
Digital
Defenders
Partnership

Digital Defenders Partnership

Narrative and financial report
Q1 2014
January – March

Program information

Grantee:	Hivos
Project title:	Digital Defenders Partnership
Grant Number:	State Department: S-LMAQM-12-CA-1126 Dutch Ministry of Foreign Affairs: 1000293 Republic of Estonia: - Foreign Commonwealth Office: - SIDA: 5403043801 Republic of Latvia: - Czech Republic: -
Country:	Internet repressive and transitional environments
Funding Amount:	State Department: $ 1.250.000 Dutch Ministry of Foreign Affairs: € 1.000.000 Republic of Estonia: € 80.000 Foreign Commonwealth Office: £ 500.000 SIDA: € 1.000.000 (9.000.000 SEK) Republic of Latvia: $ 10.000 Czech Republic: € 10.057
Grant Dates:	State Department: 5-9-2012 / 30-9-14 Dutch Ministry of Foreign Affairs: 1-10-12 / 31-12-14 Republic of Estonia: 2014 Foreign Commonwealth Office: 1-10-12 / 31-12-14 SIDA: 1-1-2013 / 31-12-2015 Republic of Latvia: 2014 Czech Republic: 2014
Quarter (Dates) being Discussed:	1-01-2014 / 31-03-2014
Date Progress Report is submitted:	April 30st 2014
Primary Point of Contact:	Sabine Maresch
Phone Number:	+31 70 3765500
Email:	s.maresch@hivos.nl

Contents

Digital Defenders Partnership
Executive summary
Q1 2014

This reporting period the DDP has conducted several emergency responses in situations of heightened tensions between governments and activists due to civil unrest and protests. In several of these cases, such as the [redacted] governments responded with increasing repressive measures as censorship, intensified surveillance and digital attacks. The Digital Defenders Partnership has been able to act quickly on requests from communities in need, often those most vulnerable for repression and digital threats. By connecting human rights defenders and journalists with organisations that could offer the necessary support, providing emergency grants and through activities of strategic partners.

Furthermore, this period we have established two more strategic partnerships with experienced key-actors in the digital security support for at-risk communities, realizing more capacity for secure hosting and safe communication methods.

A short selection of our cumulative results up to Q1 in 2014:

Grant making;

- Through grant making the DDP supported 14 organisations to mitigate digital threats. The grants provided 351 users with direct emergency response, such as DDoS mitigation for websites under attack, legal support, the replacement of equipment and retrieval of hijacked accounts or temporary digital security helpdesks. On top of that, 164 people were trained on digital security, to make them and their organizations more aware of risks and less vulnerable for attacks.

Strategic Partnerships

- Out of these 14 organisations, the DDP supported 6 strategic partners, involved with key activities, such as providing legal support in cases related to digital security threats, personal and organisational security through regional digital security consultants, secure hosting for very high-risk websites and developing user friendly integrated platforms for secure communication. Furthermore, over 5800 usages a day are supported to circumvent censorship by browsing anonymously by increasing the architecture behind Tor.

Brokering

- The DDP has engaged in various brokering activities for 19 different human rights defenders- and media organisations that suffered a digital emergency. By either providing direct assistance to mitigate the digital threat or broker third party intervention from an extensive network of lawyers, technical specialists and training organisations with specific experience in this area. In some cases, brokering has led to project grants. One of the examples this reporting period, is the brokering activities after an emergency request from journalist and bloggers from [redacted] Besides advising them we connected

them with a Spanish speaking organisation who could support them with digital security issues. This has led to an Emergency Grant for this organisation to provide secure VPN connections, a digital emergency helpline and a mini-guide on safe communication.

Linking and Learning

- The focus of the DDP is not only to connect at-risk communities to the needed specialised support in case of digital threats, but also to strengthen the connections and coordination *within* the digital emergency response community. The DDP continues the facilitation of coordinating different actors working on digital emergency support around the world. This coordination has led to an emergency response group, sharing knowledge, requests and support for solutions. This not only provides the DDP with a trusted entry point for support in digital emergency situations, but also first hand and timely information of digital threats and insight in the needs of at risk communities. Besides advice and coordination of support in different cases, one of the more tangible activities of this group is the development of a digital first aid kit. The first version has been drafted, and alpha testing by organisations working with human rights defenders facing digital emergency threats will start next month. The kit guides journalists, human rights defenders and bloggers in conducting a self assessment to understand if they are hacked or DDoSed. The kit also provides first steps for mitigation. This way organisations with little knowledge on digital security threats will be better equipped to respond to emergency situations.

Spending:

Up to Q1 2014 the cumulative amount that was contracted was 1.139.587,09 Euro/ 1.401.692.12 USD Of which;

- 590.142,07 Euro / 725.874.74 USD has been spend on grants (for Q1 this was a total amount of 210.475,96 Euro / 258.885,43 USD has been spend on grants)
- 549.445,02 Euro/ 675.817,38 USD that has been committed in contracts to sub-grantees that will be disbursed in tranches in 2014.

1. Relevant Context Information

In the reporting period, there were several cases of civil unrest and protests causing governments to respond with repressive measures such as censorship, intensified surveillance and digital attacks.

One such clear example is the Ukraine. As mentioned in our last quarterly report, we received reports that many media who independently report on the large-scale "Euromaidan" protests that broke out in late November were under DDoS attacks and needed help. The political situation meanwhile has completely changed, but there are similar concerns. The events in Ukraine unfolded on a rapid pace in the first months of 2014. In January, the repressive 'Dictatorship laws', curtailing free speech and freedom of assembly, caused mass indignation and radicalized the protests. The civil unrest spread and clashes between protesters and police became increasingly violent. The government escaped the capital Kiev the 22nd of February. Again, we have seen how social media was of utmost importance in disseminating information during the protests.
In March the unrest moved to Eastern Ukraine, the heartland of support for Yanukovych and pro- Russian supporters. In a powerplay of Russia, the region Crimea was annexed by Russian troops. In this highly polarised situation, independent media and critical bloggers are under attack as well. DDoS attacks are still a major issue. In March, multiple NATO and Ukrainian media websites were hit by a pro-Russia group calling itself Cyber Berkut (KiberBerkut).[1] In the Crimea, Ukraine's Ukrtelecom reported that "unidentified uniformed people" seized several of its key telecom nodes and damaged its fiber optic cables and zone networks, resulting in a partial communication shutdown. Crimea may be more vulnerable than the rest of Ukraine because it has only one Internet exchange point controlling all traffic in the peninsula.[2] As tensions continue to rise, the DDP is looking into supporting the protection of human rights defenders, bloggers and independent media who can be unknowingly exposed. More attacks related to the conflict are reported in the region: [redacted]

Another source of civil unrest and political turmoil the last months is Venezuela, where massive anti-government protests have been going on since February. Protesters have been expressing discontent about food shortages, violent crime, inflation and other socio-economic problems, as well as indignation about the repression of the protests. The response of the Venezuelan government is more censorship and other repressive measures. Official media have been curtailed to report on the protests. As in many other cases, valuable information is disseminated through social networks, specially twitter. By smartphone videos and photographs of ample aggressions of the repression forces are spread. But

