them. Unfortunately, the response rate was poor among both critical internet users and responders. Despite different reminders, out of a total of 30 invitations, we collected a total of 10 completed surveys; 6 among critical internet users and 4 among responders. In addition, there were 6 incomplete surveys that were not taken into account. Because of the poor response rate, the data was to a lesser extent used in this report, but mainly employed to validate the qualitative data.

3. DESCRIPTION OF THE PROGRAMME

This chapter clarifies and summarizes DDPs programme design and the strategies.

Key conclusions

- DDP focuses on incidental emergency response, on sustainable and holistic emergency response and on improving the digital response eco-system that supports critical internet users under threat.
- All individual interventions are logically linked to the aims of the programme.
- A visual presentation of the Theory of Change (see Figure 3.1) was developed as part of this evaluation to provide a clear overview of the different activities in relation to the outcomes of the programme.

1. Programme design
How do the different DDP parts (granting and linking & learning interventions as described in ANNEX 3) interlink?

Box 3.1 The problem tree

As part of the evaluation, a problem tree was developed to study the central problem that DDP is aiming to address (i.e. critical internet users that are hindered by digital threats in their work to voice their rights). Based on a draft developed by the evaluators, the problem tree was discussed by participants of the participatory workshop and it was adapted to make it more in line with the programme as perceived by the strategic partners (Figure 1). A clear view on the causes of the problem allows to identify how DDP aims to intervene to address the problem.

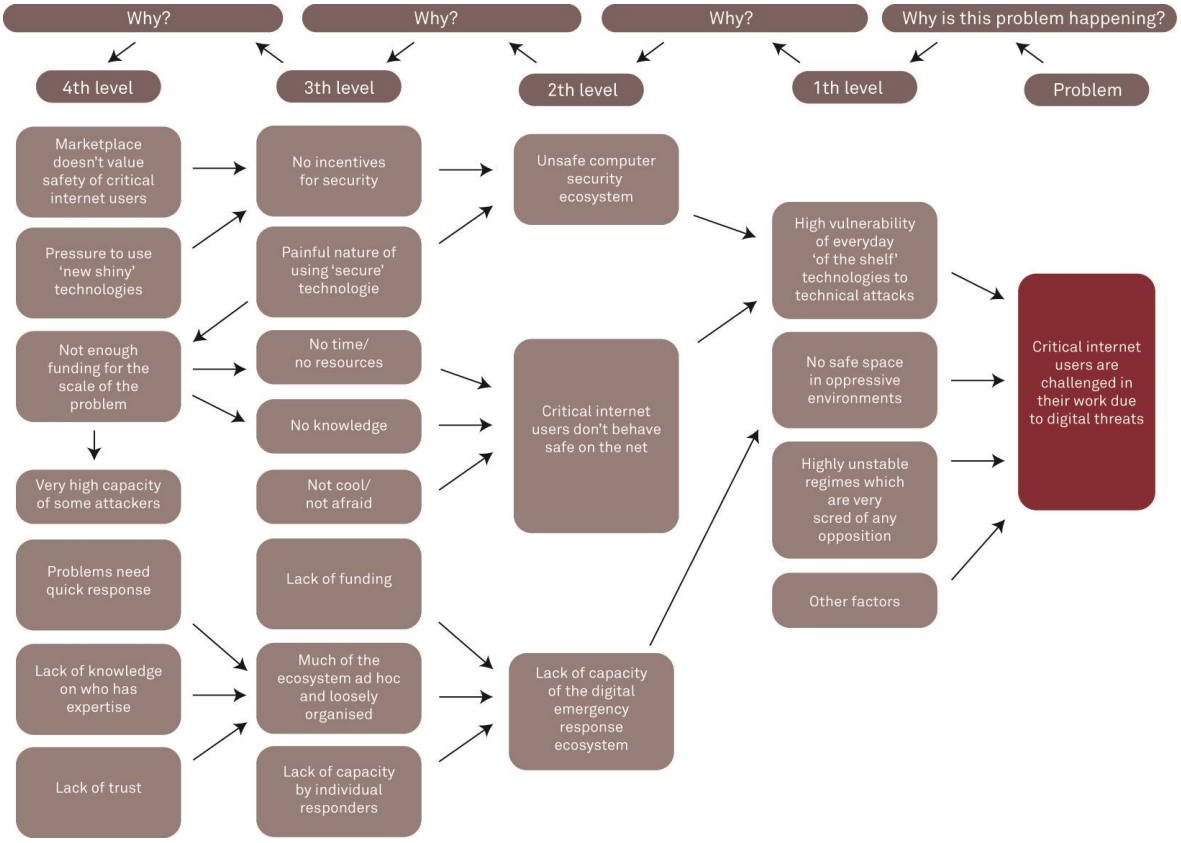

Figure 3.1 Problem tree of DDP that gives insight into the central problem DDP is addressing

DDP aims to contribute to solving the problem of human right defenders that are hindered in their work because of digital threats. High vulnerability of everyday technologies, no safe space in oppressive environments and unstable regimes that do not allow any opposition, are – apart from other major causes - factors leading to this problem. DDP

mainly intervenes on this problem by supporting and stimulating critical internet users to behave safer, although only when users are under attack (and not preventative). In addition, it aims to improve the digital emergency response eco-system. Looking at the entire problem tree, DDP responds to particular elements of the causes of the problem. DDP does not address the role of the companies that deliver unsafe' technologies, nor is it advocating for space in oppressive environments or working preventatively to raise awareness under critical internet users to behave safer. As DDPs central problem has multiple causes, it is evident that a relatively small programme as DDP is only able to focus on specific elements and cannot involve all the factors contributing to the central problem.

3.1. DDPs strategies: granting and linking &learning

This paragraph provides an overview of DDPs strategies, including information on how the interventions were implemented in 2016.

A. Granting

Table 3.1 provides an overview of the different grants provided by DDP. Incidental emergency grants are provided for critical internet users in an urgent emergency situation. Sustainable grants are provided for critical internet users under attack to find long term solutions for their situation. DDP also invest in responders via capacity building grants to equip them in serving critical internet users.

As from 2016, DDP has started a strategic partnership with three organisations to establish an integrated, holistic response mechanism. Each organisation - Media Legal Defence Initiative (legal defence), Front Line Defenders (regional/physical safety) and VirtualRoad, (infrastructural responses) - fulfils a specific need within the digital emergency response ecosystem. The partners each receive a strategic grant to provide quick, holistic emergency response. Although this grant is given to responders, the actual beneficiaries are the critical internet users that receive emergency assistance. Working with selected and trusted partners secures a high-quality response.

Table 3.1 Overview DDP grants

Target group	Type	Description	Budget allocation in 2016	Amount of awarded grants in 2016
Critical internet users	Emergency grants (incidental) max 10,000 USD	Mitigating consequences and damage of attacks, and enable critical internet users to continue their activities.	43.831	11
	Emergency Grants (sustainable response): max 50,000 USD.	A sustainable response to organizations under attack, when incidence response is not sufficient or would leave irresponsible security vulnerabilities	113.747	8
Responders	Capacity building grants 20,000 –250,000 USD	Invest in capacity building of responders to be able to provide emergency response.	389.643	5
	Strategic grants 200,000 USD annually	Individual partners provide different types of (emergency) responses as, legal defence, regional/physical safety and infrastructural responses.	482.857	3

In 2016, 67 application were submitted and 27 grants were awarded; two third of the applications could not be granted. Most grants were given to incidental emergency support, however overall this was a relatively small post. Table 3.1 includes a budget allocation of 2016 showing that the largest sum was spent on the strategic partners, who - through this grant - supported many critical internet users. With support of DDP, VR hosted in 2016 44 media or human right sites, with the five largest sites attracting 4,3 million visitors a month. FLD supported 112 individual HRDs and 168 organisations (725 HRD's) in 2016 with DDPs support. And lastly, through DDPs strategic grant MLDI was enabled

to give legal defence to 5 new cases of online bloggers, HRDs or journalists, concluding 2 cases and whilst 20 cases were still ongoing.

B. Linking and learning

Rapid Response Network
At the end 2013, Global Rapid Response Network (RaReNet) was established by the DDP to increase cooperation between responders. This closed network consists of a group of digital safety and security experts and some civil society members, who combine their expertise and support each other to better deal with the different kinds of attacks. Currently, in total, 24 members from 15 organisations are part of the network. Apart from sharing knowledge about threats via an email list, responders meet twice a year to discuss and share lessons learned. DDP, as a neutral player, has a supportive and facilitating role in this network. Apart from the global network, regional meetups were organised in collaboration with regional partners in South-East Asia and Ukraine (2014), the post-Soviet region (in 2015) and Central America (in 2016). Also, a mail list for responders has been established in the Middle East and North Africa region.

Besides the value of the network for responders, DDP staff also benefits directly from this network. It helps the staff to obtain an overview of the relevant issues in the field, to keep track of developments in the responder field as well as different threats and mitigation in different contexts. This information helps DDP staff to assist and mentor grantees to adapt the programme to the needs and developments in the field.

Digital Integrity Fellowship
The Digital Integrity Fellowship (DIF) was initiated in 2015 to provide sustainable, holistic safety and security support for organizations under threat. The digital integrity fellows provide comprehensive support to organisations under attack to build (digital) security expertise inside organization over the period of 6-8 months. An employee within the organisation, the digital integrity champion, is selected to assist this process from within the organisation. Management commitment is found to be very important to make the fellowship effective and this is an important selection criteria. The DIF is one of the more innovative means of DDP. An important reason for the set-up of this long-term intervention, was the notion that in many cases stand-alone solutions, such as digital safety trainings, did not lead to sustainable and organisational digital safety changes. In 2016, 12 organisations were supported by 5 fellows.

Digital First Aid Kit
The Digital First Aid Kit provides preliminary support for human rights defenders, bloggers, activists and journalists facing the most common types of digital threats, offering a set of self-diagnostic tools for attacks, as well as providing guidelines for digital first responders to assist a person under threat. The guide is a joint creation by members of the Rapid Response Network, supported by DDP. This reference for responders and end-users is a (well-developed) beta-version, that can be consulted via a website. In 2016, the DFAK was consulted by 2005 visitors.

Advice & Referral
DDP also has a brokering role by referring people with certain needs to those who might be able to help them. In 2016, DDP supplied 25 advice & referrals to critical internet users; this was less than the output target for 2016 of 50 cases.

Box 3.2 Donor relations

Currently, DDP is supported by 7 donor countries. Based on the 3 interviews with representatives of 3 separate donor countries conducted for this evaluation, it can be concluded that donors have different wishes with regards to DDPs focus and that the length of support and size of budget varies significantly among donors. Especially the shorter arrangements threaten the sustainability and implementation of the program; a large chunk of DDPs man-hours is spend on proposal writing and at the start of 2016 some activities were put on hold (Capacity Building Grant, the Sustainable Emergency Grant and Digital Integrity Fellowships) and smaller grants were supplied to the strategic partners due to funding insecurities.

Donors are informed about DDPs progress through quarterly and annual reports. Each spring, the annual report and plan is presented at a DDP donor meeting. Donors feel that the DDP fulfils the reporting requirements, although it donors value different parts of the information and have different wishes with regards to information sharing. For example, one donor feels that DDP is reporting too much and prefers not to receive the confidential annexes, as these can be requested by outsiders; another prefers these confidential annexes as way of threat sharing information and wonders if this could not be increased to a higher but more informal level. Each donor has different reporting requirements where their grantees need to adhere, leading to a relatively large part of staff time spent on reporting.

3.2. Visual presentation of DDPs theory of change

DDP has an elaborate log frame, structuring the outcomes the programme it is aiming for, which helps to monitor programme implementation. However, a log frame is less suitable to capture the big, messy "real world" picture, with all the possible pathways leading to change, and the assumptions behind these pathways. An important step in this evaluation was therefore to make the Theory of Change (ToC) of DDP more explicit. A ToC can be described as "the process through which it is expected that inputs will be converted to expected outputs, outcome and impact" or, in other words, a "set of assumptions that explain both the steps that lead to the long-term goal and the connections between programme activities and outcomes that occur at each step of the way". Hence, a ToC articulates the theories and assumptions which underpin the anticipated change process, and provides the supporting evidence. A ToC often combines a 'simple' visual presentation which quickly communicates the theory to all audiences and a more detailed narrative that does justice to the complexity of the programme and explores the assumptions and evidence that underpin it. The ToC should also be consistent with the logical framework of the programme. In this evaluation, we focused on developing the visual presentation on the Theory of Change, that can be used by the DDP team to adapt and develop the narrative that goes along with it. This visual presentation makes it clear how the different DDP parts interlink with each other.

DDP started off as a grant facility, but through the years' different elements that seemed necessary to reach the aim of improving the safety of digital internet users have been organically added alongside the grant facility. Apart from the granting facility with emergency and more sustainable support, DDP now works with strategic partners and provides linking and learning facilities, like the Rapid Response Network and the Digital Integrity Fellowship. As becomes clear from the visual presentation, DDP contains a wide range of activities. Donors and experts, but also grantees seem sometimes slightly confused by DDPs diverse strategies. For example, a donor: *"The response network, sustainable grants, strategic grants, all those things make sense but when you are trying to explain, it is difficult. It is a challenge to understand all aspects and how they fit."* A clear theory of change and a well worked out narrative could help DDPs stakeholders to get a better overview of DDPs work.

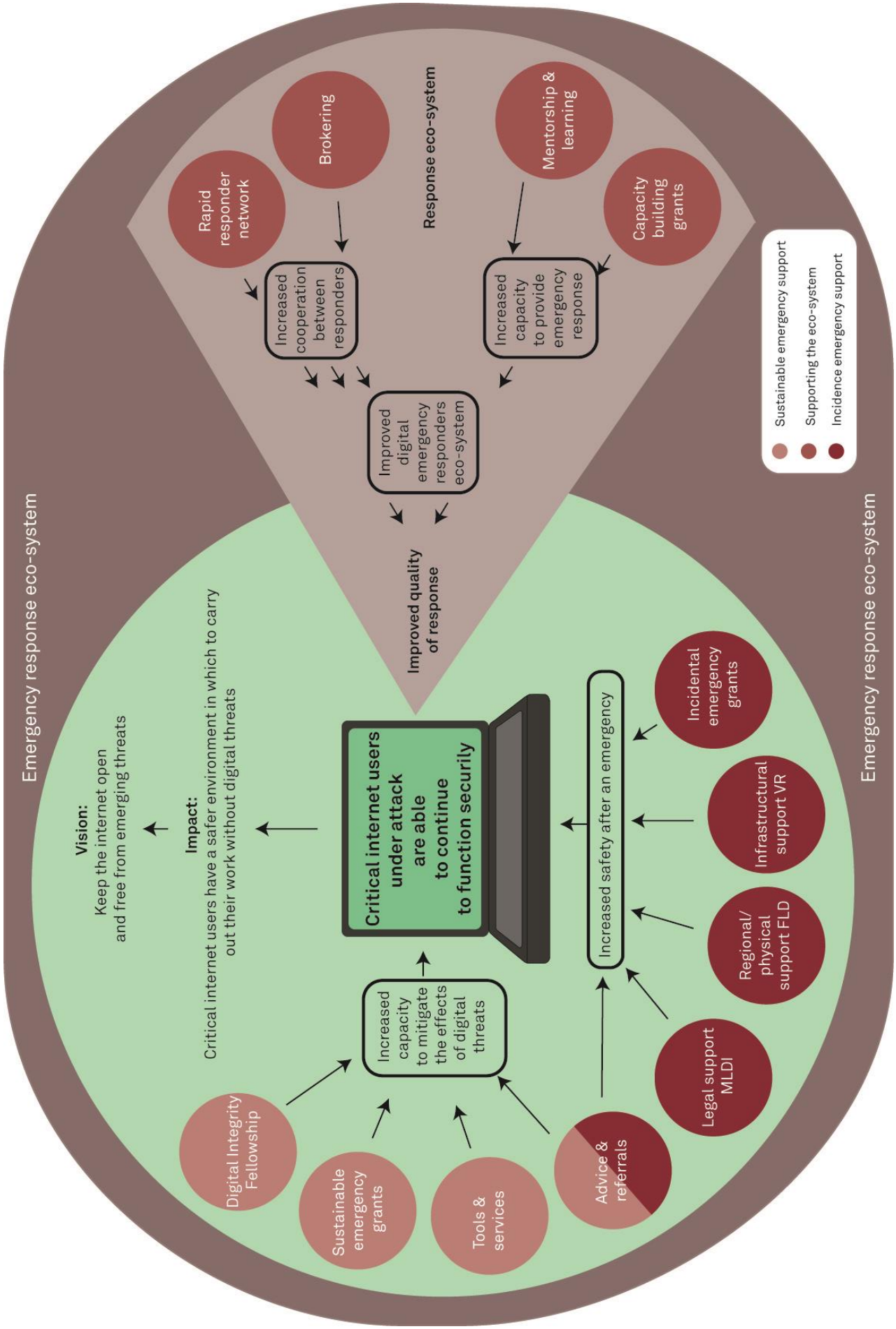

Figure 3.2 Visual image of the Theory of Change

From a Theory of Change perspective, interventions should be categorized by the (intermediate) outcome they are aiming for, rather than the types of activity. When looking at DDPs interventions, it can be concluded that DDP comprises three different types of interventions, each type aiming for particular intermediate outcomes. The first group of interventions is focused on incidental emergency: tools like the incidental emergency grant, the support of the three strategic partners and some of the advice & referrals DDP provides. The second group of interventions contains sustainable emergency support, such as the digital integrity fellowship, the sustainable emergency grants and tools like the Digital First Aid Kit. The third group of interventions aims to enhance the digital emergency response eco-system, in order to improve the quality of response towards critical internet users.