[1] http://jeffreycarr.blogspot.co.uk/2014/03/cyber-berkut-and-anonymous-ukraine-co.html
[2] http://advocacy.globalvoicesonline.org/2014/03/12/netizen-report-leaders-at-odds-over-social-media-in-turkey/

activists and media workers using social media to report on protests are also facing big hurdles. Since protests escalated, hundreds of blogs and websites covering news and political issues have been reported as blocked, people throughout the country have reported difficulty accessing Twitter and a dramatic overall drop in internet speed. Furthermore, communication through chat app Zello was blocked after the government denounced it for being used to organize recent protests and citizens have been arrested for spreading "destabilizing" information through social networks.
While implementing measures to restrict the flow of information online and developing a base of social media followers who spread pro-government information and hashtags (the so-called "guerrilla communication").
Journalists and activists actively reporting on expressed concern about mobile phone seizure and surveillance through our contacts, and we also received reports of mobile phones being confiscated and records deleted. In response DDP set up and supported various activities to improve security, such as a mini-guide for digital security and a helpline.

Censorship and repression of critical media and journalists is a common reflex of the Erdogan administration in Turkey. New internet restrictions give telecoms authority the power to order a webpage blocked without a court order. These restrictions are seen as a reaction on dissent and (online) publication of documents and audio recordings exposing of high level corruption of Prime Minister Erdogan's inner circle. He showed his threat to a block on major social media sites, was not en empty threat by blocking access to Twitter on 20 March 2014. The ban was hardly effective; Turkish users massively circumvented the block by using text-messaging services or disguising the location of their computers, and internet analysts reported a surge in tweets since the ban was imposed.[3] The government in turn, responded by limiting the possibilities of circumvention.[4]Acces was restored beginning of April, when the nation's Constitutional Court ruled that blocking the site was an illegal violation of freedom of expression and after the reelection of Erdogan. Meanwhile YouTube remains completely blocked, even though criminal court has determined that the block should be limited to 15 specific videos on the platform.

In Egypt the case of prominent blogger and activist Alaa Abd El Fattah keeps dragging on. After more than 100 days in prison, he was brought to court March 23th. The judge ruled that he would be released on 10,000 EGP bail. The charges against Abdel Fattah still stand. On the day of his release 500+ pro Morsi supporters where sentenced to death for their involvement in protest. In these protest a police officer died and all 500+ people where held responsible fort his death by the Egyptian court. Later the wife of the police officer who died stated to the press: it is good that they got sentenced, to bad the people who killed my husband where not amongst them. After pressure from the international community the Egyptian president has said they will look into this verdict.

---

[3] http://www.theguardian.com/world/2014/mar/21/turkey-twitter-users-flout-ban-erdogan
[4] http://www.theguardian.com/world/2014/mar/23/turkey-twitter-ban?INTCMP=ILCNETTXT3487

Chinese internet watchdog GreatFire reported[5] on the greatest internet outage in China last 21nd of January, affecting two-thirds of Chinese internet users. Greatfire analysed the outage, and concluded that ironically, it was a mistake in censorship measures: instead of preventing access to sites that Chinese authorities wanted block, they accidentally may have directed vast amounts of Chinese internet traffic to those sites[6]. One of the theories of GreatFire is that the Chinese out to attack their unblockable mirror websites.

2. Programme Activities

The DDP aims to keep the internet open and free from emerging threats specifically in repressive and transitional environments. In Q1 the DDP has engaged in grant making, research, linking & learning and brokering which contribute to the DDP's aim under the outcomes: A. Increased safety and improved opportunities for emergency support for the internet's critical users (m/f) like bloggers, cyber activists, journalists and human rights defenders when under threat and B. Strengthening emergency response capacity amongst relevant stakeholders (DDP, partners and other stakeholders). Below more information on each activity can be found.

2.1 New granting structure

One of the lessons learned from 2013 is that we had change the granting structure to make the distinction between the different types of support provided by the DDP more clear, make it easier for potential grantees to apply and focus more on emergency and direct support. In consultation with the donors the new structure was adopted. These new grant types clearly emphasize that the DDP can also be approached for emergencies and smaller grants, to be granted in a relatively short timeframe. The DDP has now three different types of grants[7]:

1. Emergency Grants to critical internet users who are facing an urgent digital emergency in internet repressive environments. These grants provide direct advice and financial support to individuals with emergencies related to cyber attacks, compromised accounts and devices, secure connection and legal support. The grants can provide to a maximum of 5.000 USD, run for a maximum of four months and can be awarded within one week. Eligible grantees for emergency grants are journalists, HRDs, NGOs, activists and bloggers.
2. Direct Support Grants are aimed at supporting the improvement of digital security apparatus of organisations suffering from digital attacks, set up temporary helpdesks or test and research specific threat. These grants can provide to a maximum of 50.000 USD, run for a maximum period of one year and can be awarded within a minimum of one month. Eligible

[5] https://zh.greatfire.org/blog/2014/jan/internet-outage-china-jan-21
[6] *http://www.bbc.com/news/blogs-echochambers-25868297*
[7] More information on the new granting structure can be found in Annex 1

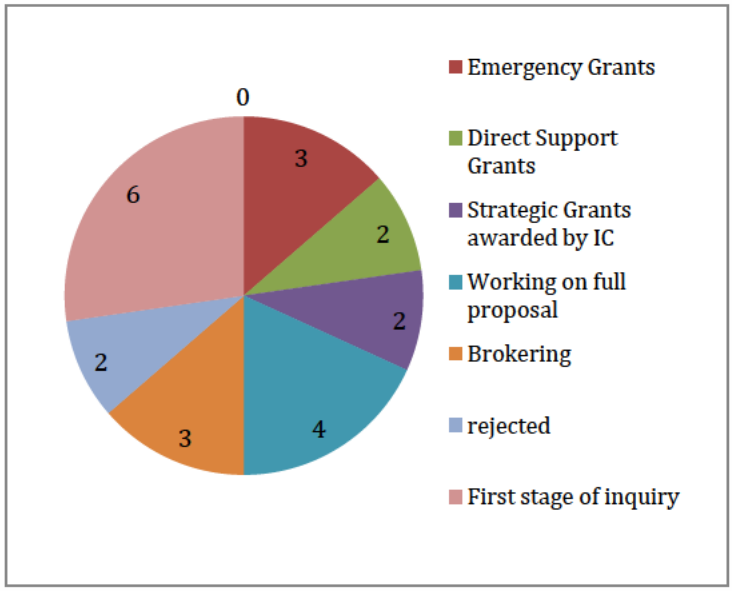
grantees are HRDs-, media- and bloggers organizations that mitigate digital emergencies.

3. Strategic partnerships to non-government organisations and professionals working to strengthen the digital emergency field. These grants can provide to a maximum of 400.000 USD and run for a maximum of two years. Eligible grantees are NGO and professionals that work to strengthen the digital emergency field.

It should be noted that for grants under the 50.000 USD (Emergency Grants and Direct Support Grants) the Investment Committee and Donor Committee are only consulted if it is a sensitive grant.

2.2 Grants making

Since the start of the DDP the programme has received 67 project ideas, of which 45 in 2013 and 22 already in Q1 2014. In Q1 three emergency grants and two Direct Support Grants have directly been awarded by the DDP secretariat, and two grants have been approved by the Investment Committee. Three project proposal where supported directly by the DDPs brokering activities as they required direct and not financial support. Two proposals where rejected as they did not fit the mandate from the DDP. The remaining 10 proposals are in varying stages of development ranging from simple inquiries for possible funding to brief project ideas to comprehensive project plans that are almost ready to be presented to the next IC meeting. Generally, if a proposed idea fits the mandate of the DDP and shows promise, the DDP secretariat will mentor the potential grantees by bouncing the proposals back and forth with the organizations before officially presenting them before the Investment Committee.



[redacted]

2.3 Investment Committee

Approved

[redacted]

[redacted]

[redacted]

[redacted] These report are meant to to raise awareness within the organisation on the threats they are facing, but also give them proof about the attacks when talking to advoc org./policymakers/donors. [redacted] contract of 189,559 Euro has been signed.

Leap (public)

LEAP and Riseup are two organisations that working on secure online communication tools. The platform that they are developing aims to make encrypted internet and secure email easy. Once finished organisations and service providers can easily host their own secure communication and also provide it to others. LEAP and Riseup are working on this project because they believe that front line human rights activists, journalists and bloggers do not have access to secure communication due to current barriers that include: the complexity and cost involved, lack of secure tools, linguistic barriers and the fact that most communication systems are designed without the particular needs of repressive contexts

Under the Digital Defenders Partnership Hivos will support LEAP and Riseup to finalize the development of their platform; to offer encrypted internet and secure email services to its users. The project will result in a stable and mature platform for secure communication. The organizations will test and continue to improve the platform and client to the point where the system can be recommended for more repressive contexts. The proposed project will be a first step towards the ultimate goal of a global ecosystem of secure service providers offering services in the local languages and where these services are most needed.

The DDP and the Investment Committee saw the importance of finalizing the development of a service like LEAP and Riseup in the digital emergency field, as critical internet users, NGO's and media organisations in developing countries are targeted due to the lack of secure communication lines and email services. Since the NSA revelations many of the critical internet users lost faith in the bigger email providers and are looking for alternatives. Riseup has seen a very big increase in their user base in the Global South. This platform should make it easier for organizations and providers to run their own secure mail servers and internet connections. This will be dummy proof. A contract of 249,947.52 USD has been signed.

Emergency grants

[redacted] Police have been taking demonstrators phones, reviewing and deleting data and images. Twitter and other media have been blocked and there has been talk about throttling and cutting the internet and mobile networks.

The DDP has provided advice and PGP training but the protesters need more assistance [redacted]

To strengthen their expertise they have also asked if the DDP can support the participation of their security person at Rights Con. We think he would be a very valuable person to participate in the 2nd Rapid Response [redacted] in helping people on the ground. A contract of 3,280 USD has been signed.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Direct support grants

[redacted]

[redacted]. They came to the DDP with a request to 1)test secure communication tool with their target group 2) swap infected equipment from their network [redacted]

[redacted]

[redacted]

[redacted]

[redacted] They do advocacy work and they document and report human rights violations in [redacted] With the increased crackdown on human rights defenders and (digital) attacks there is a great need for [redacted] to invest in equipment to do their work securely and to

increase their digital security for the protection of their team and witnesses that assist in their work.

[redacted]

[redacted] support for an investment several aspects of their digital security.

1. Clean devices for the team on the ground in [redacted]
2. Training of trainers to a have digital security trainer in [redacted] who can train their staff
3. Secure data storage and sharing devices [redacted]

A contract for [redacted] has been signed.

2.4 Partner results

Since the start of the DDP 35 organisations have benefitted directly through the DDP grant making mechanism or through the DDP brokering mechanisms. This has been 14 grants to the organisation mentioned in this report or in the 2013 reports, and brokering for 21 organisations. A total of and 351 individuals have been supported by the DDP brokering activities or our partner results (see annex 2 Logframe).

Specifically in this reporting period, the DDP and our partners established the following results; 7 grants have been awarded and mentioned above. A total off 43 organisations and 95 individuals have been provided emergency support by the DDP and its partner organisations through DDoS mitigation, secure hosting, legal support, replacement of equipment, cleaning off malware, reactivation and blocking of email and social media accounts.

MLDI continued its defense and legal advice for bloggers, journalists and Human Rights Defenders under threat. During the reporting period, MLDI provided financial assistance for the defense of four new cases and legal advice in a further two. Overall, ten cases have been supported under the project, of which 6 were individual cases of activists and bloggers under threat

[redacted] Assistance was related mostly to personal digital security, infrastructure in organizations and defence of websites and web-tools from attacks (such as DDoS and potential intrusion). Since December, the [redacted] supported 11 organisations and 34 individuals.

[redacted]

The project developer has already tackled several elements of these issues and after an initial delay work is progressing at a steady pace. Expected completion of this part is expected in May.

On technology to mitigate digital threats during Q1, we can report more progress on the Tor project. Another server was added in March. All four servers are now up and running, with each of the servers hosting 253 bridges. This strengthens the decentralized model of Tor and increases the speed and anonymity of users in internet repressive regimes like [redacted] Between 1500 - 2000 users run through the 250 IPs/bridges each day.

To create a security management framework, [redacted] Chief Security Officer and Security Manager participated in a 5-day Security Management course. Through this training, both participants gained the knowledge and tools to design a solid security policy, including guidelines on how to implement, train and involve members of staff.

2.5 Linking and learning

The linking and learning mandate of the DDP has always included efforts to better coordinate the international rapid response between different actors and to be better prepared to digital emergencies as a sector. In this light the DDP organized a [redacted] meeting, Secure Hosting and Rapid Response coordination meeting in 2013. In the Q1 of 2014 Access now organized the second Rapid Response meeting prior to Rights Con in San Francisco.

Second Rapid Response meeting

Access had the lead on organizing the second meeting, however due to illness of one of the key staff, the DDP stepped in a week prior to the meeting to help and get the agenda and all of the meeting on its way.

The topics that were discussed where;

1. Catch up; what have we done so far, what is working and what is not working and what is on which to do list
2. Create a plan for approaching commercial companies at Rights Con and asking for more streamlined access to their 24/7 support desks
3. Continue the discussion on DDoS mitigation; what are the biggest challenges, where can we work together and is there a good overview of when to turn to which secure hosting organizations
4. Next steps; how to move forward from here and how we can grow and include other people without killing the cooperation that exists at the moment
5. A third meeting will be held at Stockholm Internet Forum, as most of the organisations involved with the Rapid Response Coordination are already there

The DDP will follow up on all the things that were put on the to do list in Q2, as we have been pushing the coordination between the different actors in the Rapid Response network. We will also work on the next Rapid Response meeting

Digital First Aid Kit

The day after Rights Con the DDP and a small group of the Rapid Response network came together to make the triage document, from the first meeting, readable. The first step was to turn it into a self-help guide called the Digital First Aid Kit. We are about 90% ready and in Q2 the Digital First Aid Kit will be published in its Beta phase on all the Rapid Response network websites. It will also be published on Github so that people can add and change the content. Once this is done we will publish a definite format.