4. OUTCOMES OF DDP

In this chapter, the assessment and value of the DDP outcomes from the perspectives of all involved stakeholders will be discussed, followed by a reflection on the benefits relating to the costs of the programme.

Key conclusions

- All stakeholders linked to the programme assess outcomes of DDP as valuable and positive.
- DDP has a clear impact on the critical internet users they reach.
- Grants and support lead in many cases to sustainable change, in particular interventions with a more sustainable character, although in many cases more needs evolve.
- There are still barriers for critical internet users to change organisational behaviour with regards to digital safety.

2. Value of outcomes to participants
How valuable were DDP outcomes to critical internet users, the emergency response ecosystem, the rapid response community, digital integrity organizations, donors and strategic partners? What has happened as a result of the program?
How do others (non-grantees, others in the response or internet freedom field) experience/recognize/value the DDP program, approach and interventions?
What are some of the stories that show the effects of the DDP program? What real difference has the activity made to the beneficiaries? What have beneficiaries done in terms of changing their behaviour so as to avoid or supersede the same threats after going through DDP or grantees interventions? And if they haven't changed anything, why is that?
Does the value of DDP outcomes outweigh the costs of implementation?

4.1. Value of DDP outcomes

The different support mechanism of DDP have a clear impact on critical internet users and responders. In each of the sub sections below, the value of the outcomes of DDP for each stakeholder – critical internet users, responders, RaReNet members, donors and DDP outsiders/experts will be discussed in more detail.

4.1.1. Critical internet users

DDP tools: incidental and sustainable emergency grants, Digital Integrity Fellowship, indirect beneficiary via strategic partners, DFAK

"The support received by the DDP has changed the organisational culture completely. Nowadays all the information and risks analysis conducted by our members including details from the organizations they work with, are shared via secure channels –i.e. all the emails are exchanged and hard drives are encrypted. These practices have increased the sense of security and made our work more efficient despite the long distances within the country."

DDP implements several interventions to support critical internet users (see above). All these tools seem to positively influence the critical internet users, although organisations that received long term support (via the digital integrity fellowship or by receiving a sustainable emergency grant) report more behavioural and organisational changes compared to organisations receiving incidental support as

they had time to adopt practices and develop protocols over time[4]. In addition, the critical internet users more at-risk were more inclined to change their digital safety practises. In half of the cases, critical internet users felt that the support given was not a quick fix, but led to sustainable changes. The incidental emergency grants made it possible to address an immediate problem, for example by buying new equipment after being robbed or setting up a safe internal network. Of the 13 critical internet users that were interviewed, only 1 respondent reported that the impact of DDPs support was limited. An indirect beneficiary receiving support of one of the strategic partners complained that the financial support was not sufficient to set up a litigation cause; the legal ground work where the budget was spent on, was not fully used. And from DDP documentation and qualitative research findings (an interview with a fellow), another case was mentioned where the digital fellowship did not have impact, because the champion had to flee out of the country and the work that was built up, could not be continued.

Important results

An important first outcome valued by many critical internet users, was an increased level of awareness of security threats. *"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."* As one grantee pointed out, this increased knowledge about security threats was accompanies with more feelings of insecurity. *"But it is better to be aware of the threats than to remain ignorant and happy."*

A second outcome mentioned by critical internet users is that they are working more digitally safe then before, as they increased their knowledge and improved their digital skills. The beneficiaries learned to make use of different key security tools, such as surveillance cameras, anti-virus software and passwords. Some have also installed security applications in their mobile phones and learned how to send and receive encrypted emails. This is confirmed by the survey data; the 6 critical internet users that filled in the survey, assessed their organisational digital safety skills after the DDP programme with a 7 out of a 10 points scale, while at the start they assessed it with a score of 3,5. In the survey, a critical internet user receiving a sustainable emergency grant explained: *"We have achieved a shift in our organizational culture, in which digital security is no longer a mysterious or scary thing, but rather something we can talk about and work to improve together. Without this, trainings and tools can't have much impact. We're very grateful that we've come this far."*

And as a third outcome, the support, and particularly the sustainable emergency support, did not only impacted the beneficiaries, but in some cases also the people and organisations they collaborated with. With the acquired knowledge, beneficiaries set security standards for information management and communication within their network. One grantee receiving an incidental emergency grant passed on the skills and practices he acquired. *"Whenever I go to member organisations I give security tips to their staff. I have trained 15 individuals from four organisations in our network."* (See also Box 5.4)

Another grantee explained that his organisation has offered advice on safety issues to some journalists, and they also developed protocols on security focusing on dealing with sensitive information and sources relating to their target groups. So, the programme impacts on the individual and organizational level, but also the level beyond; the community around the critical internet users. According to another beneficiary the delivered support offered by a strategic partner was also an opportunity to develop relationships and partnerships with other organisations and individuals. As a grantee of a sustainable emergency grant via the survey points out: *"The work on security has become one of the main programmatic themes in our work. We incorporated this framework with*

[4] In total, 13 critical internet users were interviewed, that received support of DDP; directly via a grant, or indirectly via a strategic partner or responder. In addition, 6 critical internet users filled in the survey.

support of DDP. We believe the focus on security is actually one of the greatest impact areas for our cause and network partners. Improved security leads to empowerment. Empowerment brings more activism."

Barriers and limitations

Even though critical internet users value the grant and its outcomes, several respondents point to different barriers they face to change their behaviour, making it difficult to adhere to digital safety procedures in some cases. For example, safe tools that are not user friendly or cause problems with other software, or the need to use unsafe social media to reach an audience as part of their human rights work. An overview on these barriers is provided in Box 5.1 in Chapter 5.

Another limitation that is mentioned is the global scope of the strategic partners or responders DDP works with. Some beneficiaries prefer to collaborate with locally based responders/fellows instead of strategic partners or fellows that are not based in their country or region. Locally based responders/ fellows can be easier reached to offer advice over a longer period of time at shorter notice and can also provide follow up to check on the implementation of the advice given.

Respondents also point out that in many cases the support of DDP was insufficient to meet the organisational needs. Different grantees point to the fact that new needs continue to emerge. "*New threats appear all the time. Attack on telephones are now done differently than 3 years ago. You need to be trained regularly to catch up with these changes."*

And lastly, some critical internet users referred at the limitations of the programme. In some countries, the needs are so high, that a strong support network is needed, as an incidental emergency grantee via the survey pointed out: "*In countries with continuous emergency situations, it would be better for creating a team in every country to work daily and execute many activities such as training sessions for example every month, 24-hour online help and support for defenders, and if it is possible translating many guides and lessons to local languages."*

Box 4.1 Story of change: Digital Integrity Fellowship

Four years ago, we started a network of female HRDs in our region. When we got some successes, for example a woman becoming municipal president of the town, our members became a threat to male powers and attacks started. Women were using technology to document problems in the community and slowly we realized that this was a weak spot: cell phones and laptops were stolen, and a smear campaign was set up against a female journalist who was covering political issues. In the beginning, we were not even aware that these were organized attacks. The network now has a registry of security incidents and at least one third of the incidents has a 'digital component'. Particularly smear campaigns via social media are very destructive; once a woman has been attacked through social media and her character is questioned by the community, all her previous work and efforts are questioned.

We knew the Digital Integrity Fellow via our network and this was key to be able to trust him. We were under attack but had no idea how to protect ourselves, what was needed or what kind of tools were available. The fellow delivered workshops on digital security for our women defenders in the network: one initial face-to-face, some online workshops and another face-to-face session at the end. The face-to-face workshops were particularly helpful, more than the online sessions. Alongside, the fellow supported the champions of the network via emails and jitsi calls to make sure we could handle all the questions from our members. The fact that the fellow was based in another region and in a different time zone made practical coordination sometimes difficult.

The impact of the support on each of our members is hard to tell, but our network surely benefited from the fellowship. All participants of the workshop installed security applications in their mobile phones including encrypted emails. So far, these tools are still used by these members, although more follow up is needed for members that were not present during the workshops. Another clear change is the organisation of monthly clinics on digital security for our members to address individual questions. The fellowship raised awareness among our members about digital safety and gave us the knowledge and digital skills to keep our work and ourselves safe. It also helped us to develop relationships with other organisations that can support us in this journey.

Side note: An additional success of this case study is the fact that the (female) champion of this network was promoted to become fellow of the Digital Integrity Fellowship to support other organizations in digital safety.

4.1.2. Responders

DDP tools: capacity building grant, DFAK

"We were able to start programming in responding to huge gaps in information security of NGOs and insufficient responses from other actors. We changed our programme to address it."

Important results

The three interviewed responders that received a grant, agree that the level of awareness of digital security threats – including their own - has increased because of the capacity building grant. They used the grant to deliver tools and software to partner organisations and individuals at high risk who lack awareness and knowledge of digital security threats. They also trained their beneficiaries how to protect themselves. The responders themselves also got a better view on the existing problems and challenges within the network they support. One responder said they adjusted their support programme after receiving the grant and the training. *"We started with some assumptions, then we learned much more from experience."*

Like the critical internet users, the interviewed responders also point to barriers for digital safety behaviour; they experienced some resistance when supporting critical internet users (see also Box 5.1 Barriers for digital safety practices). These barriers hinder the impact of their work. For that reason, responders seem to believe in more long term solutions that aim to tackle these barriers more in-depth, in addition to incidental support. They stress the importance of both support mechanisms by DDP. *"Emergency support is important. But if people are not taught how to work safely, no funding will be enough for all the emergencies."*

Barriers and limitations

Responders are slightly more critical on two issues. First, although grateful for the grant received, they pointed out that the support was insufficient to meet all the existing needs. Addressing all the security needs in the region would require a lot more (structural) funding. *"We need a fundamental understanding of organizational change. We have learned a lot, but still have much to do in this regard. Different forms of organizations beyond classic NGOs are becoming more common requiring other forms of support. How do we provide those groups with what they need to stay safe?"*

Secondly, the existing digital emergency ecosystem as a whole lacks capacity, which wasn't addressed through the capacity building grant. Service providers are not used to working together or share information on what they do. However, as one responder indicated: while the grant was insufficient to build the capacity of the digital emergency ecosystem, DDPs support did work as an 'eye-opener' on the importance of this digital eco-system to improve the response. To expand and improve the network of digital experts in the country, the responder initiated a Digital Security Alliance in the country (see also Box 4.2 below).

Box 4.2 Story of change: capacity building grant for a responder

We work on the security and protection of human rights defenders (HRDs). They face multiple risks, such as intimidation, harassment and office burglaries. As a result, people fear to raise their voice. These HRDs organisations are at high risk, but lack the knowledge to protect their digital information and they need genuine equipment and tools, like anti-virus software and licensed operating systems. We used the DDP capacity building grant to deliver tools and software to these HRD organisations. We also trained more than 30 HRDs in the use of digital security tools. We gave out more than 80 antivirus software, thereby increasing organisational security. As a result, their level of awareness of digital security threats increased.

Because of the grant and the training, we now have a much better understanding of the digital security challenges faced by HRDs. The grant also helped us and the participants to get to know more service providers in the digital security area, so we and they know who to contact in case of an emergency. The participants of our training (and ourselves) are now able to communicate in a

secure manner, giving them confidence to do their work in a secure way and helping them to fight for their rights

The grant was insufficient to meet all the existing needs, for example computer locks, genuine software etc. and did not influence the capacity of the digital emergency ecosystem. We realised that this was indeed a gap and that there is a need for coordination. As a spin-off, we are now setting up a Digital Security Alliance with financial support of another fund. Because of DDP, we became aware of the variety of organisations that deal with digital security. We took the initiative to bring these organisations together to coordinate the work of various actors. By working together and sharing information, the safety of the digital emergency ecosystem as a whole will be increased.

The beauty of the DDP is that the staff of DDP keep in touch after giving the grant. They make reminders on when to submit the report a month before it is due and they have specific reporting regulations. They want to hear about impact. When we started implementing, we were not too good with (reporting) impact of the programme, but we have gradually improved. They're really in touch.

4.1.3. Rapid Response Network members

DDP tools: global rapid responder network, regional rapid responder meetups

"RaReNet provides a dedicated, safe and trusted space where we can share very sensitive information. It also serves as a referral network."

Important results

The four rapid responders that are part of RaReNet and were interviewed during a focus group discussion, feel a distinct result of RaReNet on their work. DDP staff and rapid responders agree that there is more coordination and collaboration between rapid responders compared to before this network was set up. Responders mention different added values of the network. They already collaborated incidentally through work cases, but in the Rapid Response meetings they can discuss more strategically how to collaborate, for example on threat sharing and monitoring. Through the built-up trust, they now share knowledge and resources. In the last meeting for example, they tried to jointly share and develop templates on internet blocking and account hacks. In addition, the vetting of grants is easier and quicker, because trusted partners can backup applicants. Another important aspect of the collaboration is the improved quality of the response. A responder: *"Trust is very sensitive, to build trust takes a long time and a lot of resources. Through the regional networks of RaReNet, the quality of our response improves. 3 or 4 people are not able to cover a region, but by linking up you can cover a larger area and refer to specific expertise of other members."*

Barriers and limitations

Global RaReNet members stress the importance of this network for their work, but at the same time emphasize it is difficult for them to spend time on the network, due to their own work strain. A responder says: A*fter the meeting, we promised to do stuff, but we are all overloaded. If I don't get it done during a meeting, it won't happen"* And another responder "*Threat information sharing is useful, but to do it properly, you need to analyse the data, which takes time and that is an issue."* Although the network has added value according to the network members, they are still discussing what its focus should be and who should be a member. When the network started, it was a new and interesting step for many responders, but currently, the network seems to have less momentum then 3 years ago. Members might already collaborate with each other outside the network, and because relationships are established through the network, it is easy to connect each other outside the formal network meetings.

The last global rapid response meeting in 2016 was however very valuable, and it was much appreciated that DDP took the organisational lead as members themselves don't have sufficient time. Responders feel that the network could benefit from appointing a community manager and feel that

there is sufficient trust with DDP to allow DDP to take a stronger role in supporting the network, or to financially support staff at one of the RaReNet members to take up a role as community manager.

Rapid responders feel that the network could eventually also work more towards long-term solutions and try to solve the problems where they start, at the large IT companies. When responders join forces, they have more mandate to negotiate as a united front with companies like TechSoup for licenses, Facebook, Microsoft etc. Responders already discuss this between each other on an ad-hoc base, but this issue could also be taken up in a more structured way.

Although the responders value each other's role in the response eco-system, the evaluation team also noticed some implicit organisational tensions between responders due to competition for funding or wish for increasing their visibility in the field. Although individuals - and not organisations - are members of the network, individuals still take these organisational interests along in meetings. DDP has a more neutral role, but it also still requires a finely balanced approach to deal with this.

There is strong regional interest this type of network; global RaReNet members mention that local responders are interested in the lessons learned from the network. They feel that RaReNet could provide a blueprint of their work, so other groups can use this format for their own regional community. One of the interviewed regional responders, took part in the regional rapid response network and really appreciated the network building event: *"1,5 years ago DDP facilitated a meeting of people who worked on digital security. It was a fascinating exchange, it led to further engagements and communication. It helped us expand and strengthen our network of partners in the region."* It seems however, that the regional meetups have a more ad hoc character, while most local responders feel a need for structural network facilitation. Also, not all regional networks flourish; for example, a network in South East Asia stopped because of the lack of a shared language.

4.1.4. Strategic partners, including the digital integrity fellows

DDP tools: strategic grants, financial support for digital integrity fellows

"W*e often support emergency cases before we know whether that particular action gets funded. The turnaround of many other grant mechanism is at least 3 days. In many cases, we need to take immediate action, and DDPs funding allows us to do this. It makes us more flexible and faster."*

The strategic partners value DDP very much because of the trust given by DDP and the long-term support they receive through the program, which in turn increases the sustainability of their own organisation. It decreases time spend on fund raising and gives them more resources to help those in need. The liaison with DDP also gives more credibility to the strategic partners. A partner: "*you don't have to discuss with your grantees whether you might actually work for the CIA."* They also feel that DDP, as a grant mechanism, is more flexible than other programs, and indeed 'partners with the partner' "*It is not jumping through funders' hoops, DDP is really collaborative."* Three strategic partners and a digital integrity fellow that filled in the survey, all agree that due to the Digital Defenders Partnership program, their network with other responders has been enlarged and that trust between responders has increased.

Although the strategic partners feel very much valued by DDP staff, they feel to a lesser extent responsible for or part of DDP; they seem to view the grant more as a way of support their organisation and seem to feel less part of DDP themselves. There is a tension in the roles of strategic partners, in particular in regard to whether they are considered stakeholders, partners, implementing organisations or grantees. The position of digital integrity fellows is slightly different than the other strategic partners. Their work would not exist if it was not for DDP, so they have a stronger ownership to make the fellowship work, and feel more part of DDP as an entity. As a Digital Integrity Fellow

reflects in the survey: *"The ability to finally move beyond the dependence on training in digital security for HRDs was extremely valuable. DDP had faith in the idea of the fellowship and opened up to trying something quite radical and new. They have had great trust in us and allowed us to develop the methodology as we progress, while often offering useful input along the way. The space created by DDP was a key enabler. They have done a great service to the community, but the intervention needs to be made sustainable."*

The strategic partners agree that the partners fit well together and to DDP, because they all have a similar approach that reflects the nature of DDP. DDP stands out compared to other grants, because it is not about tools or processes, but focusses on empowering individuals. A strategic partner: *"Among DDP partners, we share a belief that an individual has the capability, but needs to be empowered to use it. It has to be about the person, not just the process or the tool."* Another characteristic of DDP is that it is taking a sustainable and holistic approach and that it is needs-based and focused. The partners assess DDP as quite effective, although each of them agrees that DDPs ambitions are much larger than the budget, which is one of the main barriers to achieving impact.

Despite the general appreciation of DDP, partners feel that the partnership could be improved, as was discussed during the workshop with DDP staff and the partners. Strategic partners developed a strong relationship based on trust with DDP staff, however to a lesser extent they developed this with the other partners. One of the strategic partners: *"There are no structured bridges between the strategic partners. And the physical distance between the partners is a barrier, making collaboration difficult. We don't see each other that often."*

All partners express the wish for more collaboration and feel there should be more regular meetings between the partners to explore how the collaboration could be improved. Referral or sharing of practices between partners seems to happen mainly through DDP staff, the partners themselves are less frequently in contact with each other. One of the partners suggested making the partnership more formal, with for example a Memorandum of Understanding with agreements on preferred ways of partnering. It is not clear if this is a shared view, but it would be advisable to jointly explore how the partnership could be improved. More work is needed to establish a genuine partnership in which all members participate.

4.1.5. Donors

"I asses the DDP outcomes as positive. DDP maintains a good balance between emergency and sustainability, the staff collaborates in harmony with similar players, and importantly for us: they feedback trends and signals to our ministry. The DDP programme are our eyes and ears, delivering information on what is happening in the world with regards to digital emergencies."

DDP is currently funded by seven international donors: the US state department, the Ministries of Foreign Affairs of the Netherlands, Finland, Estonia, Latvia, the Swedish International Development Cooperation Agency (SIDA) and Department of Foreign Affairs Trade and Development Canada. The three donors that were interviewed for this evaluation are motivated to support DDP because digital safety is an important aspect of their overall support to human right defenders. Digital safety is a growing concern, as many incidents show that digital attacks can be very effective to stop human right defenders. Two donors mention that in the future, digital safety might be integrated and mainstreamed in human right programs, which might lead to a decrease of funding of digital safety as such.

Donors associate DDP mostly with incidental emergency support. They mention this as the main feature of the programme. More sustainable interventions like capacity building grants for responders and the digital integrity fellowship are not mentioned spontaneously, although two donors also emphasize that they value the combination of incidental emergency support with a more sustainable

long term approach. In general, donors are positive about the outcomes of DDP, however as they have divergent ideas about the importance of DDP, they value different parts of the programme differently.

All donors agree that DDP has established a strong and broad network of actors, and that the programme works with trusted strategic partners. According to the donors interviewed, DDP stands out compared to other funding mechanism, because it seems to give a more quality response to emergency cases; first identifying the real long term need and then trying to solve that need in a sustainable way. Or as donor framed it "*DDP does rapid response like it should be done."*

Box 4.3 Story of change: incidental emergency grant

I am a knowledge and network development coordinator of an LGBTI network. In my country, LGBTI activities are banned. We face discrimination and persecution. The LGBTI community makes use of digital space to meet and to communicate, but this online communication increases the vulnerabilities, also for me. I had no access to internet and [external] hard drives. We used flash discs so we would go to cafes to send emails, which is not safe. That is how I got problems. While leaving an internet café, I was physically attacked by people who beat me up, castigated me for being gay, and grabbed my laptop, mobile phone and hard drive, making it impossible for me to continue my work as network coordinator.

Before giving me the grant, DDP staff took me through a process of understanding other systems I would need to improve my security. They advised me to download safe communications software. They also sent me a digital security expert and provided an online mentorship in using the online toolkit. The DDP staff showed personal care for my situation, and the communication was cautious and confidential. I used the grant to buy a new laptop and hard drive, and install anti-virus software and laptop tracking software. The grant procedure took three weeks, which was little time.

I am not sure I would have found another funder. Maybe for a new laptop, but DDP goes an extra mile by providing equipment, software and support. After receiving the grant, I have become more cautious regarding safety issues. I have several backups for every file. I always update and I rarely use hard copies. I also communicate more securely with others whom might be at risk of attacks and persecution. I have also passed on the skills and practices I acquired. Whenever I go to organisations in our network, I give security tips to their staff. I have trained fifteen individuals from four organisations in our network. For these four organisations, as well as for all computers at our organisation, I have downloaded the Digital First Aid Kit and taught the staff how to use it.

The funding proved to serve both as a quick fix for the urgent problem after the personal attack, as well as a sustainable solution for the long run. It helped me to address an immediate security problem, but in the long run it has helped me to develop skills that I am using to assist others who might be vulnerable to attacks. Without receiving this grant my life and my work would have been very difficult.

4.1.6. Outsiders

"What DDP did is forcing a function for a convening space; it wasn't only DDP; but it was an instigator and a catalyst for rapid change. There is lots of innovation because of DDP (and other stakeholders) forced information sharing. Before [innovation] was happening in silos."

For this evaluation, 10 external stakeholders were interviewed about DDPs work including 6 local experts as part of the country case studies. Around half of the outsiders were not aware of DDPs existence and the ones that knew DDP, were not very familiar with DDPs activities. This shows that although DDP has a strong network, it is limited to a certain group of established contacts. All outsiders however valued the existence of DDP, due to the sheer need for digital safety support in many countries. According to them, civil society space for human right defenders is shrinking in their and many other countries, which is also reflected in increasing digital pressure for human right defenders.

In general, outsiders are also aware of other grant mechanism, such as AccessNow and Open Technology Fund, but they also mention that is quite difficult to apply for these grants and no local support mechanisms for digital safety issues are available in their country. Having a grant mechanism

in place for incidental and more sustainable support is therefore very much valued. Outsiders feel however that the outreach of DDP is quite limited, or as one outsider – a responder - comments: "*I wished we knew about the DDP before, as we could have recommended many organisations that have asked us for help, to try to get funding or support*." Some also mention that the language barrier might be a problem for local HRDs, since DDP mainly communicates in English.

The digital integrity fellowship is appreciated by outsiders and seem to fit in a wider plead from the digital security community for more sustainable interventions as short interventions, like 5-day digital safety trainings, seem not effective. An outsider "*We did these short safety trainings also. We decided to stop with this after an evaluation, because it doesn't work. People are enthusiastic during the training, but once returning to their daily work, nothing changes because it is too difficult for them to apply the gained skills. The organisation has not changed; learning should be repeated, preferably within the organisation itself."* Outsiders stress the importance of capacitating organisations so they can work on their own digital safety in the future themselves. As one respondent says: *"Digital safety is a process, you are never finished."* Types of threats are changing rapidly, making it more important to increase the organisations resilience so they can adapt to these changing circumstances in the long run. Most outsiders therefore believe sustainable and long term solutions to prevent the acute threats are important, although incidental support will still be needed. DDP played an important role in this shift in the digital safety community. One expert noted that: "*Although I myself work on technology, I know that this field is not going to be saved by tech. It's going to be saved by deep capacity building and a holistic approach. That sort of approach can come from DDP by creating these spaces."*

Several outsiders, in particular responders, emphasize the importance of supporting the rapid response community within countries or regions, which could also enhance the outreach of the programme. These outsiders agree that local responders do not collaborate or only on an ad-hoc base and that more collaboration and knowledge exchange and build-up of trust would lead to improved quality of the response. In many cases, local HRDs with an acute digital safety emergency do not know who could help them. A stronger rapid response community could improve the links with the target group.

Box 4.4 Story of change: incidental emergency grant and additional support

I am an investigative journalist. I specialize in anti-corruption and cross-border investigations, such as the Panama Papers. I face elevated risks. Physical safety threats include a risk of assassination or assault. I frequently notice that I am followed. Sometimes I must temporarily leave the country when it gets too dangerous. However, information security is my number one concern, since my sources even face a higher risk than I do. My adversaries want to know my sources, so they try to hack my e-mail or employ other methods.

We bought computers with a DDP grant, including my laptop. I can do things now that I wouldn't be able to or that would take much more time. Thanks to the new hardware, I can make it much more effectively and fast. For instance, some online databases take a lot of space, and my old computer couldn't work with them. Everything is much easier now. I also attended trainings. It changed my user habits. For example, in my job, the use of PGP is paramount to protect identities of my sources. I also learned how to securely store data and how to use full-disk encryption. I learned how to use VPN.

Without this grant, I wouldn't be able to do these investigations. I would probably have to spend my own money on it, which I simply don't have. Neither do I have the expertise to decide what I need specifically. Using my old ways, I would just "hit the ceiling" with too much sensitive data that I couldn't process or transfer. Because I learned more about threats, I probably feel less secure than before. But it is better to be aware of the threats than to remain ignorant and happy. You can protect yourself better if you know what threatens you.

Risks grow and change all the time, methods of our adversaries also change. Therefore, we need constant training in new topics. Attacks on phones are now done differently and much easier than 3 years ago. You need to be trained every year to catch up with these changes.

4.2. Reflection on costs versus benefits

The collected data shows that DDPs resources are effectively spend; almost all respondents supported through DDP feel that they have benefitted from the support. Critical internet users improved their digital safety practices, although in some cases adherence to digital safety procedures remains a bottle-neck. In half of the cases, critical internet users felt that the support given was not a quick fix, but led to sustainable changes. Responders feel that the quality of their response has improved through DDP support. Rapid response members of RaReNet are positive on the effect of this network for their work, although they agree that the benefits could be higher if the network was even more actively managed. Strategic partners value the trust DDP gives to them and the grants help them to sustain their work. Donors and outsiders also mainly value the outcomes of DDP as positive. DDP documentation made clear that hardly any grants were wasted on non-authentic cases and in only two cases the invested support did not lead to impact. In general, it can be concluded that the DDPs expenditures led to positive outcomes for individuals and organisations that were supported and influenced the community around them. Although the evaluation team did not explore the financial information of DDP in-depth, it seemed that no resources were ill-invested. If the value of the outcomes as described in this chapter indeed outweigh the costs is for DDPs donors to decide.

5. ASSESSMENT OF DDPS PROGRAMME DESIGN

In this chapter, DDPs programme design is assessed. Firstly, the various instruments of DDP are assessed and it is analysed whether they contribute to DDPs aim. Secondly, DDPs approach with 5 guiding principles is further explored. In the third paragraph, DDPs focus on gender is assessed and in the last paragraph an overall assessment is executed with regards to the programme design and the current needs of DDPs target group.

Key conclusions

- DDPs Interventions impact the supported individuals and organizations in a positive way and all interventions seem to contribute to DDPs goals.
- The budget is a limiting factor in relation to DDPs ambitions and the needs of the target groups.
- There is a large group of CIUs in need that is not reached by the programme. A critical factor is the outreach and selection: does DDP reaches the most vulnerable and strategic cases?
- DDPs approach fits to the needs of the diverse stakeholders; especially the guiding principle with regards to confidentiality is highly valued.
- Although a gender focus is part of DDP, some stakeholders feel this could be more emphasized.
- DDPs strategy and interventions should be consolidated, although some adaptions could be done to fit to existing needs.

1. Programme design
How do the different DDP parts contribute to increased safety & strengthened human rights for critical internet, and increased capacity of the global emergency response ecosystem?
How does DDPs approach contribute to increased safety & strengthened human rights for critical internet users and increased capacity of the global emergency response ecosystem?
How does DDP gear the work to actively include women? Is the target group defined enough?
To what extent are DDPs strategy, objectives, interventions, approach and choice of strategic partners still valid and appropriate to the needs of critical internet users, emergency responders and the emergency response ecosystem? Are the activities and outputs of the programme consistent with the intended impacts and effects?

5.1. DDP interventions related to aims

As was discussed in Chapter 4, almost all individuals and organisations supported through DDP feel that they have benefitted from the support. Critical internet users acknowledge that they increased their digital safety, responders feel that the quality of their response has improved through DDP support. It means that – according to DDPs beneficiaries – all the different interventions have a certain impact and contribute to the goals of DDP. None of DDPs intervention is negatively assessed. In general, the Theory of Change (see figure 3.2 in Chapter 3) seems confirmed by the data. We will consider this in more detail in this paragraph.