Research

The temporary communication officer has been working to get the scouting missions in a readable format, proofread, take out the sensitive information and brand it with the DDP design. They will be published early Q2.

Brokering

More people are directly reaching out to the DDP and we are together with our strategic partners and others trying to mitigate digital threats to critical internet users. In the unrest of [redacted] the DDP has brokered the following things.

[redacted]

[redacted] The person was recommending that people back up their data in the cloud but he wanted advice on the safe use of mobile phones for reporting on the protest. Together with our strategic partners we gave advice and the DDP also gave online PGP training to the intermediary who where in contact with groups on the ground.

After this it was decided that timely advice from Spanish speakers, secure internet connections and some materials was needed with independent media and bloggers, so the DDP approach [redacted] if they could do this for us. Under there contract they set up a temporary Spanish speaking digital security helpdesk, VPN connections and the distribution of mini security guides.

Then there is also a reversed type of brokering, where the DDP brokers between findings from the technology community and the people at risk. The DDP got approached that there was a suspicion of compromise of devices of human rights defenders and media organizations in the Middle East. As we suspected that some of their devices were compromised we could not reach out to them directly. Therefore, the DDP spend 2 weeks looking for trusted contacts around these people and organisations, talked to them and explained the issues and helped them clean up their computer. In total these where 3 organisations and 5 individuals.

[redacted]

[redacted]

3. DDP Management Activities

3.1 Communication and Outreach

After the first year of setting up the program, reaching out to different target groups and learning by doing, the DDP secretariat has reviewed their grant making mechanism and communication strategy. One of the findings was that potential grantees were unaware that the DDP also offers small grants and individual support and that the DDP was not visible enough online. Based on these and other findings, the DDP drafted a communication strategy for a more structural approach towards communicating on-and offline. Aim of the strategy is to inform target groups about the activities of the DDP and on how the programme can contribute to their work. More specifically, the target group will know about:

- The work of the DDP and their objectives
- The structure of the DDP in terms of grants, brokering etc.
- How to get in contact with the DDP secretariat
- Which events the DDP participates in

The strategy contains several activities and outputs, including one-pagers, leaflets and flyers about the DDP and its grant mechanism, a new online application format, updating and clearly display the website and a more extensive outreach to the target groups about the activities of the DDP via website, twitter and email.

The DDP hired a temporary Communication Officer (1 day a week) to coordinate and complete above results. She developed several communication materials, updated the website and set up the online application format.

The DDP team worked on a fact sheet that clearly describes the program and the opportunities for potential grantees to get support. The fact sheet describes the three types of grants, which activities can be supported with each grant, who can apply for each specific grant, the assessment criteria for an application and how potential grantees can submit their proposal. It has been edited and will be broadly distributed after it has been designed in the DDP style. For the final edited text version, please have a look at annex 1.

A general flyer that will inform all who is interested in the DDP about its grant making mechanism, brokering activities and research is being drafted. It will include a number of results of the DDP and examples of grants awarded so far.

Website
The text on the website about grants is adapted in line with the new grant structure. Also, an online application form is uploaded on the website, allowing potential grantees to fill in their contact information and support requests online for emergency grants and direct support grants. It is now being finalized an once the application form is completed a notification email will be send to grantsddp@hivos.org. Please take a look at the online application form at www.digitaldefenders.org.

Twitter
The tweets on the DDP twitter account intensified over the last couple of months. On average 10 tweets are send out every day and as a result the number of followers more than doubled to 300. Twitter seems a good way to both spreading news about the DDP and giving updates about the events DDP visits.

An announcement about the change in granting mechanism and the new online application form on the DDP website, will go out to the DDP's network in the beginning of Q2. This news announcement can be found in Annex 3. It will be supplemented with the grant fact sheet. Also, the DDP will send out a fact sheet that highlights the results accomplished in 2013 and examples of grants awarded.

3.2 Staff and distinction between roles and responsibilities

As described in the reflection on the DDP in 2013, the DDP moved more into the brokering role and direct assistance of our target group that is under attack. For these new tasks we felt that the secretariat was lacking technical expertise and implementing power, as part of the SIDA grants the DDP has the opportunity to hire this expertise. The programme officer is starting April 1st and we are still looking for the technical officer. The DDP is also still looking for a junior programme officer as we had to let go of the previous one. He worked until the end of February. With the increase of staff a cleared distinction between the roles and responsibilities is needed and in Annex 4 a draft of this can be found.

In Q1 we also hired a temporary communication officer, who will be assisting the DDP to push a number of specific issues forward. Namely; the execution of the communication plan, creation and communication on the new granting structure and grant fact sheet, publishing of the scouting missions and communicating on the results of the DDP.

4. Proposed activities for next quarter

Grants management (activity 1.1)

The DDP Secretariat will have a number of activities going on under grantmaking in Q2 2014. Continue rolling out the emergency and direct support grants, in certain cases both grants can complement the brokering the DDP is doing. There will be an IC meeting mid May to review proposal.

Linking and learning (activity 1.2)
Scouting mission: These will be published in Q2
Meetings: the follow-up of the Rapid Response Coordination meeting will be organized by the DDP after the Stockholm Internet Forum. And the DDP will also work together with activists, bloggers and journalists to create strategies for political and high profile sensitive events.

DDP management activities
Communication and outreach: continue working on the implementation of the communication strategy with the distinction of the different target groups. In addition engage more with the FOC members and providing information to the Embassy's of these countries on what the DDP can do to help people that come to them.
Staff: The DDP still needs to hire 2 new staff members, a Technical Officer and a Junior Programme Officer.
Additional donor support: Develop a Hivos/DDP standpoint on including non Freedom Online Coalition support to the DDP and put this to the Donor Committee.
Monitoring and evaluation: draft a terms of reference on a programme evaluation. In the next quarter we will also focus on evaluating one of our partners activities.

5. Monitoring and evaluation

The DDP has engaged in an financial audit of the programme which will be send separately.

5.1 F-Framework indicators

F Frame indicators cumulative for 2013 and Q1 2014

- 282 of CSO actors trained in circumvention or digital safety technology
- 5 of USG supported online tools developed or improved to maintain an open Internet
- 5008 of individuals or organizations operating in internet repressive countries that are provided with technological assistance to increase online security[8]
- 17 of USG assisted campaigns and programmes to enhance public understanding, NGO support and media coverage on digital threats and promotion of the internet

[8] The Torserver bridges supported by the DDP have an average of 5800 usages a day. We do not know if these are unique visitors, due to the anonymity therefore we use the number 3000 users.

6. Budget narrative

The financial report over Q1 2014 consists of two parts; 1) A financial report for the period Q1 2014, 1st of January to 31st of March in Annex 5 2) an overview of 2014 budget versus expenditure versus commitments in Annex 6 and Annex 7.