Incidental support, be it a grant or emergency support of one of DDPs strategic partners, has the aim to solve the immediate emergency to enable the critical internet user to continue their work. In the interviews this relation seem confirmed, the emergency support was indeed necessary for critical internet users to be able to continue the work, but not sufficient to fully become digitally secure as an organisation. For example, a respondent that received emergency support of DDP strategic partner Virtual Road: *"Our website received numerous attacks caused by spambots. The website was cleaned and migrated to a secure server. Without this, the website and staff emails would be prone to attacks and this would surely hinder our work. It was however a quick fix for an urgent problem. A long term sustainable system would involve training staff on digital security, purchasing of secure digital equipment, procurement of CCTV cameras etc."*

Interestingly, some stories also show that incidental emergency support can create a wider impact, but only because the support was in-depth and additional support was given. The story of change in Box 4.3 illustrate that the additional and in-depth support of DDP also capacitated the beneficiary to change its behaviour and even to influence others to create more awareness of digital safety in his network.

Data clearly demonstrate that the holistic sustainable support, such as the sustainable emergency grants and the digital integrity fellowship, lead to organisations feeling more in control of their own organisational digital safety (see for example Box 4.1). In general, interviews confirm that these tools do capacitate organisations in the long run, as is the aim of these interventions. On the other hand, it can be concluded that many organisations struggle to secure their organisations in a thorough way. More than half of the respondents mention barriers for organisational change (see Box 5.1 below). Barriers mentioned are safe tools which are not user friendly and safe tools that cause problems with other software, or unsafe communication with clients of the organisation who do not have the means to communicate safely. Interviews also show that once organisations start to learn how to deal with digital threats, it also becomes clear that there is no one final solution and that a learning attitude is necessary by all staff members. So, although organisations acknowledge that they are more capacitated, at the same time they also realise there is a lot more to learn and change, because new needs keep emerging. This is not to say that this sustainable support does not work; it mainly shows that it is not easy to become and stay digitally secure and that long-term support is needed to change organisations.

The third group of interventions, such as rapid response networks and capacity grants for responders, is centred around the digital response eco-system. Supporting rapid responders is strategic, by focusing on these groups, DDP can indirectly reach a much larger group of critical internet users then via direct support. The impact of these interventions is more difficult to gauche; it is hard to measure changes in ‘the eco-system’. However, speaking to responders clarifies two issues: 1) there is a very clear need for more collaboration between responders, particularly on a regional level. This collaboration does not occur automatically, mainly because of a lack of trust 2) Once responders collaborate, they can define several added values of the network (see also 4.1.4). The investment in the global Rapid Response Network seems to indeed improve the quality of the response, with many critical internet users benefitting from this, however the regional networks seem currently too fragmented and ad-hoc to establish a similar effect.

The capacity grants for individual responders seem to have a weaker effect on the digital response eco-system. The result of the investment is mainly limited to that responder receiving the grant. As mentioned in section 4.1.2, investing in a responder does not automatically lead to an improved eco-system. Interestingly, not so much the eco-system, but critical internet users benefit from these types of grants, since the responder invest the grant to support several HRD organisations under attack. The grant links therefore more to sustainable emergency support for critical internet users and less to the eco-system.

Box 5.1 Barriers to digital safety practices

Although many respondents are positive about DDPs outcomes, more than half of the respondents comment on the difficulties of improving digital safety. Barriers that hinder digital safety practices that are listed below, show how persistent unsafe behaviour can be and why many responders and experts belief that parachute interventions do not work and more sustainable interventions on the level of the organisation are more likely to be successful.

“It is about a systemic change; Useful skills taught at trainings are not always transformed into real practices. Organizations need to realize that it is not just tools that make information secure, but practices”. Barriers that were mentioned, can be divided into three different groups: barriers on an individual level, on an organisational level and lastly technical barriers

Barriers on the individual level:

- Some of the critical internet users are semi-literate lacking sufficient educational background and will generally struggle with changes; they feel most comfortable to stick to old habits.
- Social media is often used to voice rights, and although not secure, for many HRDs it is not possible to quit social media like using Facebook because it is an important mean to reach their audience.
- A lack of awareness about the need for digital safety under critical internet users and a persistent myth that digital safety only concerns individuals that have something to *hide "We have nothing to hide. And [the regime] will crack it anyway. A security policy won't help."*
- No real urgency: until there is a fire (a real cyber-attack), people are reluctant to change their behaviour.
- The clients of some organisations don't always have the means or the skills to operate anonymously and securely, for example via pgp. The internal organisational communication of organisations involved in the programme can be secure, but communication with the client is not be possible in a secure way.

Barriers on the organisational level

- Individuals receive training, but eventually organisations as a whole need to change. If the organisational structures are not addressed, the individual will resume their old patterns. *"Digital security is not assumed as a collective responsibility. It remains as an isolated rather than an institutional effort focusing on one member due to the own interest and expertise in the subject of the specific staff member".*
- Different levels of expertise and digital skills among members of the organisations. Organisations had to constantly adapt their training programs to involve all staff members including less savvy members to 'catch-up' and understand not only the basic elements of digital safety but also the rationale behind digital safety.
- Internet security is not about a problem that is fixed once and solved, but instead organisations need to be capacitated to be able to react to new threats.

Technical barriers

- Safe tools are too complicated or not users friendly, with less features, and so on. For example: *"We tried Signal for the internal communication via mobile phones but it did not work well on group chats so we returned to use WhatsApp".*
- Safe tools do sometimes not mix with organisational software and cause additional technical problems.
- Lack of technical infrastructure and resources from organisations. There is a lack of updated systems, many are exposed to malware and are vulnerable even to very simple attacks. There is often no structured IT support, and there is lots of pirated software. *"We use the tool although we are aware of the digital risks involved, choosing a secure channel for communication is a luxury that we cannot afford".*
- There is not one best solution to improve safety. For example, although most open source software has advantages, it only works with sufficient technical support. This can even make secure systems vulnerable. A *responder "Open software can also lead to problems, hired IT specialist can turn out to be working for the regime and install a worm on the machine".*
- Capacity and resources of 'the repressors' are in many cases more elaborate, making it difficult for non-governmental organisations and critical Internet users to counteract many of the digital threats.

5.2. DDPs approach

The DDP is based on a set of guiding principles, which are the following core values:

1. Human rights & Internet freedom	DDP works with donors, partners, consultants and grantees committed to the universal human rights
2. Trust & Confidentiality	Establishing and maintaining trust with partners
3. Mentorship & Partnership	A partnership with our grantees on equal footing
4. Quality & Expertise	No quick fixes but qualitative and trusted response that increases resilience is vital
5. Not claiming, but facilitating	We want individuals and organizations to have and take ownership of their own interventions, activities

Grantees, indirect beneficiaries, donors and experts have been asked to reflect on these values in the interviews. The consensus is that these values are very relevant in this field and that the right values are selected by the DDP staff. One of the grantees says *"Because DDP adheres to these values they are a unique player. They engage in a way that other donors (mostly American based or European governments) don't."*

Especially the value on trust & confidentiality is deemed very important and it is acknowledged that the DDP staff strongly adheres to this principle. This give applicants the necessary trust to share personal

information. For example, a beneficiary narrates: *"Whenever the DDP person communicated she would follow up in a different email to ascertain whether I had got her earlier email. One time she called to say I have sent you an email, please respond. She called again to ask whether the response email she had received was indeed sent by me. There was a lot of cautiousness about my security and the confidentiality of our communications."* And a donor that compares DDP with other HRD programs they support: *"When it comes to trust and confidentiality, DDP is ahead of those other emergency networks. DDP has put a lot of thought into ways of communicating with their grantees."* Although many agree that adhering to these values contributes to good relationships between DDP and its grantees, and this is a requirement to realize the aim of the program, some respondents also acknowledge that the guiding principles are based on Western or humanistic values, and in that respect, might not always fit with the cultural background of some grantees. For example, a respondent commented on the value of equal partnership *"This is less important in our country. Most people want coaching and analysis. A "big brother" attitude [i.e. more patronizing] is better, as it brings more trust and authority."* An open and sensitive attitude for what is appropriate in a certain context is therefore also necessary.

Particularly value 3 'Mentoring & Partnership' and 4 'Quality & Expertise' reflect DDPs specific approach compared to other digital security grant facilities. DDP is known to assess requests for assistance more in-depth in order to analyse the needs of the grant applicant and it is also known to look out for more long-term solutions. In particular, the strategic partners value principle 3 'Mentoring & Partnership' and value 5 'Not claiming but facilitating'. They feel that as strategic partners, they receive a lot of trust and space to develop what they themselves think is best to be most effective. Compared to other grant facilities or donors, DDP is less rigid. A donor however commented that with regards to mentorship & partnership, DDP can still develop and learn from more established human right funds.

Principle 5 'Not claiming, but facilitating' might also have a slight downside. Although DDP has a well-established position in the response network, the programme is not well known outside their direct network. Several small interviews at the Internet Freedom Festival and interviews with local experts in the country case studies revealed that many persons in the digital safety community have not heard of DDP. This might be due to DDPs modesty and adherence to this value. In addition, and perhaps not surprising, many of the indirect beneficiaries of DDPs strategic partners were not aware of the fact that they received support thanks to DDP.

5.3. DDPs gender focus

In general, female CIUs are more vulnerable to digital threats; there are specific forms of harassment targeting women specifically and there are few women working in cyber security[5] [6]. For these reasons, and because of donors' requests, DDP has added a gender focus in the strategic plan 2016 -2019. DDP incorporates a gender focus by working with intermediaries who consider this aspect in their work (annual plan 2016). In addition, the digital integrity fellowship aims to work specifically with females within (women's) human rights organizations. Off all the 12 digital integrity fellowships that were started in 2016, 4 organisations were women HRDs organisations and 6 of the 13 champions were female. Since 2016, a female DI fellow was added to the DIF team.

From the documentation and the interviews, it becomes clear that DDP indeed focuses more on women compared to the past. The consensus of experts, donors and responders is that this focus on women is necessary; all acknowledge that female HRDs and journalists are in even higher needs than

[5] http://www.ictworks.org/2015/01/12/gender-violence-2-0-the-digital-safety-gap-for-women/
[6] http://www.genderit.org/sites/default/upload/flow_tbtt_mapping_analysis_final.pdf

their male counterparts. Some of them would even welcome a more stronger gender specific focus. Donor: "*Often men have more access to networks, and are more willing to report than women. It takes twice as much effort to target and reach women. I feel this is an area where DDP could develop in their referral network, building trust etc.*"

According to the respondents, the target group is well defined, it is merely a matter of more strategic partnering with for example large women HRD networks to make sure that DDP is more well-known under the target group. Most respondents felt that DDP is doing sufficiently to target women, but two organisations, a women HRD organisation and an organisation that works with women activists, suggested how DDP could improve the programme to make it more women friendly. Both organisations feel DDPs technical experts could receive more training on particularities of (digital) violence against women and gender issues, so they can be more sensitive when dealing with women defenders. Another suggestion is to make some of the communication more inclusive for women (with use of less technical language which might put women at a distance). Box 5.2 presents a story of change of one of these organisation, including their views on how DDP could become more women friendly.

Box 5.2 Story of change: indirect beneficiary strategic partner Front Line Defenders

We provide psychological support and guidance to human rights defenders, activists, journalists and victims of human rights violations. We want to help them to cope with the violence they face. In almost every counselling session, issues of digital security are raised. The victims and defenders we work with experience constant attacks, from identity theft to violent threats. The most pressing issue we - as organisation - face in terms of digital safety, is the storage and management of the sensitive information that we collect during counselling sessions. We cannot encrypt this information, because there is a lack of knowledge and tools.

One of us knew the fellow of FLD through an earlier collaboration in a former job. FLD helped us by means of technical support as well as capacity building support. The technical support helped us with an urgent problem allowing us to separate our internal and external network. By doing so, we were able to work without being connected on Wi-Fi, thereby reducing the exposure to digital attacks. The capacity building support consisted of training workshops and personalised support from the FLD Fellow. The workshops addressed from the basic strategies of digital safety –passwords and encryption– to more sophisticated issues for those savvier in the subject.

The workshops – although insufficient in terms of time to address all the needs of the participants– has raised awareness of the risks and made the vulnerabilities of the organisation evident. The support has made a clear difference. Not only our information is safer, but we also feel safer doing our work and feel more confident addressing the subject. We have developed our own guidelines and good practices in terms of digital safety. We are also learning to differentiate between certain tools and software. There are still some struggles, for example our administrative software does not run properly, so long term support in these organisational processes is really needed. A barrier that hindered the impact of the support was that the Digital Protection Consultant (DPCs) was not located in the country; this complicated communication and coordination of workshops. As an almost all-female organisation (supporting many women human rights defenders), we feel that DPCs should be more aware of gender issues. Some of our users have experienced attacks directed to women's sexuality, preferences and private life. These types of attacks were not addressed during the workshops, even though all the participants were women. Sometimes female participants are minimised or dismissed by DPCs or conveners of the workshops to favour male counterparts. We don't think that this is an intentional response, but it demonstrates the importance of having DPCs in the programme that are sensitive to possible (implicit) biases against women and its possible impact on results.

5.4. Assessment of DDPs programme design

5.4.1. The needs

All respondents participating in this evaluation agree that digital security is a pressing societal issue worldwide. In the three country case studies executed for this evaluation, an overview is given on the current state of affairs of human rights and digital safety in each country (see confidential report Country Case Studies) illustrating that although the three countries differ very much from each other in terms of culture, economics, language, law and order etc., there is shared agreement on the urgency

of digital safety of human right defenders, journalists and bloggers. The need for digital security support in each of these countries is high and resources are lacking. A RaReNet member also comments on the scale of the problem: *"The needs are so high; we could use an entire DDP for each country we work in."* Many responders face burn out, because of the amount of request of help and lack of resources to support all these needs. And, as one of the external stakeholder said, "E*ven we, as the digital safety community are overwhelmed; the needs, shrinking civil space, the pace of new technologies appearing and systems to repress people."* Compared to the needs present, the ambitions of DDP are high and experts feel that the ambitions of DDP are high in relation to DDPs budget, or with a nicely put metaphor of one of the RaReNet responders: *"DDP is trying to catch a dragon with a tiny bird cage."*

Bearing this in mind, DDPs interventions will never be sufficient for all the current needs, which is something to be accepted. It makes it even more important to be very strategic in the focus of the programme and who to support. This might be more relevant than considering the exact type of interventions. As evaluators, we assess DDPs outreach and selection processes as somewhat weaker compared to other elements; because of the conscious choice to not undertake a strong outreach, there is a dependence on DDPs (elaborate) network to connect to organisation in need of support, see also Box 5.3. with more information on DDPS outreach and selection below. Further, less needs were expressed with regards to legal support, which raises the question if DDP should continue with this type of support. In this evaluation, only one interview dealt with this type of support making it insufficient to draw any conclusion on this. However, this might be something to consider in more detail by DDP staff in a later stage.

Box 5.3 DDPs outreach and selection

DDP does not spent a lot of time on outreach, which is related to the fact that the grant facility already receives more requests than it can grant. According to DDPs documentation and interview with DDP staff, there are several means of reaching out. Firstly, via Hivos own network, strategic partner networks and regional rapid response networks responders are asked to propose local organizations for grant applications (strategic plan 2016 – 2019). Secondly, DDP also coordinates with similar funds as OTF and Access Now and actors who manage help lines to refer potential grantees to funding opportunities. And thirdly, DDP approaches embassies to provide material, although this does not happen on a structural base due to a lack of time of DDP staff. From the interviews, it becomes clear that almost all grantees and organisations participating in the digital integrity fellowship, got to know DDP through their personal network. HRD's or HR organisations with an international network and with English proficiency are therefore more likely to reach out to DDP then the ones that operate more locally and that experience a language barrier*. If DDP would be more known by local responders, it would enlarge its outreach. A donor reflected on this *"The difficult part is to be able to decide who should have access to that support - that is or might be a weak spot, even if I do trust the DDP staff. We would need better and more information on the strategic choices of who to service".* In particular, community based organisations and HRDs and bloggers operating independently, might not be aware of DDPs support, as an outsider points out.

With regards to selection procedures, the most important reasons for refusal of applications are lack of funding, grant request which are not in line with the mandate or applications that are difficult to assess whether the emergencies or requests are authentic (DDP Q3 2016 report). Staff and digital integrity fellows confirm that in the assessment of grants and organisations applying for the fellowship, several indicators are considered: presence of threat (relevant for critical internet users), diversification of target groups, track record (in particular relevant for responders) and strategic relevance in a country. Fellows add to these criteria that a personal relationship between them and the organisation is important.

After selecting potential grantees, a vetting procedure is started. This procedure is not standardized; the procedure can be quick if DDP can identify a reliable source that can back up the validity of the request. Vetting procedures take more time for organisations that are not familiar to DDP, since it is more difficult to examine if the application is authentic. DDPs vetting seems sufficient, there are hardly any occasions reported where a grant was supplied for a non-authentic case (only one in 2015). Because of the network DDP has built up over the years, the vetting procedure has become easier; there are more contacts DDP can reach out to verify information. With regards to the fellowship, vetting is in most cases not necessary, since a relationship already exist in many cases between the fellow and the organisation that is applying. Fellows discuss however between each other and together with DDP staff, which organisation would benefit most from the fellowship and decide on this together with DDP staff as a team.

* *The fellows of the Digital Integrity Fellowship were selected to cover several world languages like Spanish, Arabic, Portuguese, French, in addition to English; so language barriers are partly tackled in the DIF.*

5.4.2. Objectives

DDPs has two main objectives: 1) Increased safety for critical internet users under attack and 2) Increased capacity of the digital emergency response ecosystem. Both objectives are assessed as relevant by respondents. It might be advisable to clarify to stakeholders, in particular to donors, that the second goal is instrumental to the first goal and that the first goal is the main aim of the programme. It is evident that this instrumental goal of improving the eco-system is strategic. DDP can influence the situation of many critical internet users by improving the response eco-system.

Apart from the two goals, DDP also formulated a long-term impact goal 'critical internet users have a safer environment in which to carry out their work without digital threats' and vision 'keep the Internet open and free from emerging threats' (see also Fig 3.2). The impact and vision that were formulated at the start of DDP seem to focus on the technical side ('safe environment without digital threats' and 'internet open from emerging threats') that is not congruent with DDPs people-oriented approach, in contrast with a tools- or technology-oriented approach. DDPs intension is to capacitate users to continue their work, notwithstanding digital threats. It would make sense to adapt the long-term impact goal and vision more in line with the people-oriented focus of the programme.

5.4.3. DDPs strategy

When looking at the problem tree (see Box 3.1) that tried to explore the roots of the problem DDP is aiming to solve, it becomes clear that DDPs nature is mainly reactive. Although it addresses the lack of collaboration between responders, it does not address root causes like the influence of the large companies or lack of awareness by HRDs on digital security. However, since DDPs ambitions are already high in relation to its budget, we feel it is wise that DDP stays focused on the core of its ambition: sustainable and holistic emergency response.

To be or not to be: funder or intermediary

DDP started as a grant facility, but nowadays DDPs strategy is much more diversified. However, the duality of DDPs nature raises the question by external stakeholders whether DDP is a funder or an intermediary running a programme. This ambiguity should be considered and both options are reasonable. DDP is now still mainly seen as a funder and one of the better ones; DDP stands out compared to other funders. By positioning DDP as an intermediary this uniqueness would decrease. As one expert points out, there are already a lot of Western intermediaries with similar programs, so DDP might have more difficulties to distinguish itself in the digital safety community.

On the other hand, there are also benefits to position DDP as a program with a grant facility alongside. When an emergency occurs, many beneficiaries do not know where to start, so their problem is not solved by a grant only. A responder said: "*In most cases, it is more important to receive contacts of certified, trusted service providers and to get equipment or services instead of cash. It takes time to receive money, find the thing you need, buy it, learn how to use it, etc. Direct provision of services and tools is more efficient."* When DDP would position itself as an intermediary with a programme, it would simplify the grant structure: DDPs strategic partners could become implementing partners, which might help to strengthen the strategic partnership, and makes it easier for outsiders to understand that this earmarked output of strategic partners would count as output of DDP; the organisations that they support would be direct beneficiaries instead of indirect beneficiaries. From an outsider perspective, it is not entirely clear that the strategic grants directly serve critical internet users. Proposing DDP as a programme with implementing partners could give a more realistic overview of the actual output, and clarifies that many direct internet users under attack are direct beneficiaries of DDP, instead of presenting three grants for three responders. To be able to explain DDP well to outsiders, and to improve DDPs branding and profile, it might be wise for DDP to reflect with strategic partners and donors on what its core nature is and should be.

Strategic partners

Experts and donors agree that the selected strategic partners are partners with a good reputation each responding to a unique need. Country exports however point out, that DDP is mainly linked to global responders and to a lesser extent to local partners. Some beneficiaries also feel that local responders are easier accessed; a locally based partner would be able to offer advice over a longer period and at shorter notice. It is advisable that DDP should invest in building up strong regional/local networks and locally embedded fellows and keep providing grants for organisations that want to work with a local responder instead of a global strategic partner.

Types of interventions

a) Incidental emergency support

Incidental support is very much valued by the recipients, enabling critical internet users to continue their work. Donors particularly emphasized and valued the incidental emergency response. This should stay an important element in the programme. It is interesting to note that responders and experts favour sustainable emergency over incidental response, they prefer to capacitate organisations under attack for the long term, to prevent incidences. But they also admit that both elements are necessary and DDP should find a good balance between those two elements.

b) Sustainable emergency support

DDP is known for its sustainable response which is something DDP could be proud of. Generally, long term comprehensive approach to capacitate organisations is attracting more attention in the digital safety field, the fellowship fits in this wider trend or might even be one of the trendsetters. Not only responders, but also critical internet users themselves are eager to receive sustainable support. For example, a HRD: *"We want in depth support that allows us to actually become independent in terms of digital security and able to help other organisations and individuals."* There is a discussion between DDPs strategic partners, and under responders in general, how holistic the response should be and if other aspects of safety, such as physical, legal, emotional safety should be taken into account. Some of the Digital Integrity Fellowships already included some holistic components (see also Annual Plan 2017), and this need for holistic response is confirmed by quite a few respondents who explain that digital safety cannot be separated from other aspects of safety. From the interviews however, it also becomes clear that DDPs asset and unique selling point is exactly the knowledge and network of digital safety that makes them stand out. It seems advisable to have the digital safety aspect as an entry point, but not to exclude other aspects, when necessary, as is the case now. In addition, some strategic partners, responders and experts would prefer to also work preventatively; supporting critical internet users before they are attacked and before emergencies kick in, would make more sense than waiting until the attacks starts. Looking at the high needs, it might be wise however to keep the focus to holistic emergency support.

DDP could put more emphasis in their communication to the outside world, that the sustainable emergency support still targets organisations under attack; this is not entirely clear to some stakeholders. This selection criteria 'under attack' should also be adhered to. Some current cases which are supported are not marked by a concrete threat incidence, so it seems from some interviews[7].

Travel and time distance are mentioned as a practical issue that hinders the effectiveness of support from a responder/fellow that is not present in the country. In our view, the Digital Integrity Fellowship should aim to work more with local embedded fellows, ideally growing from a champion position

[7] It might be possible that during the interview, the respondents trivialize incidents or are not able to list a concrete recent attack, making it difficult for them to point out if or how they are under threat.

within an organisation towards becoming a fellow that can help other organisations in the country. So far, DDP has succeeded to do this once and this story illustrated the potential power of DDP to transform entire communities and networks. Local embedded fellows could be coached by the more senior fellows that DDP has attracted, as is already DDPs ambition according to the Annual Plan 2017.

Organisations also stress the importance of being connected to other organisations and responders. It might be advisable – in contrast to the global character of the incidental emergency support – to focus the sustainable emergency support to particular regions, where also a stronger investment is made in rapid response networks and link these groups together. As a responder says: "*By providing continuous support to these 'hubs' it is possible to maintain the momentum and motivation, strengthen and deepen their learning, as well as securing good practices and behaviours."*

c) Supporting the emergency response eco-system

Investing in rapid responders is an efficient strategy due to the wide scope; many more critical internet users can be indirectly supported via rapid responders then via direct DDP support. The global rapid responder network and regional networks seem key in DDPs vitality. Based on this evaluation, it can be concluded that investing in RaReNet surely has added value. In addition, there is a real and unaddressed need for regional/local rapid response networks. A strategic partner reflects via the survey: *"The most important need that is not addressed enough is supporting organisations and networks in jointly enhancing their practices and setting up policies and processes. Response, prevention and mitigation is largely dependent on practice with peers, as well as a strong and diverse community of support."* The global RaReNet is an established network, where global responders know how to find one another and meet – apart from RaReNet meetings - also on more occasions, like international conferences. These networks and opportunities do not exist on a regional level; although some regional network meetings are organised by DDP, there is no structure established yet according to some participants[8]. When budget allows, DDP could invest more strongly in these regional networks to fill this gap and integrate the valuable experience and lessons learned that were built up from the global RaReNet. Regionally based responders stress the need for face-to-face meetups to build trust. A responder *"In our country, there is for example a community of activists, which took decades to build and evolve. With IT, there are more and more policy issues, you need to work with lawyers, etc. It takes years to build such a community: identify, train, connect these people. Webinars alone cannot achieve this objective."* From a knowledge sharing point of view, it might be interesting to connect the global and regional level with each other. For example, selecting a topic (holistic response, gender approach etc.) and facilitate capacity building on that theme, both on global and regional level and share lessons learned with each other. RaReNet members also prefer a stronger facilitation of the global network; if there is sufficient space in DDPs budget to allow this, the network could gain strength.

In case choices need to be made due to scarcity of the budget, DDPs capacity building grant for rapid responders seems to have more of an influence on the individual responder and their beneficiaries, and to a lesser extent to the total rapid response ecosystem. If DDP mainly aims to improve the rapid response eco-system, capacity building of responders might also be done in a more efficient way via regional rapid responder communities and by building the capacity of several responders at once in training sessions.

[8] It is interesting to note that interviewed participants of these meetings are not always aware that these meetings are organized through DDP, not always clear to them what the goal of this meeting is (to establish a network) and they are also not aware that it is the intention to have these meetings annually. In practice this is also not always the case, due to budget limitations.

5.4.4. In conclusion

So, is the DDPs strategy valid considering the needs of critical internet users and responders? Overall, we can say that DDP has established a good portfolio of instruments to service both target groups. Since DDP has rapidly grown from a grant facility to a portfolio with diverse interventions, our advice is to focus to consolidate and improve the existing instruments, rather than breaching out into new directions. Chapter 7 provides practical recommendations to build on existing instruments.

DDP could explore two areas, that are not part of DDPs strategy now. First, according to some respondents there might be an upcoming trend under donors to embed digital safety within larger HRD programs. It would be wise for DDP staff to consider what implications this could have for DDP as a programme and interesting to explore how and in what way DDP could collaborate with these existing HRD programs and networks, to be prepared it this trend really sets in.

Second, and related to this, DDP and DDPs responder network have so much knowledge to share with regards awareness raising on the topic of digital safety. Responders comment that a large part of their work is - not efficiently - taken up to raise awareness and explain to HRDs why they should work digitally safe. It might be interesting to explore how DDP could collaborate with existing HRD programs and networks to work on this awareness. For example, by investing some budget to develop a booklet or video with ‘failure stories’, what could happen when organisations are not prepared, including references to DDP and its network of responders, and use this as both a preventative tool as well as an outreach strategy to become more visible for DDPs target group.

6. ENABLING AND CONSTRAINING FACTORS

To assess the effectiveness of a program, it is important to consider the overall programme in a holistic manner and to analyse specific factors that supported or hindered to the success of the programme. In this chapter, we will identify these factors. To answer this question above, we rely on qualitative data from interviews with stakeholders, beneficiaries, donors and programme staff.

Key conclusions

- Factors that contribute to DDPs success are a dedicated and flexible team, the strong network and its needs-based approach.
- Factors that might hinder DDPs success, are a vulnerability in the outreach that is mainly based on DDP's network and less developed communication skills.

3. Process
What enabled successful implementation and outcomes to occur? What barriers existed that led to less than successful implementation and outcomes?

6.1 Enabling factors

Dedicated and flexible team

DDP staff is very dedicated and committed to make DDP successful, with an attitude of going the extra mile to make sure that grantees are supported in the best possible way. Many compliments were given by respondents to the staff, including their personal interest, their close follow up of cases and their flexibility in procedures. Not the application or procedure, but the grantee is central in their approach which was highly appreciated.

Agility

DDP started as a grant facility only but developed different elements to address needs of their target groups over the years. Some of DDPs tools can be seen back by other stakeholders in the field (for example the Rapid Response Fund and the Digital Integrity Fellowship Programme of the Open Technology Fund), showing that DDP could be a trendsetter or at least aware of the current developments and responding to this. This agility to respond to emerging trends is needed in the area of digital safety where so many developments take place.

Strong network

DDP has built up a good and thorough network with stakeholders that are part of a wider digital security community. They are well established in the technical responders' community and are trusted and respected. DDPs approach of mutual respect and partnerships pays off, as many of their partners and grantees values this approach, leading to a positive attitude towards DDP.

Needs-based approach

With their needs-based approach, DDP stands out compared to other funds. Staff makes sure that first a good diagnosis is made to find out what 'the real needs' are, before taking action. DDP has at a more holistic and comprehensive approach to solving a digital security problem, whereby also other safety aspects that might be relevant are addressed. DDP has a full range of support tools, from incidental quick fixes to more sustainable solutions, from technical to legal support etc.

Trusted neutral partner

Apart from DDPs approach, where trust and neutrality plays an important role, DDP is also trusted which is related to the fact that DDP is a European based fund. Many other grant facilities are based in the US, and for some organisations in need of support this can be complicated. The European

roots, also reflected in DDPs approach and values, are considered as more neutral compared to US based funds, making this fund accessible for organisations from countries that have a tense relation with the US.

Expertise of partners
In general, respondents feel that DDP collaborates with trusted partners with a global reach and a high level of expertise. The indirect beneficiaries that received support of the strategic partners and that were interviewed for this evaluation, are positive about the level of expertise and quality of support received by the strategic partners. Some local experts however feel, that DDPs network is too global oriented and local partners should be more taken into account.

6.2 Constraining factors

Outreach and selection
DDPs network is an asset, but a dependency on personal relationships with regards to outreach and selection procedures can also be vulnerable (see also Box 5.1). It seems likely that DDP struggles to reach those in need that aren't connected to the digital safety community. It is unclear whether the most vulnerable or most strategic cases receive support. Because the needs for support are much higher than the programme can offer due the limitations in funding, strategic selection of cases is key to create the highest impact.

Communication and story telling
It seems DDP seems not very good to explaining to its stakeholders what the programme does and more importantly, what the impact is. Donors, grantees and experts are struggling to get a clear overview what DDP does and still associate DDP mainly with providing emergency funding, whereas DDP does much more. Also, the interlinkages between different interventions are not completely clear. Grantees are not aware that there are other DDP tools that might be of interest to them. Rapid responders who are not part of DDP and are reflecting on DDP as outsiders, are not aware of all the DDP tools. They feel this lack of information and communication is a missed opportunity. They are very interested to learn what DDP does, and know more about its successes and lessons learned. In addition, as evaluators we felt that DDP is very good in explaining at a technical level what has been the funding, however they pay less attention or are less capable to explain the impact of the support in the lives and work of HRDs, journalists etc., while it is obvious the programme has a strong impact of people involved. Illustration of these impacts were provided in the Boxes in Chapter 4 and 5. If DDP could improve these narratives, it might be easier to make a strong case for DDP to expand and grow further. Again, as DDP staff explained, the wish for these more elaborate outreach and M&E actions is present, but time and budget constraints limited the efforts of the team on these aspects in the past year.