Cumulative a total amount of 867.938,69 Euro / 1.067.564,59 USD has spend in 2012, 2013 and Q1 2014. Of which;

590.142,07 Euro/ 725.874,74 USD has been spend on grants
277.796,62 Euro/ 341.689,85 USD has been spend on personnel, travel and other costs

In addition a total amount of 549.445,02 Euro / 675.817,38 USD has been committed in contracts to sub-grantees that will be disbursed in tranches in 2014 and beginning of 2015.

The **total amount spend in Q1** is 266.867,04 Euro/328.246,46 USD of which

210.475,96 Euro/ 258.885,43 USD has been spend on grants
56.391,08 Euro/ 69.361,03 USD has been spend on personnel, travel and other costs

In making the budget DDP has taken a fixed exchange rate of 1.23 for the Euro and Dollar conversion, in the quarterly reports we use this conversion rate.

The Q1 financial report
The financial report is divided into 4 main line items; 1. Activities 2. Direct Management Costs 3. Office 4. Other costs and services:

1 Activities:

1.1 Grant making: in Q1 three emergency grants, 2 direct support grants and two regular grants have been approved. In addition, for two contracts that where signed in 2013 the second payment upon contract has been made.

1.2 Linking and learning the last payments for the Rapid Response Coordination meeting in December of 2013 and for the scouting mission, the payment for the translation of a CIS scouting report and final payment for the MENA.

2 Personnel:

Hivos is responsible for the overall management of the DDP. In Q1 has one full time employee for three months, the Programme Manager. One full time employee for two months, due to termination of contract, the Junior Programme Officer. Two part-time staff members were employed, 1 day the secretariat and 1 day the financial officer. One communication officer for one day a week for two months

3 Office:

4 Other costs:

4.1 Communication: Costs have been made including an application form in the website for the new granting structure.

4.2 Travel: In Q1 the programme manager has travelled to Boston, San Fransisco and Toronto. The costs include international airfare, in country travel and per

diems are charged here. It also includes the flight to Geneva for a Freedom Online Coalition meeting.

4.3 Annual meeting: these are the costs of the teleconferencing meeting of the Investment Committee

4.4 Other costs, miles declaration to Hamburg and calling credit

Annex 1 Grant Fact Sheet

Digital Defenders Partnership

GRANT FACT SHEET

The Digital Defenders Partnership is a grant-making mechanism that coordinates digital emergency response and provides financial support through three types of grants:

- *Emergency Grants* to critical internet users facing an urgent digital emergency in internet repressive environments. These grants provide direct (legal) advice and financial and other support to individuals with emergencies relating to cyber attacks, compromising of accounts and devices and secure connections.
- *Direct Support Grants* aimed at providing advice and support to organisations suffering from digital attacks and seeking to improve their digital security apparatus, set up temporary helpdesks or test and research specific threats.
- *Strategic partnerships* to NGOs and professionals working to strengthen the digital emergency field.

'THE WEB DOES NOT JUST CONNECT MACHINES, IT CONNECTS PEOPLE.'

TIME BERNERS-LEE, DIRECTOR OF THE WORLD WIDE WEB CONSORTIUM AND 'FATHER OF THE INTERNET'

EMERGENCY GRANTS

What constitutes an emergency?
An emergency is an urgent need for assistance arising from threats to the individual's or organisation's security. A digital threat can range from cyber attacks to loss of property or equipment and legal proceedings.

Types of emergency support
Emergency grants are intended to provide small and timely financial emergency assistance to individuals and organisations who are suffering from a cyber attack. Emergency grants can provide a maximum of 5,000 USD, run for a maximum period of four months and can be awarded within one week.

The grant can be used for urgent needs such as:
- digital security audits for organisations
- equipment replacement
- secure hosting
- VPN connections
- safe internet connections
- finding legal representation
- payment of legal fees
- other types of urgently needed expenses

Who can apply?
Journalists, human rights defenders, NGOs, activists and bloggers who come under attack because of their online activities in internet repressive and transitional countries and are in need of immediate financial emergency assistance.

DIRECT SUPPORT GRANTS

What constitutes a digital threat?
A digital threat faced by organisations working on human rights, media or blogging can range from cyber attacks, unsafe data use, compromising of devices or weak digital security practices.

Types of direct support
Direct Support Grants are intended to provide small and timely financial support. Direct support grants can provide a maximum of 50,000 USD, run for a maximum period of one year and can be awarded within a minimum of one month.

The grant can be used to:

- Provide temporary helpdesk or other support needed to mitigate a specific digital emergency situation that affects a larger group of independent media, human rights defenders, journalists, bloggers and activists. These emergencies can arise during elections, periods of protest or other politically sensitive times.
- Kick start the digital security of journalists, activists, human rights defenders and blogging organisations by engaging in a security assessment and implementing the subsequent recommendations that focus on infrastructure, incidence response procedures and/or digital security training. The following can fall under infrastructure: web hosting, secure mail hosting, encryption, burner devices, VPN or equipment replacement.
- Test and research a specific threat to the critical internet user in a specific repressive country.

Who can apply?
Human rights defenders-, media- and bloggers organisations that mitigate their own or others' digital emergencies in internet repressive and transitional environments.

STRATEGIC PARTNERSHIPS

Strategic partnership grants are meant for those organisations that are working to target a specific need and build capacity on this need in the digital emergency response field. Emergency response capacity can be both technical, personal protection and organisational development. The support can only be awarded if it concerns a project in internet repressive and transitional countries.

Who can apply?
NGOs and professionals working to strengthen the digital emergency field, or working to mitigate threats in a specific repressive country.

ASSESSMENT CRITERIA

Emergency and direct support grant applications will be assessed and approved or rejected by the DDP secretariat. An independent Investment Committee will review the strategic grants. The following criteria will be used for assessing the applications:

- Nature of emergency support: the project must fall within the aim of the Digital Defenders Partnership, i.e. provide emergency response to urgent digital threats to critical internet users and/or keeping the internet open and free
- Activities concern repressive and transitional environments
- The activities benefit critical internet users, independent media, human rights defenders, journalists, bloggers and activists
- Need and context assessment
- Technical need, feasibility and security
- Value for money
- Complementarity
- Organisational track record
- The DDP secretariat will inform the potential grantee about the outcome.

SUBMIT YOUR APPLICATION

- Applications for emergency and direct support grants can be submitted by completing the online grant application format on our website www.digitaldefenders.org.
- Potential grantees for strategic grants can submit their proposal to the DDP secretariat via email at grantsddp@hivos.org.
- If you are in need of direct assistance or have questions about digital emergencies you can also send an email to the DDP secretariat at grantsddp@hivos.org.

For more information on the Digital Defenders Partnership please look at www.digitaldefenders.org, contact us via email at ddp@hivos.org or follow us on Twitter @DigiDefenders.