Front desk response
Although many respondents expressed satisfaction with the granting process, some grantees (as well as a donor) indicate the requirements of the application on the website can be complicated. This applies especially for individuals who can be overwhelmed by an emergency. They are asked to write an email with a project proposition and to include a budget, but many of these individuals only know they have a problem, but no idea how to solve it or what budget is needed. The application process should be simplified, particularly for the incidental emergency grants.

Lack of structures and clarity of roles
DDPs is valued by grantees and partners for its flexibility, however this flexibility has a downside as well; there is less emphasis on structures or institutionalisation. DDP exists since 2012 and has a relatively short life span, where a lot of emphasis has been put on network building, programme development etc. so this received less attention and it also seemed to interfere with DDPs flexibility.

For example, documentations and reports from partners and grantees have quite different lay-outs and scopes; fellows communicate every month with DDP about the progress of the fellowship, but not in a consistent and structured way, according to the documentation that was provided to the research team. The lack of structure can also be noted in comments of respondents indicating that they struggle to get a clear overview all DDPs different interventions and how they are connected to each other. Organisations that are supported via a strategic partner as FLD, or that participate in the Digital Integrity Fellowship do not know what exactly they are entitled to, for example how many hours the Fellow is able to support them etc. DDP might be at a stage to establishes certain structures, making sure is does not become not too bureaucratic at the same time to ensure it retains its flexibility as a key strength.

Lack of donor coordination

DDP is supported by different donors, which increases its sustainability. However, a lack of donor coordination interferes with efficiency and strategy of DDP. DDPs staff spends a large amount of time on writing proposals for applying to funding opportunities and writing reports, whereby donors have different reporting formats. Proposal and report writing decreases staff time for strategizing and implementation. Apart from the yearly face-to-face donor meeting, donors don't have contact with each other and there is no shared agreement where DDP should focus on. In addition, donors do not communicate to each other the amount of funds they will contribute for a specific year, leaving budget issues for DDP staff to solve. Although this has been thoroughly discussed at the donor meeting last year, it is clear that donor coordination and longer term donor commitments would create more efficiency, with less staff time being spend on proposal and report writing. This is however not necessarily something that DDP would have to organise itself. Rather greater coordination could be conducted by the DDP donors themselves as a mechanism to improve the DDP programme overall.

Small team

DDP has a small team of 3 members to maintain the entire programme. Since the needs in the field are so high and quite some staff time is spent on proposal and report writing, DDP seems to be understaffed to respond to and reflect on rapid developments in digital security; most attention is given to emergencies which need immediate action and coordination of all the different DDP interventions. It has been suggested by a donor and a grantee that some DDP staff are literally doing the work of two or three people in other similar organisations. As the pressure on staff is high, time is lacking to reflect, learn, keep track of new developments and strategic thinking.

7. CONCLUSION AND RECOMMENDATIONS

In this chapter, we draw conclusions on DDPs effectiveness and formulate recommendations to improve the functioning of DDP, as well as giving some suggestions with regards to the monitoring of results.

Lessons learned and recommendations
What are the lessons learned and recommendation regarding DDPs strategy, objectives, interventions, approach, choice of strategic partners and gender-dimension?
What are the recommendations regarding the DDPs log frame and monitoring of results?

7.1. Overall reflections

Digital freedoms are under threat worldwide. The three countries that were studies as part of this evaluation, showed that Human Right Defenders, journalists and bloggers are increasingly challenged in their work, particularly when it comes to their digital safety. In many other countries, this situation is not much different; civil society space is shrinking worldwide[9]. In this environment, digital technologies play a crucial role in enabling or disabling civil society to engage in their activities. There is a strong need for digital safety support for critical internet users and improved response mechanism in case critical internet users are attacked. It is evident that the Digital Defenders Partnership has an important role to play to address these needs.

DDP is a comprehensive programme with an extensive portfolio of instruments to service both critical internet users and rapid responders. We can conclude that almost all individuals and organisations spoken to for this evaluation, feel that they have benefitted from the support. Critical internet users under attack that were reached by the programme, acknowledge that they increased their digital safety, as was the aim of the programme. And although it is difficult to assess whether the capacity of the digital response eco-system has increased, responders feel that the quality of their response has improved through DDP support. DDP stands out with their holistic approach which puts them "*at the top of the pile*" of present funders, as one of the expert framed. DDP seems to be trendsetting at two points. They played an important role in setting up a convening space, in particular for rapid responders. Second, DDPs acknowledgement that digital safety behaviour change of critical internet users is a lengthy process that takes time, and could be better addressed via a digital integrity fellowship was also innovative. Experts and responders spoken to in this evaluation confirm that this holistic sustainable approach is legitimate and sensible and recognized by many others in the digital safety community as a necessary step. Emergency responses are important but are viewed by all the experts and grantees interviewed as potentially highly problematic if simply conducted as 'helicopter interventions' or short term band aids. In many ways DDP can be seen as an innovative response to this problem, by ensuring that short term and long term measures go hand in hand and that a holistic, sustainable, long-term approach is consistently applied.

However, this innovative response by DDP took place in a rapidly developing field in which some elements of the DDP model are being duplicated by other actors. As the landscape in the community has changed, with more funding opportunities for rapid response and other actors following the emerging trend for holistic solutions, DDPs challenge in the coming years will be to adapt to the changing conditions and continue to innovate within the field. It is important to acknowledge not just the impact DDP has directly and indirectly on users, but also how it plays an innovative role in

[9] https://www.fidh.org/en/issues/human-rights-defenders/shrinking-space-for-civil-society/

shaping the community working on these topics. This influence cannot be measured in monetary value, but rather in the higher quality of interventions that DDP helps support across the digital emergency community through its own innovative approach.

From this evaluation, it can also be concluded that DDPs interventions are unlikely to be sufficient any time in the near future given the scale of the global needs in this area. Because of its global scale, DDPs impact to change digital safety landscape in a region or in a country is limited; interventions and beneficiaries are quite scattered. Budget limitations and uncertainties are a considerable constraining barrier. However, DDP surely can and did improve the digital safety situation of the critical internet users they supported. Who to serve is a critical question and the outreach and strategic selection of cases are slightly more vulnerable elements compared to the other strong components of the programme. In table 7.1 an overview is given of the key conclusion for each of the research questions and in the following paragraphs a list of recommendations – on a generic, operational and M&E level – is given that could be considered to maximize the impact of DDP.

Table 7.1 Key conclusions per research question

1. Quality of programme design	Key conclusions
How do the different DDP parts (granting and linking & learning interventions as described in ANNEX 3) interlink and contribute to increased safety & strengthened human rights for critical internet, and increased capacity of the global emergency response ecosystem?	DDP focuses on incidental emergency response, on sustainable and holistic emergency response and on improving the digital response eco-system that supports critical internet users under threat. All individual interventions are logically linked to the aims of the programme.
How does DDPs approach contribute to increased safety & strengthened human rights for critical internet users and increased capacity of the global emergency response ecosystem?	DDPs approach fits to the needs of the diverse stakeholders; especially the guiding principle with regards to confidentiality is highly valued.
How does DDP gear the work to actively include women? Is the target group defined enough?	A gender focus is part of DDP and the target group defined enough. However, stakeholders feel that the gender focus could be more emphasized
To what extent are DDPs strategy, objectives, interventions, approach and choice of strategic partners still valid and appropriate to needs of critical internet users, emergency responders and the emergency response ecosystem? Are the activities and outputs of the programme consistent with the intended impacts and effects?	DDPs strategy and interventions should be consolidated, although some adaptions could be done to fit to existing needs. The budget is a limiting factor in relation to DDPs ambitions and the needs of the target groups. There is a large group of CIUs in need that is not reached by the programme. A critical factor is the outreach and selection: does DDP reaches the most vulnerable and strategic cases?
2. Value of outcomes to participants	**Key conclusions**
How valuable were DDP outcomes to critical internet users, the emergency response ecosystem, the rapid response community, digital integrity organizations, donors, strategic partners? What has happened as a result of the program?	All stakeholders linked to the programme assess outcomes of DDP as valuable and positive. DDP has a clear impact on the critical internet users they reach. DDPs Interventions impact the supported individuals and organizations in a positive way and all interventions seem to contribute to DDPs goals.
How do others (non-grantees, others in the response or internet freedom field) experience/recognize/value the DDP program, approach and interventions?	Outsiders value the existence of DDP, due to the sheer need for digital safety support in many countries but feel that the outreach of DDP is quite limited Outsiders stress the importance of long term support, like the digital integrity fellowship, to capacitate organisations to deal with digital safety issues themselves
What are some of the stories that show the effects of the DDP program? What real difference has the activity made to the beneficiaries? What have beneficiaries done in terms of changing their behaviour so as to avoid or supersede the	Grants and support lead in many cases to sustainable change, in particular interventions with a more sustainable character, although in many cases more needs evolve.

same threats after going through DDP or grantees interventions? And if they haven't changed anything, why is that?	There are still barriers for critical internet users to change organisational behaviour with regards to digital safety.
3. Process	**Key conclusions**
What enabled successful implementation and outcomes to occur? What barriers existed that led to less than successful implementation and outcomes?	Factors that contribute to DDPs success are a dedicated and flexible team, the strong network and its needs-based approach. Factors that might hinder DDPs success, are a vulnerability in the outreach that is mainly based on DDP's network and less developed communication skills.
4. Cost Benefit	**Key conclusions**
Does the value of DDP outcomes outweigh the costs of implementation?	DDPs resources are effectively spend; almost all respondents supported through DDP feel that they have benefitted from the support
5. Lessons learned and recommendations	**Key conclusions**
What are the lessons learned and recommendation regarding DDPs strategy, objectives, interventions, approach, choice of strategic partners and gender-dimension?	Clarifying roles and responsibilities, improving grantee outreach and selection criteria, ensuring better communications and collaborating with local partners, fellows and networks directly will allow DDP to grow further
What are the recommendations regarding the DDPs log frame and monitoring of results?	Less focus on outputs and more on outcomes Collect more evidence of impact on indirect beneficiaries

7.2. Generic strategic recommendations

First, we would like to provide some generic recommendations on how DDP could build and develop its strategy in the coming years.

- **Focus and consolidate**

DDPs niche is sustainable and holistic emergency response. In the five years of DDPs existence, DDP developed many different interventions and invested in building up a good network. For the coming years, it seems advisable to focus on consolidating and improving the existing instruments, rather than breaching out into new directions. DDP should continue providing emergencies response grants as key support for critical Internet users but also provide additional support –both as grants and as learning activities – for organisations to develop sustainable projects aimed to long-term solutions on digital security.

- **Determine DDPs core purpose: is DDP funder or running a programme?**

DDP is still mainly recognised in the field as a funder, but DDPs activities are nowadays much more diversified. Because of this ambiguity, it is difficult to brand DDP and outsiders are puzzled by what DDP exactly is; it is challenging to be both a funder and a programme at the same time. DDP should – with its donors and strategic partners – decide what the core purpose of DDP is and stick to this decision.

- **Stay agile and innovative**

DDPs asset in the past was to understand the lacunae in the digital safety field and to develop ways to meet those needs. To continue the impact DDP had in the digital safety community, DDP also needs to keep evolving itself within a highly innovative field and listen carefully to other funders and stakeholders around DDP. As mentioned above, the challenge is to adapt to changed conditions with more competition with other funding mechanism and intermediaries.

- **Improve communication on all levels**

One of the reoccurring themes in the interviews was a lack of clarity in internal and external communication, that was expressed on many different levels. From local experts and beneficiaries not being aware of DDPs existence, confusion by donors about the comprehensive portfolio of DDP, organisations part of the fellowship not knowing what they are entitled to, responders part of regional

rapid response meetups not being aware that it was sponsored by DDP, to grantees and responders asking for a manual and not being aware of Digital First Aid Kit. These different levels might indicate that solutions for this lack should also be sought on different levels. DDP should improve its narrative, in particular with regards to storytelling of its impact. In addition, DDP should structure information much better to its stakeholders. Such improvements are likely to require the existing DDP team to grow. The following communication improvements could be made:

- Improve communication channels between DDP team and the organisations. Pay attention to communication after the completion of the grant to establish what sort of collaboration or continued support (if any) the organisations can expect from the programme.
- Provide more information about the DDP, including objectives, structure and learning activities to beneficiaries of the programme (both direct and indirect) but also to strategic local partners.
- Disseminate the DDP resources available regarding tools and strategies on digital safety –such as the Digital First Aid Kit– for beneficiaries to share with their own users or continue learning on their own. In addition, create a database with information on how to interpret digital safety incidents and with new tools and resources that organisations can test on their own to solve emergent needs making the learning process more efficient and self-regulated.
- Create a database of frequently asked questions with guidelines on how to apply for the grants and general considerations for organisations to apply. These guidelines could be based on real cases and successful applications.
- Re-brand DDP to attract other types of donors. DDP is now funded by governments and is seen by external stakeholders as a programme that is governmental by nature and connected to the Freedom Online Coalition. As DDP rethinks its communication strategy, a rebranding of DDP should also be considered to make it easier to attract other donor types, for example private foundations or corporations.
- DDP should look out for means to make its work more known and disseminate its narratives far more widely. This will help audiences better understand DDP's role and contribute to widening its existing networks.

- **Clarify direction for strategic partnership and roles of partners**

The strategic partnership is not functioning as a proper partnership; partners are mainly in touch with the DDP team and less with each other. They also do not systematically engage in planning DDP's objectives and it is unclear whether they wish to do so. DDP should together with its partners discus what the exact aim of the partnership is, and what roles and responsibilities should fit with this aim and then adjust the partnership accordingly.

- **Institutionalize**

DDPs strengths are its flexibility to its grantees and beneficiaries and its agility to adept and innovate. After 5 years of DDP, DDP should establish clearer structures, and processes, for example in reporting and communication.

- **Strengthen gender focus**

DDP should look out to strengthen the focus on gender, which could also have strategic value as it helps DDP to stand out as grant facility. DDP should partner with for example large women HRD networks to make sure that DDP is more well-known under the target group. DDPs could invest in training for technical experts on particularities of (digital) violence against women and gender issues, so they can be more aware when dealing with women defenders. In addition, some of the communication could become more inclusive for women (with less technical wording that could put women off). DDP could impose a quota as one of their selection criteria that 25% of their support benefits women or women organisations or DDP could request that grantees have a minimum percentage of women benefitting from DDP-supported activities.

- **Improve Donor coordination**

In addition to the yearly donor meeting, informal donor coordination calls between DDP donors (without DDP staff) once or twice a year could help to establish an agreement between donors where DDP should focus on and to create some agreement – if possible – on reporting requirements. In addition, it could also help if donors could inform each other what budget they can put in for that year, creating some joint responsibility for the annual budget. Donor coordination and longer term donor commitments would create more efficiency, with less staff time being spend on report and proposal writing.

- **Enlarge DDP team**

As was pointed out in the constraining factors, the DDP team is small, coordinating many activities and the amount of time spend on proposal writing. DDP should consider enlarging the team with additional staff members, or bring in expertise with specific skills, for example on communications, to add to the skills set of the team.

7.3. Recommendations on operational level

Second, some recommendations can be made on the operational level of the program and its interventions.

- **Improve outreach**

The outreach of DDP is a vulnerable element, as DDP now mainly relies on personal networks that can exclude vulnerable critical internet users. Although DDP already collaborates with existing HRD networks, DDP should invest in this more heavily to create broad referral networks. As none of the grantees spoken to in this evaluation were referred to DDP via these HRD networks, it seems that as an outreach strategy these collaborations have not fulfilled their potential. As an outreach strategy and as a preventative measure, some respondents suggested that DDP should produce instructions and other materials in an accessible, easy-to-use form, either as a well-written short booklet, webinars for example on the dangers of not being digitally secure, or digital security in general. A stronger outreach should be balanced against risks for the program's operations and its beneficiaries that will also increase in this case.

- **Improve selection**

In the selection procedure, emphasize the criteria of strategic selection – choose organisations that can have a profound effect in their surroundings and other critical internet users - to create the highest impact. These criteria should also be regularly evaluated internally to ensure that – given limited resources – the strategic selection criteria are effective in ensuring the greatest impact. Here greater coordination with partners or donors could be helpful to ensure maximum impact of DDPs within specific communities.

- **Improve front desk assistance**

Simplify the application form and application process, particularly for the incidental emergency grants. Critical internet users in need should be able to send an introductory mail to explain their emergency and receive hands-on advice how to proceed with a grant application and what is needed for this emergency. For some, writing an email with a project proposition and a budget might be a step to quick.

- **Need for audits and assessments**

Beneficiaries also emphasized the importance of security audit for civic groups as opposed to just providing training or funding. Develop a collaborative approach to help organisations with initial and final diagnosis on digital safety as many of the beneficiaries have not enough expertise or experience on the subject to successfully identify their needs. Although DDP funds this kind of activity via sustainable emergency grants, some critical internet users are not aware of this, particularly those that receive support via a strategic partner or a responder that received a capacity building grant. As

quite a few respondents express this need, it is important that this type of activity is sustained and supported through the grants and possibly also through the strategic partners.

- **Continue with sustainable emergency support**

Continue with sustainable emergency support in addition to incidental emergency support since this is a need is expressed by both critical internet users as responders. Respondents emphasised the need to develop learning activities that could have a real multiplier effect to increase the impact both in terms of scope and depth.

- **Consider a geographical focus for sustainable emergency support**

Keep the global character for incidental support but consider focusing the sustainable emergency support on particular regions, connected to regional response meetings to create digital safety hubs to sustain long-term and wider impacts in countries. Link organisations that benefitted from DDP, both responders and critical internet users. Continue with the holistic approach to address safety, but keep the digital safety always as the main entry point.

- **Establish proof and document added value of long-term mentoring**

From a donor perspective, there is a discussion about the 'mentoring' concept, such as the Digital Integrity Fellowship. Does it remedy some of the shortcomings of one-off trainings, and is it worth the additional costs? While the community clearly agrees that this long-term sustainable is best in principle, how this can best be achieved in practice is open to debate. It is important to establish proof that this approach works and document it's long-term added value in comparison to short-term interventions. Here collaboration with other similar organisations could be helpful to establish credibly what effects this approach actually has and to document the concrete benefits of such an approach.

- **Invest in locally embedded fellows**

The Digital Integrity Fellowship should aim to work more with local embedded fellows, ideally growing from a champion position within an organisation towards becoming a fellow that can help other organisations in the country. Locally embedded fellows could be coached by the more senior fellows that DDP has attracted and serve as a key link between DDP and local and regional contexts. In these examples the power of the DDP network was most evident in its ability to transform entire communities and networks. This ambition is already formulated in the Annual Plan 2017 and if DDP succeeds in realizing this the coming years, the impact of the DIF would likely to be increased.

- **Follow up for grantees/beneficiaries that have been supported in the past**

Training on digital security and safe communication is still necessary for individual activists, HRD organisations and responders, since digital threats change over time. Make periodic follow-ups to update skills including on new tools, and to encourage compliance with safety practices such as email encryption. Consider for example developing a follow-up programme for beneficiaries to assess their progress over time (e.g. every three years). For organisations having external accountability on the implementation of good practices and security protocols can help them to sustain changes and keep the motivation of their members.

- **Invest in rapid response networks, particularly on the regional level**

Evidence of this evaluation seems to suggest that investing in rapid response networks does improve the quality of the response. Particularly on regional levels, responders express a need for regional and/or local networks. We advise to support regional rapid response meetups on a more structural basis. DDP should gather more knowledge and evidence on how responders can benefit best from these networks before starting to facilitate those. Are responders helped with regular meetings to establish trusts, they do want to share work, or are they interested in threat monitoring? Link these regional networks to critical internet users who express need of local continuous support and often do not know who to trust. With these regional networks, DDP should aim to create regional digital safety hubs, that could also increase DDPs outreach.

- To the extent that it is safe and feasible, encourage grantees and other responders in a region (e.g. a country) to share resources and work more closely together as a way of creating long term sustainability to support critical internet users.
- Invest more time in linking the global network of RaReNet to regional networks, and share lessons learned of the global with the regional networks and vice versa.
- With budget limitations in mind, consider replacing the capacity building grant to capacity building of responders within these regional response networks.

- **Consider providing documentation of trustworthy partners**

In several cases, there have been an evident stated need by critical internet users to better know which responders could be trusted. This may be a local organisation who can help with security audits or local language materials, or a hosting provider. In both cases having some form of lists of partners who have been audited/vetted as trustworthy by DDP would be highly helpful while ensuring that these partners are still reasonably protected. If DDP were able to list trusted partners, and DDP would also be known to be a good source for this kind of referral and advice, this would surely serve a need.

7.4. Recommendations with regards to Monitoring and Evaluation

Third, the evaluation team was also asked to reflect on the monitoring and evaluation of the programme to see what could be added to improve the current M&E structures.

- **Standardize template reports for grantees**

The evaluation team reviewed grantee reports and DIF reports and noticed different reporting and documentation styles. It would be advisable to standardize the type of information requested of the different grantees necessary to inform the program progress. The standardization would also enable quicker analyses of the outputs and outcomes of the support given. In addition, the progress of the fellowship is now reported on by the fellows, but at the end of each fellowship, it would be a sensible step to ask the champion of the organization participating in the Digital Integrity Fellowship to report on the impact of the DIF on the organization, using this same template. Please note the second recommendation and make sure that this template report focuses on outcomes and narratives.

- **Less focus on outputs and more on outcomes**

Both in the documentation of grantees and the program itself, there is a tendency to describe what has been done in the organization on a technical level and how the budget was spent, and less on the actual impact is of the support in the organization. In the monitoring process, stimulate grantees and organizations benefitting from the program what the actual impact is in the organization itself, in a narrative format. DDP could aim to collect stories of change – as were collected in this evaluation – to organize proof of the effectivity of the program.

- **Collect more evidence of impact on indirect beneficiaries**

Grants given to responders, such as the strategic grants or the capacity building grants seem not so much to have an effect on the responder, but much more on the critical internet users they support, the indirect beneficiaries. DDP should reflect with the strategic partners, what kind of information they would like to receive on the level of those indirect beneficiaries and in particular consider including not just numbers but short narrative stories (see the Boxes in earlier chapters) to illustrate impacts. Although case examples are given in a confidential Annex, again the focus is on technical aspects of the support and to a much lesser extent to the impact on the indirect beneficiaries. Ideally, this impact narrative should be formulated by the beneficiary itself.

- **Elaborate the Theory of Change narrative and clarify assumptions underlying the different steps in the theory of change**

In this evaluation report, we visualized the Theory of Change, but as time was limited, the descriptive narrative that goes along with it, including all the different assumptions that lie underneath the visual

presentation, was not written out. This is something that the DDP team could work on it themselves, particularly in clarifying the assumptions. For example, the DDP staff has an assumption why the strategic partnership would work better than individual grants to different responders. By making assumptions like these explicit, it would be easier to test if assumptions are correct in real life, for example through monitoring or in a possible end-evaluation in 2019.

- **Pay attention to mechanisms of change within the M&E**

Through monitoring DDP could also aim to learn what the ingredients are that create impact. Or in wording of the realist evaluation approach: to identifying pathways of change. Ask organizations receiving support, what the most important element was in the DDP support that allowed the change. For example, with the rapid response networks, it would be interesting to learn what the exact elements are that lead to change. Is it the networking aspect, getting to know other responders and building up trust, is capacity building, is it the sharing of templates etc.? By knowing what works, it will become easier adept the interventions to maximize impact.

- **Consider readjusting the log frame to the newly developed visual theory of change**

When the DDP team decides to use the visual ToC in future to communicate about DDP, it would be wise to examine the log frame and the ToC to make sure that these fit together. Although the log frame of DDP is worked out well, it could be looked at again from the perspective of the visual theory of Change. For example, '1.5 DDPs strategic partners provide essential help to critical internet users under attack' is clustered in the log frame under '1b. Invest in responsive long-term solutions mitigating digital threats', whereas in the visual ToC, these are clustered under incidental emergency support as agreed on by DDP staff. The Emergency Grants (sustainable response) seem not to be mentioned in the log frame, but would fit under '1b. Invest in responsive long-term solutions mitigating digital threats'.

7.5. Conclusion

To conclude, the Digital Defenders Partnership provides a valuable and important response mechanism to many of the key emerging digital threats around the world. By successfully resisting the pressure to just increase the quantitative output of responses and focus instead on a sustainable and holistic approach it has considerably contributed to innovation within the whole field of digital rapid response. At the same time, DDP is becoming less unique in the field of digital safety. By remaining flexible, agile and responsive to constantly evolving threats in a rapidly developing field, it has seen some of its innovations duplicated by similar organisations. Whilst this is not necessarily a bad thing, since the needs are high and more actors are necessary that support critical internet users in a thorough way, it challenges DDP to ensure its innovative position within the field.

While the field will continue to develop rapidly and DDP will need to continue to innovate, consolidation and greater focus will be equally important for what remains a relatively young program. Thus, elements of the program that had to be developed quickly during its initial development should now be re-evaluated in the light of changed conditions. Here, clarifying roles and responsibilities, improving grantee outreach and selection criteria, ensuring better communications and collaborating with local partners, fellows and networks directly will allow DDP to grow further. Many of these challenges are not unusual for a relatively young program like DDP, however as DDP and the field grow and mature it will be important to resolve them and ensure that they are not just now but also considered in future to be "at the top of the pile."

ANNEX 1 OVERVIEW RESEARCH QUESTIONS AND METHODS

	Desk study	Interview Hivos	Online survey	ToC workshop	Interview critical internet users and responders	Interview external stakeholders	Interviews indirect beneficiaries	Interview digital integrity fellows	Interviews Donors	FGD rapid response community	FGD external stakeholders
1. Quality of program design											
How do the different DDP parts (granting and linking & learning interventions as described in ANNEX 3) interlink and contribute to increased safety & strengthened human rights for critical internet, and increased capacity of the global emergency response ecosystem?	x	x		x							
How does DDPs approach contribute to increased safety & strengthened human rights for critical internet users and increased capacity of the global emergency response ecosystem?			x					x			x
To what extent are DDPs strategy, objectives, interventions, approach and choice of strategic partners still valid and appropriate to needs of critical internet users, emergency responders and the emergency response ecosystem? Are the activities and outputs of the program consistent with the intended impacts and effects?		x	x	x	x	x	X			x	x
How does DDP gear the work to actively include women? Is the target group defined enough?			x				X	x		x	
2. Value of outcomes to participants											
How valuable were DDP outcomes to critical internet users, the emergency response ecosystem, the rapid response community, digital integrity organizations, donors, strategic partners? What has happened as a result of the program?			x		x	x	X	x	x	x	
How do others (non-grantees, others in the response or internet freedom field) experience/recognize/value the DDP program, approach and interventions?						X		x	x		x
What are some of the stories that show the effects of the DDP program? What real difference has the activity made to the beneficiaries? What have beneficiaries done in terms of changing their behaviour so as to avoid or supersede the same threats after going through DDP or grantees interventions? And if they haven't changed anything, why is that?			x		x	x		x		x	
3. Process											
What enabled successful implementation and outcomes to occur? What barriers existed that led to less than successful implementation and outcomes?		x	x		x	x		x		x	
4. Cost Benefit											
Does the value of DDP outcomes outweigh the costs of implementation?		x							x		
5. Lessons learned and recommendations											
What are the lessons learned and recommendation regarding DDPs strategy, objectives, interventions, approach, choice of strategic partners and gender-dimension?	x	x	x	x	x	x		x	x	x	x
What are the recommendations regarding the DDPs log frame and monitoring of results?	x	x		x							

ANNEX 2: INTERVIEW GUIDE FOR (INDIRECT) BENEFICIARIES

Evaluation of the Digital Defenders Partnership (DDP) for HIVOS
by Kaleidos Research

Set-up of the document
This document consists of three main parts. It first outlines the objectives of the interviews, the targeted respondents and provides instructions. The second part provides introductory information that should be shared with the respondent. The third part is the interview guide. The interview guide consists of three main topics:

- Awareness and quality of program design
- Value of program outcomes to participants and society as a whole
- Lessons learned and recommendations

Objective
In order to get a good feeling of the impact of the DDP programme in a local setting and to ensure that local voices are heard, we will conduct three dense case studies in 3 different local contexts. Hivos has selected three countries in three regions of the world where the programme is active: Mexico, Russia and Uganda.

Participants
We aim to conduct 7 in-depth interviews per country. A local researcher who will conduct seven interviews in the local language and report the notes from each interview elaborately in English. Kaleidos Research will identify a local internet freedom expert in each of the three countries. The local expert will make recommendations on who to contact and connect us to at least 4 persons active in the internet freedom scene in that particular country. Together with Hivos, Kaleidos Research will also identify at least 4 persons who are connected to the DDP activities in that country. Via these two routes at least 8 persons are identified and max 7 of these persons are interviewed. Of these 7 individuals who will be interviewed, we have stipulated that we will interview these four types of stakeholders in each country:

- 1 direct beneficiary (received a DDP grant) who is a critical internet user
- 1 direct beneficiary (received a DDP grant) from the emergency response ecosystem
- 3 Indirect beneficiaries, for example human right activists who have been supported by strategic partners, including digital integrity fellows, or local responders that benefitted from DDP
- 2 local external stakeholders or experts who are not connected to the program

Instructions
Before the interview starts, it should be clear to the interviewer on topics are most important to focus on in depth. This decision needs to be made in agreement with the evaluation team.

Material

- Interview guide
- Paper and pen

Secure Methods
To protect the anonymity of the respondents, we have agreed that any data collected is stored only on devices using robust full-disk encryption. All communication involving collected data will only take place using PGP encryption to ensure a high level of protection of communications.
As an interviewer, this means the following:

- Do not use a recording device, keep all your notes on paper and store them in a safe place.

- Do not write down ANY personally identifiable information as part of interview. Any information that you write down on paper should ensure that it is not possible to identify who you spoke to at a later date.
- Any communication about the interviews and in particular the transmission of the notes MUST take place using end-to-end encryption using technologies like PGP, Jitsi or Signal. If this is causing you problems, please get in touch and we will do our best to assist you.
- If you have any questions about these methods, please don't hesitate to get in touch.

The two goals of the program to keep in mind

1. Increased safety for critical internet users under attack
2. Increased capacity of the digital emergency response ecosystem

Semi-Structured Interview Guides
Evaluation of the Digital Defenders Partnership (DDP) for HIVOS
by Kaleidos Research

Introduction

Good morning. My name is …….. …….
Thank you for agreeing to take part in this interview.
I am a researcher working with *Kaleidos Research* to review the Digital Defenders Partnership and to recommend ways to improve the program. Kaleidos Research is a research organisation working on global challenges in Amsterdam, the Netherlands, that is asked by Hivos to conduct this evaluation. We feel it is important that you are able to talk about this in your own language face to face to someone, and that is why Kaleidos has asked me, as a local researcher, to conduct these interviews. During this interview, we will discuss what you know about the DDP program and the situation of critical Internet users in [country]. Any information shared will be kept confidential and used only by our team to develop recommendations to help improve the performance of the programmes. We will anonymise any personal identifiers linked to you in our reports or in any transcripts developed out of this interview. If you don't want to respond to certain question that is ok. I want to emphasise that for this research we will only use devices with robust full-disk encryption and will use end-to-end encryption for the transmission of the notes to Kaleidos.
Do you have any questions about our research?