Hivos
people unlimited

Hivos
Attn. Digital Defenders Partnership
P.O. Box 85565
2508 CG Den Haag
the Netherlands

Ddp (at) hivos.nl

+31 (0)70 37 65 500

Ontwerp: Redamo

SWEDEN
Ministry of Foreign Affairs of the Netherlands
Ministry of Foreign Affairs of the Czech Republic
Foreign & Commonwealth Office
Republic of Estonia Ministry of Foreign Affairs

Annex 2 Logframe DDP

Outcomes	A. Increased safety and improved opportunities for emergency support to the internet's critical users B. Strengthening emergency response capacity amongst relevant stakeholders			
Indicator	Baseline	Estimated Target	Actual Target	Data Source
A.1 Number of users in target countries reached by infrastructure, software and/or hardware solutions		x per year	3400	Report of grantees, evaluations
A.2 Number of context specific examples of people benefiting from interventions supported by the DDP	0	3 per year	11	Report grantees, fieldtrips/conversation with grantees and beneficiaries
A.3 Percentage of the campaigns of the DDP that have resulted in national or international pressure on a regime			2	Reports grantees, evaluations, press attention
B.1 Number and type of emergency response that has been provided to critical users by DDP grantees	0		13 different types, 237 people and	Hivos management system, report of grantees, evaluations
B.2 Number of context specific examples of how increased knowledge has equipped individuals and organisations to counter threats to internet freedom		3 per year	4	Report grantees, fieldtrips/conversation with grantees and beneficiaries
Outputs	1. Provision of secure communication and online security for critical users under threat 2. Increased emergency protection for critical users who are subject to immediate danger because of their activities 3. Digital emergency response mechanisms developed and established 4. Improved knowledge of stakeholders on emerging threats to the internet and greater effectiveness of emergency response mechanisms			
Indicator	Baseline	Estimated Target	Actual Target Cummulative Q4	Data Source
1.1.1 Number of organisations directly supported	0	35 by the end of 2014	57	Hivos management system
1.1.2 Number of individuals directly supported	0	5 by the end of 2014	351	Hivos management system
1.2 Number of technological inventions	0	4 per year	4	Hivos management system
1.3.1 Percentage of infrastructure or technology development projects with a direct feedback loop mechanism	0%	75%	1	Hivos management system, reports grantees
1.3.2 Percentage of feedback loops with specific attention to gender	0%	50%	0	Hivos management system, reports grantees

2.1 Percentage of people who requested immediate support that have been assisted	0%	80%	100%	Hivos management system
2.2 Percentage of cases in which the nature of the threat can be matched to a specialized organisation	0%	80%	80%	Hivos management system, reports grantees
3.1 Number of organisations that have been supported to set up emergnecy internet desks	0	3 by the end of 2014	1	Hivos management system
3.2 Number of global events on emergency response organised by DDP	0	1 per year	1	
3.3 Percentage of trainees that know how to secure data after an attack	Unknown	75%	0	report grantees, evaluations
3.4 Number of peer-to peer exchanges organized by DDP	0	2 per year	#REF!	Hivos
4.1 Number research projects implemented	0	4	5	Hivos
4.2 Research project with a focus on gender needs in relation to activism, internet security and emergency response	0	1 in 2013	1	Hivos

Annex 3 Announcement new Granting Structure

DDP announces new granting structure and opens up an online application form

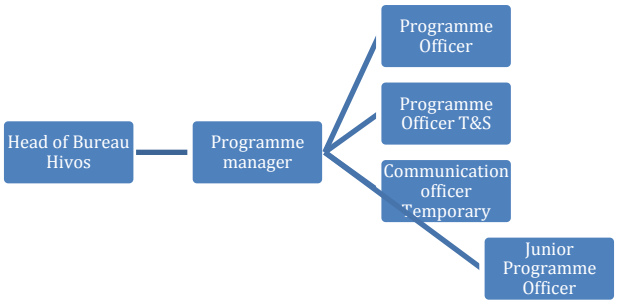
The Digital Defenders Partnership is pleased to announce a new granting structure and online application form for submitting grant proposals. As of today, potential grantees can apply for three different types of grants:

1) **Emergency Grants** to critical internet users who are facing an urgent digital emergency in internet repressive environments.
2) **Direct Support Grants** to support the improvement of the digital security apparatus of organisations suffering from digital attacks.
3) **Strategic partnerships** to non-government organisations and professionals working to strengthen the digital emergency field.

Applications for emergency and direct support grants can be submitted by filling in the online grant application form. Potential grantees for strategic grants can submit their proposal to the DDP secretariat through email at grantsddp@hivos.org.

For more information on the new granting structure and eligibility criteria please take a look at the Grants section on this website.

Annex 4 Roles and Responsibility DDP secretariat



Roles and Responsibilities
Programme manager:

- General oversight DDP
- Daily management staff DDP
- Reports to the Head of Bureau Culture, ICT and Media
- Responsible reporting to back donors and Hivos
- Responsible for the management of the Investment Committee
- Responsible for the grant making programmes
- Outreach to human rights, journalists and activism forums
- Present the DDP and the work of partner in forum and panels
- Building network of on the ground 'consultants' in the region
- Coordination rapid response efforts

Programme Officer

- Communication on the direct support opportunities for target group under threat
- Development and deployment of direct support and incidence response to target group
- Co-responsible with Technology and Security officer for the small grants programme and the rapid response efforts
- Assist the Programme Manager with the overall DDP programme
- Building network of on the ground 'consultants' in the region
- Present the DDP and the work of partner in forum and panels
- Reports to Programme Manager and falls under by the Head of Bureau Culture, ICT and Media

Programme Officer Technology and Security:

- Development and deployment of direct support and rapid response to target group
- Co-responsible with Programme Officer for the small grants programme
- Research and forensic analysis on digital threats
- Communication on digital threats
- Assessment of technical component of grant request
- Building, maintaining and coordinating with the larger technology and security sector
- Present the DDP and the work of partner in forum and panels
- Reports to Programme Manager and falls under by the Head of Bureau Culture, ICT and Media

Junior Programme Officer:

- Supportive in the project administration of the DDP
- Communication support to Programme Officer and Programme Manager
- Supportive in quarterly and annual reports
- Update website and work on DDP twitter account
- Assist the Programme Manager in organizing events
- Administration responsibility
- Reports to Programme Manager and falls under by the Head of Bureau Culture, ICT and Media

Communications Officer (Temporary[9]):

- Implementation of the DDP Communication plan
- Creation of communication material (1 pagers of the different grants, successes of the DDP, press statements on new grantees etc.)
- Creation and communication of Call for Proposals
- Preparation of the DDP present and PR during the Freedom Online Coalition meeting in Estonia, Stockholm Internet Forum 2014 etc.
- Update website and work on DDP twitter account

[9]This position is temporary and designed to take over some tasks till the new staff for the DDP is hired and they will take over these tasks

Annex 5 Financial Report Q1 2014

Total expenses	Amount Spend Q1 2014			Total Q1	Total Q1
Dollar --> Euro rate @ 1,23	#	USD	Euro	USD	Euro
1. activities					
1.1 grantmaking					
1.1.1 Emergency Grants					
[redacted]					
[redacted]					
[redacted]					
1.1.2 Direct Support Grants					
1.1.2.1 Tactical Tech Collective					
1.1.2.2 Internews Europe	1		7.212,22	8.871,03	7.212,22
1.1.2.3 Virtual Road small grant	1		29.497,00	36.281,31	29.497,00
[redacted]					
[redacted]					
1.1.3 Strategische Partners grants					
1.1.3.1 Strategic Partnerships 100.000					
1.1.1.2.1 MLDI					
1.1.1.2.2 Torservers					
1.1.1.2.3 Frontline Defenders					
[redacted]					
1.1.1.2.5 Virtual Road	1		60.000,00	73.800,00	60.000,00
1.1.1.2.6 Leap/Riseup	1	100.000,00		100.000,00	81.300,81
1.1.3.2 Strategic Partnerships 250.000 >					
1.1 Subtotal grantmaking				255.105,39	207.402,76
1.2 Linking and learning					
1.2.1 peer-to-peer					
1.2.1 Subtotal Peer-to-Peer				0,00	0,00
1.2.2 learning on emergency response					
1.2.2 Rapid Response Coordination					
1.2.1.1.a Travel	1		759,00	933,57	759,00
1.2.1.1 b Accomodation					
1.2.1.1 c other	1		10,15	12,48	10,15
1.2.2 Subtotal learning on emergency support				946,05	769,15
1.2.3 scouting mission					
1.2.3.1 Scouting mission MENA	1	2.119,50		2.119,50	1.723,17
1.2.3.2 Scouting mission Central Asia					
1.2.3.3 Translation scouting mission CA	1	714,48		714,48	580,88
1.2.3 Subtotal Scouting mission				2.833,98	2.304,05
1.2.4 scenario emergency response					
1.2.4.1 mapping threats					
1.2.4 Subtotal Scenarion emergency response				0,00	0,00
1.3 evaluation					
1.3.1 external review					
1.3.2 audited statement					
1.3 Evaluation				0,00	0,00
Sub total activities				258.885,43	210.475,96
2. Direct management costs					
2.1 personal					
2.1.1 Programme Manager (100%)	3		10.293,09	37.981,50	30.879,27
2.1.2 Programme Officer (88,8%)					
2.1.3 Technical Expert (88%)					
2.1.4 Junior Programme Officer (88.8 %)	2		6.112,12	15.035,81	12.224,23
2.1.5 Adm/finance (50%)	1		1.210,01	1.488,31	1.210,01
2.1.6 Temporary Communications person	1		3.269,87	4.021,94	3.269,87

Sub total Direct Management Costs				**58.527,56**	**47.583,38**
3. Office					
3.1 Office set up-supply					
3.1.1 Computer/laptop					
Sub total office				**0,00**	**0,00**
4 Other costs, services					
4.1 communication					
4.1.1 Identity					
4.1.2 Website	1		2.049,74	**2.521,18**	**2.049,74**
4.1.3 Printing costs	1		393,25	**483,70**	**393,25**
4.1 Subtotal Communication				**3.004,88**	**2.442,99**
4.2 Travel					
4.2.1 International airfare					
4.2.1.A Boston	1		1.164,18	**1.431,94**	**1.164,18**
4.2.1.B San Fransisco	1		1.457,17	**1.792,32**	**1.457,17**
4.2.1. C Toronto	1		930,73	**1.144,80**	**930,73**
4.2.1.D Geneva	1		168,14	**206,81**	**168,14**
4.2.1 Subtotal International Airfare				**4.575,87**	**3.720,22**
4.2.2 In-country travel overseas					
4.2.2.A Boston	1		138,34	**170,16**	**138,34**
4.2.2.B San Fransisco	1		60,65	**74,60**	**60,65**
4.2.2 Subtotal in-country travel				**244,76**	**198,99**
4.2.3 Per diem (6 travels*7days*185perdiem)					
4.2.3.A Boston	1		676,58	**832,19**	**676,58**
4.2.3.B San Fransisco	1		786,87	**967,85**	**786,87**
4.2.3.C Toronto	1		665,56	**818,64**	**665,56**
4.2.3 Subtotal Per Diem				**2.618,68**	**2.129,01**
4.3 Annual meeting					
4.3.1 Teleconference meeting IC	1		127,53	**156,86**	**127,53**
Subtotal Annual Meeting IC				**156,86**	**127,53**
4.4 Other					
	1		188,96	**232,42**	**188,96**
Subtotal Annual Meeting IC				**232,42**	**188,96**
Sub-total other cost, services				**10.833,47**	**8.807,70**
Total				**328.246,46**	**266.867,04**

Annex 6 Budget versus expenditure USD 2014

Total budget vs expenses 2013 Dollar --> Euro rate @ 1,23	Cummalitive cost Total DDP 12/13 USD	Total Budget USD 2014	Q1 2014 USD	Q2 2014 USD	Q3 2014 USD	Q4 2014 USD	Cummalitive cost 2014 USD	Cummalitive cost Total DDP USD	Total Commitments 2014 USD	Total Commitments 2015 USD	Remaining Budget 2014 USD
1. activities											
1.1 grantmaking											
1.1.1 Emergency Grants		75.000,00	11.153,05				11.153,05	**11.153,05**	3.240,00		60.606,95
1.1.2 Direct Support Grants	82.410,00	550.000,00	70.152,34				70.152,34	**152.562,34**	22.702,00		457.145,66
1.1.3 Strategic Parnternship grants											
1.1.3.1 Strategic Partnerships 100.000	342.524,25	717.728,00	173.800,00				173.800,00	**516.324,25**	493.957,00	148.989,28	49.971,00
1.1.3.2 Strategic Partnerships 250.000 >		750.000,00					0,00	**0,00**	0,00	0,00	750.000,00
1.2 Linking and learning											
1.2.1 peer-to-peer	20.566 83	55.999 00					0 00	**20.566,83**	0 00		55.999 00
1.2.2 learning on emergency response	10.476,37	39.992,00	946,05				946,05	**11.422,42**	262,58		38.783,37
1.2.3 scouting mission	10.792,50	5.000,00	2.833,98				2.833,98	**13.626,48**	6.666,52		-4.500,50
1.2.4 scenario emergency response	219,37	10.000,00					0,00	**219,37**	0,00		10.000,00
1.3 evaluation											
1.3.1 external review	0,00	10.000,00					0,00	**0,00**	0,00		10.000,00
1.3.2 audited report		10.000,00					0,00	**0,00**			10.000,00
Sub total activities	**466.989,32**	**2.223.719,00**	**258.885,43**				258.885,43	725.874,74	**526.828,10**	**148.989,28**	**1.438.005,47**
2. Direct management costs											
2.1 personal											
2.1.1 Programme Manager (100%)	158.758,29	143.245,80	37.981,50				37.981,50	**196.739,79**			105.264,30
2.1.2 Programme Officer (88 8%)		90.740,79					0,00	**0,00**			90.740,79
2.1.3 Technical Expert (88%)		82.685,52					0,00	**0,00**			82.685,52
2.1.4 Junior Programme Officer (88.8 %)	74.892,18	94.168,80	15.035,81				15.035,81	**89.927,98**			79.132,99
2.1.5 Adm/finance (50%)	6.015,47	45.682,20	1.488,31				1.488,31	**7.503,77**			44.193,89
2.1.6 Temporary Communications person		6.033,15	4.021,94				4.021,94	**4.021,94**			2.011,21
Sub total Direct Management Costs	**239.665,93**	**462.556,26**	**58.527,56**				58.527,56	**298.193,49**	**0,00**	**0,00**	**404.028,70**
3. Office											
3.1 Office set up-supply											
3.1.1 Computer/laptop	831,96	1.100,00					0,00	**831,96**	0,00		1.100,00
Sub total office	**831,96**	**1.100,00**	**0,00**				0,00	**831,96**	**0,00**	**0,00**	**1.100,00**
4 Other costs, services											
4.1 communication											
4.1.1 Identity	11.132,48	3.000,00	0,00				0,00	**11.132,48**			3.000,00
4.1.2 Website	2.829,26	1.500,00	2.521,18				2.521,18	**5.350,44**			-1.021,18
4.1.3 Printing costs	43,05	3.000,00	483,70				483,70	**526,75**			2.516,30
4.2 Travel											
4.2.1 International airfare	6.515,22	13.500,00	4.575,87				4.575,87	**11.091,09**			8.924,13
4.2.2 In-country travel overseas	762,79	6.000,00	244,76				244,76	**1.007,54**			5.755,24
4.2.3 Per diem (6 travels*7days*185perdiem)	6.739,30	12.950,00	2.618,68				2.618,68	**9.357,98**			10.331,32
4.3 Annual meeting											
4.3.1 Annual meeting Investment Committee	3.636,77	7.380,00	156,86				156,86	**3.793,63**			7.223,14
4.4 Other											
	172,06	200,00	232,42				232,42	**404,49**			-32,42
Sub-total other cost, services	**31.830,93**	**47.330,00**	**10.833,47**				10.833,47	**42.664,40**			**36.696,53**
Total	**739.318,14**	**2.734.705,26**	**328.246,46**				**328.246,46**	**1.067.564,59**	**526.828,10**	**148.989,28**	**1.879.830,70**