Name of Interviewer	
Name/Code and function of Interviewee	
Date of Interview	
Duration of the interview	

1. Introduction, needs and context Interview questions and prompts	Comments
Please, give an introduction to yourself and your work. What do you do/what organisation are you part of? How is your work/your organisation valued in your country, e.g. is there pressure against what you do?	These answers should give a background of the respondent and organisation they work for Active on what topic, is this a sensitive topic? Is the respondent at risk, does he/she work nationally or globally?
What are the most pressing (digital) safety issues you encounter in your work? How do these hinder you in your work? How do these digital safety issues compare to non-digital threats, e.g. prosecution, physical attacks, legal restrictions, smear campaigns, etc	Get a feel how digital safety compares to other safety threats.
What are your needs with regards to digital safety?	Probe for: do they need knowledge and skills, networks, tools, money etc.?
Can you explain a bit more about the human rights context in the country?	Get a clearer understanding of the local situation with regards to human rights offline and online. This question will also be discussed with experts, so can be skipped if you feel that the questionnaire is too long

2. Process and quality of program design Interview questions and prompts	Comments
When and how did you first hear about the Digital Defenders Partnership (DDP)?	
How would you describe DDP to someone who is not aware of it? What is the aim of DDP and, in your personal experience, what are the most important services DDP provides? For indirect beneficiaries: have they heard of DDP before this interview? Can they describe its aim and most important activities?	
What is your relationship with DDP? Did you request a grant? For what and why? For indirect beneficiaries: what support did you indirectly receive via DDP? How did they get in touch with the responders that supported them?	For indirect beneficiaries: they could receive digital safety consultancy via digital integrity fellowship or Front Line Defenders, legal support via Media Legal Defence Initiative, or technical support via Virtual Road.
Only for grantees: How do you assess the grant procedure?	Probe for: clear and understandable application procedures, contact with DDP team (at Hivos), trust in how Hivos dealt with confidential data, speed of decision making process
Only for grantees Do you have any recommendations with regards to the grant process	
Only for grantees Do you think it is easy to obtain a DDP grant? Would you have found funding somewhere else, if this funding was not granted?	
What did you do with the grant you obtained? For indirect beneficiaries: what kind of support did you receive, please elaborate what the problem was, what support was given and why you received this support	Indirect beneficiaries: this question is quite broad, but please elaborate quite in-depth how they benefitted indirectly from DDP (a lot of other questions in this block are not applicable) so ask additional questions to get a clear view of what happened in their organisation due to DDP
When trying to solve your need with the grant or the support of DDP, what worked really well?	
What things did not work so well/factors that hindered success?	

2. Process and quality of program design Interview questions and prompts	Comments
Did you also participate in other DDPs activities?	DDP has 3 core activities: grant facilities, linking and learning and capacity building. These last 2 strategies have different activities like: Advice and referral Participated in the Digital Integrity Fellowship as a beneficiary Additional Training Participated in Rapid Responder Network meetings Use of Digital First Aid Kit (online self-help tool) Learning exchanges Mentorship Academy / summer school Other
When reviewing your experience with DDP, do you feel that DDP has adopted a women friendly approach? What could you recommend to make it more women friendly or to target women in a better way?	

3. Value of program outcomes Interview questions and prompts	Comments THIS BLOCK IS KEY IN THE INTERVIEW
What is the most significant change in your work/your organisation due to support you received from DDP? What difference did it make to your work that you received the support of DDP? Important note: Please ensure that none of your response includes information that could allow yourself or other individuals to be identified personally.	Probe for actual changes in how they work. Make sure you ask for changes on the level of outcome, not on output. Not: our website is now securely hosted e.g. That is output. Outcome example: our website is not attacked so now we reach xx viewers a month, there is more awareness and knowledge in our organisation how to work digitally safe etc.
How did DDP contribute to this change?	
How do you value this change?	Probe for negative/positive and unimportant/very important
What would have happened if you were not able to obtain a grant/support?	Without funding, serious trouble?
Was the support you received sufficient to address the needs you had when you applied for the grant/for the support?	
Do you feel that this support was a quick fix for an urgent problem or is it a sustainable solution for the long run?	
After the support from DDP, did other needs emerge with regards to digital safety?	
Did you in any way change the way you work to avoid or supersede the same threats after going through DDP or grantees interventions? What did you change and why? < if they haven't changed anything > Why is that?	DDP aims to actually change behaviour of how CIUs work. So, this question is very important, please make sure you address this properly
For critical internet users: DDP aims to increase safety for critical internet users under attack. Do you feel that the support of DDP led to an increased safety for you/your organisation? For responders: DDP has 2 objectives 1. Increased safety for critical internet users under attack	Check if the respondents feel that the objectives of the program are reached. Mind: Critical internet users can both be direct beneficiaries that received a grant, as indirect beneficiaries that received support via a

3. Value of program outcomes **Interview questions and prompts**	**Comments** **THIS BLOCK IS KEY IN THE INTERVIEW**
2. Increased capacity of the digital emergency response ecosystem Do you feel that with the support of DDP these two goals have been achieved in your case?	strategic partner or a responder that received a grant. For responders goal 2 is both their own capacity as responder as well as the entire responder system (if for example they have exchanged and linked with other responders). Responders are likely to be a grantee.

4. DDP's approach and values **Interview questions and prompts**	**Comments** In case the interview takes too much time, this block can be done a bit quicker
DDP approach is based on 5 values, see below Explain each value one by one with the respondent and ask them how important this value is for them and if they can give an example in their experience with DDP how DDP is adhering to this principle.	See also this webpage https://www.digitaldefenders.org/ Scroll to 'About DDP' to read the guiding principles in more detail For indirect beneficiaries: the strategic partners they received support from, should also adhere to these principles, so check if
Human rights & Internet freedom DDP works with donors, partners, consultants and grantees committed to the universal human	
Trust & Confidentiality Establishing and maintaining trust with partners.	
Mentorship & Partnership A partnership with our grantees on equal footing.	
Quality & Expertise No quick fixes but qualitative and trusted response that increases resilience is vital.	
Not claiming, but facilitating We want individuals and organizations to have and take ownership of their own interventions, activities	
Which of the 5 values do you feel is most important? Why?	
Should values be skipped or replaced with different values?	

5. Lessons learned and recommendations **Interview questions and prompts**	**Comments** This block is important, since we need to feedback how the program can be improved
As far as you are aware, what are they key factors for DDP achieving a successful impact?	If this generic question is too difficult, make it more specific for respondent: what worked really well in your case
In your opinion, what are the main barriers for DDP achieving a successful impact?	Idem: if this generic question is too difficult, make it more specific: what barriers did you experience that DDP should adapt.
In the field of internet freedom, what is the main challenge left unaddressed by DDP?	
DDP's activities focus on three areas: emergency funding, capacity building and linking and learning. Should DDP focus on other issues/causes that are related to digital safety?	
How important is it in your view that DDP reserves budget for emergency funding, that is more focussed to quick fixes, compared to capacity building	

5. Lessons learned and recommendations **Interview questions and prompts**	**Comments** This block is important, since we need to feedback how the program can be improved
that leads to more long term solutions? Should DDP do both or choose one over the other?	
What activities of the DDP, if any, overlap with other programs you're aware of?	Should be asked to name any they're aware of
Based on your experience, what would be your three most important recommendations on what DDP should change?	Probe for: • Should the DDP improve its strategy and objectives? • Should the DDP improve its approach and interventions? • Who do you think DDP should work with as strategic partners?

ANNEX 3: INTERVIEW GUIDE FOR EXPERTS

Evaluation of the Digital Deferenders Partnership (DDP) for HIVOS
by Kaleidos Research

Set-up of the document
This document consists of three main parts. It first outlines the objectives of the interviews, the targeted respondents and provides instructions. The second part provides introductory information that should be shared with the respondent. The third part is the interview guide. The interview guide consists of three main topics:

- Awareness and quality of program design
- Value of program outcomes to participants and society as a whole
- Lessons learned and recommendations

Objective
In order to get a good feeling of the impact of the DDP programme in a local setting and to ensure that local voices are heard, we will conduct three dense case studies in 3 different local contexts. Hivos has selected three countries in three regions of the world where the programme is active: Mexico, Russia and Uganda.

Participants
We aim to conduct 7 in-depth interviews per country. A local researcher who will conduct seven interviews in the local language and report the notes from each interview elaborately in English. Kaleidos Research will identify a local internet freedom expert in each of the three countries. The local expert will make recommendations on who to contact and connect us to at least 4 persons active in the internet freedom scene in that particular country. Together with Hivos, Kaleidos Research will also identify at least 4 persons who are connected to the DDP activities in that country. Via these two routes at least 8 persons are identified and max 7 of these persons are interviewed. Of these 7 individuals who will be interviewed, we have stipulated that we will interview these four types of stakeholders in each country:

- 1 direct beneficiary (received a DDP grant) who is a critical internet user
- 1 direct beneficiary (received a DDP grant) from the emergency response ecosystem
- 3 Indirect beneficiaries, for example human right activists who have been supported by strategic partners, including digital integrity fellows, or local responders that benefitted from DDP
- 2 local external stakeholders or experts who are not connected to the program

Instructions
Before the interview starts, it should be clear to the interviewer on topics are most important to focus on in depth. This decision needs to be made in agreement with the evaluation team.

Material

- Interview guide
- Paper and pen

Secure Methods
To protect the anonymity of the respondents, we have agreed that any data collected is stored only on devices using robust full-disk encryption. All communication involving collected data will only take place using PGP encryption to ensure a high level of protection of communications.
As an interviewer, this means the following:

- Do not use a recording device, keep all your notes on paper and store them in a safe place.
- Do not write down ANY personally identifiable information as part of interview. Any information that you write down on paper should ensure that it is not possible to identify who you spoke to at a later date.

- Any communication about the interviews and in particular the transmission of the notes MUST take place using end-to-end encryption using technologies like PGP, Jitsi or Signal. If this is causing you problems, please get in touch and we will do our best to assist you.
- If you have any questions about these methods, please don't hesitate to get in touch.

The two goals of the program to keep in mind

1. Increased safety for critical internet users under attack
2. Increased capacity of the digital emergency response ecosystem

Semi-Structured Interview Guides
Evaluation of the Digital Deferenders Partnership (DDP) for HIVOS
by Kaleidos Research

Introduction

Good morning. My name is …….. …….
Thank you for agreeing to take part in this interview.
I am a researcher working with *Kaleidos Research* to review the Digital Defenders Partnership and to recommend ways to improve the program. Kaleidos Research is a research organisation working on global challenges in Amsterdam, the Netherlands, that is asked by Hivos to conduct this evaluation. We feel it is important that you are able to talk about this in your own language face to face to someone, and that is why Kaleidos has asked me, as a local researcher, to conduct these interviews. During this interview, we will discuss what you know about the DDP program and the situation of critical Internet users in [country]. Any information shared will be kept confidential and used only by our team to develop recommendations to help improve the performance of the programmes. We will anonymise any personal identifiers linked to you in our reports or in any transcripts developed out of this interview. If you don't want to respond to certain question that is ok.
Do you have any questions about our research?

Name of Interviewer	
Name/Code and function of Interviewee	
Date of Interview	
Duration of the interview	

1. Introduction, needs and context Interview questions and prompts	Comments
Can give an introduction to yourself and your work? What do you do/what organisation are you part of? How is your work/your organisation valued in your country, e.g. is there pressure against what you do?	These answers should give a background of the respondent and organisation they work for Active on what topic, is this a sensitive topic? Is the respondent in risk, does he/she work nationally or globally?
What are the most pressing digital safety issues in your country? From the perspective of a human right activist/journalist/blogger: how are the digital safety problems compared to other safety issues (non-digital threats, e.g. prosecution, physical attacks, legal restrictions, smear campaigns, etc.)? Is digital safety an important issue or not?	
What are the needs of critical internet users (human right activist/journalists/bloggers) in your country. What do they need most to be able to do their work? What are their needs with regards to digital safety? Which groups are most vulnerable with regards to digital safety?	Probe for: do they need knowledge, network, money etc?
Can you explain a bit more about the human rights context in the country?	Get a clearer understanding what the local situation is with regards to human rights
Are there sufficient rapid responders in your country/region, that can support human right defenders/critical internet users when they receive digital threats?	Get a feel of the support system/mechanism for human right defenders in the country
Are these responders in your country/region collaborating together? Why or why not? And how do they collaborate?	DDP also aim to improve linking of responders. This question gives insight if responders already collaborate. Is there an issue with collaborating, is there enough trust between rapid responders?
Are there funds available in your country to support critical internet users that experience digital threats?	
In your work, do you come across many critical internet users that experience digital threats? In general, what do you/your organisation advise them?	

2. Knowledge and assessment of DDP Interview questions and prompts	Comments
Have you ever heard of the Digital Defenders Partnership (DDP)?	
If yes, when did you first hear about the Digital Defenders Partnership (DDP)? What do you know about it?	Can they describe anything about aims or activities of DDP
If the expert don't know anything about the program, take a few minutes to explain how the DDP works and what it does.	The visual Theory of Change, see attachment, can be used as a tool.
DDP has 2 objectives 1. Increased safety for critical internet users under attack 2. Increased capacity of the digital emergency response ecosystem Are these goals fitting for the problems in your country? Or should the goals be adapted, changed?	It is likely that there is an issue with digital safety, but is there also an issue with the capacity of the digital emergency response ecosystem?
How important is it for human right defenders/critical internet users in your country that a funding mechanism like DDP on this topic – critical internet users under digital threats – exist?	
Do you know of similar programs/funds? What activities of the DDP, if any, overlap with other programs you're aware of?	Should be asked to name any they're aware of
DDP's activities focus on three areas: emergency funding, capacity building and linking and learning. Should DDP focus on other issues/causes that are related to digital safety?	
How important is it in your view that this program DDP reserves budget for emergency funding, that is more focussed to quick fixes, compared to capacity building that leads to more long term solutions? What is needed in this country? Should DDP do both or choose one over the other?	
To look from the angle of sustainability, is there a way to improve the safety for critical internet users from a more long term perspective in your country?	

2. Knowledge and assessment of DDP Interview questions and prompts	Comments
Is it important that DDP mainly focuses on digital threats, or should is address safety in more comprehensive way?	The digital integrity fellows and also FLD try to work more comprehensively, not only digital but also other safety issues. Is this relevant and a good approach or is it more desirable to keep the focus specifically on digital threats?
Because of a limited global annual budget of 2 million euros annually, DDP does not advertise/reach out; there are already more applications than they cater for. It means that it is likely that a lot of human right defenders/journalists/bloggers in your country etc. are not aware of this fund. Do you have any idea what types of organisations apply? Does the fund also reaches the group that is most vulnerable for digital threats?	Get an idea wether DDP reaches the group that needs the fund the most.

3. DDPs approach and values Interview questions and prompts	
DDP approach is based on 5 values, see below Explain each value one by one with the respondent and ask them how important this value is for them and how important this programme values are to address this issue	See also this webpage https://www.digitaldefenders.org/ Scroll to 'About DDP' to read the guiding principles in more detail
Human rights & Internet freedom DDP works with donors, partners, consultants and grantees committed to the universal human rights	
Trust & Confidentiality Establishing and maintaining trust with partners.	
Mentorship & Partnership a partnership with our grantees on equal footing,.	
Quality & Expertise No quick fixes but qualitative and trusted response that increases resilience is vital.	
Not claiming, but facilitating We want individuals and organizations to have and take ownership of their own interventions, activities	
Which of the 5 values do you feel is most important? Why?	
Should values be skipped or replaced with different values?	

4. Lessons learned and recommendations Interview questions and prompts	Comments This block is important, since we need to feedback how the program can be improved
To improve the digital safety of human right defenders/journalists/bloggers in your country, what is needed?	
Should this program DDP be adjusted, to fit to the needs of what you just expressed of what is needed in this country?	
DDP is a global fund with a budget of around 2 million euro annually. So in your country only a limited amount of organisation is supported (around 4 to 6 organistions in the last 2 years). Do you think we can speak of an impact of the DDP in your country? Or are these numbers to limited? What would be the best strategy to improve the impact of DDP in your country?	
Based on your experience, what would be your three most important recommendations on what DDP should change?	Probe for: • Should the DDP improve its strategy and objectives? • Should the DDP improve its approach and interventions? • Who do you think DDP should work with as strategic partners?