Annex 7 Budget versus expenditure Euro 2014

Total budget vs expenses 2013 Dollar --> Euro rate @ 1,23	Total Budget Euro 2014	Cummalitive cost Total DDP Euro	Q1 2014 USD	Q2 2014 USD	Q3 2014 USD	Q4 2014 USD	Cummalitive cost 2014 USD	Cummalitive cost Total DDP USD	Total Committed 2013 2014 Euro	Total Commitments 2015 Euro	Remaining Budget 2014 Euro
1. activities											
1.1 grantmaking											
1.1.1 Emergency Grants	60.975,61		9.067,52				9.067,52	**9.067,52**	2.634,15		49.273,94
1.1.2 Direct Support Grants	447.154,47	67.000,00	57.034,42				57.034,42	**124.034,42**	18.456,91		371.663,14
1.1.3 Strategic Parnternship grants											
1.1.3.1 Strategic Partnerships 100.000	583.519,25	278.475,00	141.300,81				141.300,81	**419.775,81**	401.591,06	121.129,50	40.627,38
1.1.3.2 Strategic Partnerships 250.000 >	609.756,10	0,00					0,00	**0,00**	0,00	0,00	609.756,10
1.2 Linking and learning											
1.2.1 peer-to-peer	45.527,64	16.721,00					0,00	**16.721,00**	0,00	0,00	45.527,64
1.2.2 learning on emergency response	32.513,82	8.517,37	769,15				769,15	**9.286,52**	213,48	0,00	31.531,19
1.2.3 scouting mission	4.065,04	8.774,39	2.304,05				2.304,05	**11.078,44**	5.419,93	0,00	-3.658,94
1.2.4 scenario emergency response	8.130,08	178,35					0,00	**178,35**	0,00	0,00	8.130,08
1.3 evaluation											
1.3.1 external review	8.130,08						0,00	**0,00**		0,00	8.130,08
1.3.2 audited report	8.130,08						0,00	**0,00**			8.130,08
Sub total activities	**1.807.902,18**	**379.666,11**	**210.475,96**				**210.475,96**	590.142,07	**428.315,53**	**121.129,50**	**1.169.110,69**
2. Direct management costs											
2.1 personal											
2.1.1 Programme Manager (100%)	116.460,00	129.071,78	30.879,27				30.879,27	**159.951,05**		0,00	85.580,73
2.1.2 Programme Officer (88 8%)	73.773,00	0,00	0,00				0,00	**0,00**		0,00	73.773,00
2.1.3 Technical Expert (88%)	67.224,00	0,00	0,00				0,00	**0,00**		0,00	67.224,00
2.1.4 Junior Programme Officer (88.8 %)	76.560,00	60.887,95	12.224,23				12.224,23	**73.112,18**			64.335,77
2.1.5 Adm/finance (50%)	37.140,00	4.890,62	1.210,01				1.210,01	**6.100,63**			35.929,99
2.1.6 Temporary Communications person	4.905,00	0,00	3.269,87				3.269,87	**3.269,87**			1.635,13
Sub total Direct Management Costs	**376.062,00**	**194.850,35**	**47.583,38**				**47.583,38**	**242.433,73**	**0,00**	**0,00**	**328.478,62**
3. Office											
3.1 Office set up-supply											
3.1.1 Computer/laptop	894,31	676,39					0,00	676,39	0,00	0,00	894,31
Sub total office	**894,31**	**676,39**	**0,00**				**0,00**	**676,39**	**0,00**	**0,00**	**894,31**
4 Other costs, services											
4.1 communication											
4.1.1 Identity	2.439,02	9.050,80	0,00				0,00	**9.050,80**	0,00		2.439,02
4.1.2 Website	1.219,51	2.300,21	2.049,74				2.049,74	**4.349,95**	0,00		-830,23
4.1.3 Printing costs	2.439,02	35,00	393,25				393,25	**428,25**	0,00		2.045,77
4.2 Travel											
4.2.1 International airfare	10.975,61	5.296,93	3.720,22				3.720,22	**9.017,15**	0,00		7.255,39
4.2.2 In-country travel overseas	4.878,05	620,15	198,99				198,99	**819,14**	0,00		4.679,06
4.2.3 Per diem (6 travels*7days*185perdiem)	10.528,46	5.479,10	2.129,01				2.129,01	**7.608,11**	0,00		8.399,45
4.3 Annual meeting											
4.3.1 Annual meeting Investment Committee	6.000,00	2.956,72	127,53				127,53	**3.084,25**	0,00		5.872,47
4.4 Other											
	162,60	139,89	188,96				188,96	**328,85**	0,00		-26,36
Sub-total other cost, services	**38.479,67**	**25.878,80**	**8.807,70**				**8.807,70**	**34.686,50**	**0,00**	**0,00**	**29.834,58**
Total	**2.223.338,16**	**601.071,65**	**266.867,04**				**266.867,04**	**867.938,69**	**428.315,53**	**121.129,50**	**1.528.318,20**