



CISSU

CARE-International
Safety and Security Unit

A review

By

W. Kok



June 2011

Table of Content

Executive summary.....	pg. 5
Recommendations.....	pg. 7
Introduction	pg. 10
1. Standard for and history of NGO Security Management.....	pg. 11
2. History, Mandate and Place of CISSU.....	pg. 13
2.1 Remarks from respondents on the mandate of CISSU	
2.2 Observations on the mandate of CISSU by reviewer	
2.3 Place of CISSU within CARE-International	
3. Output of CISSU.....	pg.17
4. CI bodies related to CISSU.....	pg.20
4.1. Human Resources Safety & Security Committee (HRSSC)	
4.2. Safety & Security Management Working Group (SSMWG)	
4.3. CI's Emergency Group (CEG)	
5. Financial considerations.....	pg.22
6. CISSU role during critical incidents.....	pg.23
7. Appeal mechanism	pg.24
8. Future of CARE-International	pg.25
8.1 CI-Internal considerations	
8.2 CI-External considerations	
9. Overall conclusions of the reviewer.....	pg.27
Annex: List of interviewees.....	pg. 28

Notes

Executive Summary

CARE-International's (CI) Safety and Security Unit (CISSU) made a significant contribution to the development of a standard and coherent approach towards safety and security of CI worldwide through the development of the Safety and Security Management Protocol, the CI Travel Guide and other security related instruments. The need for further policy – and guidance material to be developed as well as the recognition that a *strategic, confederation-broad* approach towards safety and security will only become more important because of internal and external challenges, indicates the need for a continuation of the unit.

The CI safety and security framework as developed over the past years by CISSU can surely withstand critical comparison with the policies and practices that are considered standard within the humanitarian - and development sector worldwide. This statement does not include an opinion on the state of *implementation* of the framework, as this aspect is beyond the scope of the review.

The internal dynamic of CI has its own dimensions and within the confederation, different appreciations of the functioning of CISSU are inevitable. Especially the existing asymmetry (financial, operational, legal) between the different members causes these different appreciations. This is most notably the case between CISSU and the security unit of CARE-USA (CSU). This reality must for the time being be recognised and accepted and should not blur personal relations. The positive effects of an increased level of security cooperation between CI members, enhanced through CISSU, outweighs however the at times difficult relationship that result from this asymmetry.

These different appreciations of CISSU's functioning circle mainly around the interpretation of the role of CISSU when it comes to either monitoring and/or auditing of security practices of CO's. The existing mandate provides not enough clarity on this point. In the report some suggestions for a possible approach are made.

Stakeholders throughout CI recognise and respect the need for CI members to subscribe and adhere to a common, coherent and recognizable approach towards safety and security by all members of the confederation. It is furthermore realised by a vast majority within the confederation that the future plans suggesting that CI will evolve into an interdependent network organisation only increases the need for such a central safety and security approach (and function) within CI.

The creation of a platform to discuss safety and security within CI through the *Safety and Security Management Working Group* (SSMWG) has proven an important instrument to assure attention for the subject throughout the confederation. CISSU (and the SSMWG) should build on this success.

➤ However, CISSU did not yet manage to create that one, *integrated CI-wide safety and security function* that was envisaged at the onset of the unit. The existing reality of multiple CARE entities each bearing the full legal and moral responsibility for staff in the field has prevented this to happen. In order to minimise the negative effect of this shortcoming, it is recommended that CI re-defines the status of the unit by minor

adjustment of its mandate in line with the recommendations below.

➤ If the establishment of CISSU had as an (sub) objective to prepare the confederation better for the occurrence of major critical incidents, the conclusion can only be that it failed to do so. The management of critical incidents is still based, and dependant, on the individual capacities of the Lead Members(s) to provide this response, not on CISSU.

➤ The present financial construction that supports CISSU re-enforces an existing imbalance between the members within CI. This does not help CISSU to take the central position that the unit is supposed to have on behalf of all members of the confederation. It is recommended to change the basis for the financial contribution to the unit from "number of staff in the field" to system in which all members contribute to CISSU. The existing contribution key as used to determine each member's annual contribution to the International Secretariat is a more logical reference to base the contribution to CISSU on.

➤ Only in the situation that the CARE confederation was a single legal entity would it prove possible to create one decisional Safety and Security function within CI. Given the apparent aspiration that CI evolve towards an interdependent network, this is unlikely to be achieved.

Till such a moment, the different CARE members retain an individual legal (and moral) responsibility for safety and security of their staff. Within that legal and moral reality, a central unit as CISSU will only be able to function if it is based on a robust but modest mandate of an advisory nature.

Recommendations

I. On mandate

Although the mandate as it stands is still relevant, it may be helpful to make adjustments. These adjustments serve to reduce the misinterpretations. Such an adjusted mandate should reflect the position that CISSU will have the coming years within the confederation: act as a knowledge- and resource centre with no hierarchical authority over any of the Country Offices (CO's) but with a strengthened strategic oversight role and position as described in the original mandate.

The mandate must furthermore become more realistic by a reduction of the number of tasks. An example of a possible adjusted mandate is herewith provided:

Possible revised mandate for CISSU-II

CISSU is responsible for further development *and introduction* of the agreed CI's policies and strategies for safety and security in all CO's through close cooperation with (the safety and security units/functions of) the present five CI lead members (LM's; C-USA, C-Canada, C-Australia, C-Deutschland, C-France).

CISSU is responsible for early identification of safety and security issues of strategic significance to CI. Such issues can be divided in:

Internal developments as those that will present itself via the future functioning of the confederation. Emerging issues as security practices of partners and newly emerging CI entities need to be anticipated by CISSU.

External developments as those that will present itself via global developments that has a bearing on CI's functioning as global relief and development organisation. An example is the position within and cooperation with the different humanitarian frameworks that emerged after 9/11.

An important instrument for CISSU to achieve the tasks above is through an active chairing of the Safety and Security Management Working Group (SSMWG). This body will meet at a very minimum twice/year in order to set the CI safety and security agenda, allocate tasks on implementation amongst its members and keep a general oversight over safety and security related matters.

Tasks of CISSU-II

1. Inform and advise CI Secretary General (SG), and through the SG CI's governance, on all matters pertaining to safety and security.
2. Stay current on developments in security practice and thinking within the sector, and also in respect of security crises in areas where CI is operational.
3. Develop and maintain CI Safety and Security policies and general guidance material. The need for further material to be developed will be defined within the SSMWG. CISSU will assure this material to be available for all members and CO's including via an on-line data base system.

4. CISSU will play a pivotal role in times of critical incidents crises within CI. The concrete nature of this role is to be further defined by the CISSU Director, in close cooperation with the members of the SSMWG. Inevitably, it will respect the autonomy of the lead members in the handling of critical incidents.
5. CISSU, in close cooperation with the SSMWG, maintains a monitoring and auditing role there where it concerns the implementation of safety and security related CI policies and procedures on CO level. To this end, CISSU will develop an auditing tool that allows an objective and measurable opinion to be formed on the status of the safety and security management within a given CO, based on the agreed safety and security standards.
6. CISSU, exclusively through the CISSU Director, has the mandate to activate the appeal mechanism when required.

This renewed mandate implies a certain number of tasks NO LONGER to be performed:

- CISSU will not issue or distribute travel advices; this task is better done by the LM's.
- CISSU will not perform (country/area) risk assessments, this task is better done by the regional Security Advisors or external consultants (CISSU may facilitate these assessments to take place by advising CO's and LM's on request on how's and who's).

Some Food for Thought on a "monitoring" versus "auditing" role of CISSU:

A possible approach towards a solution for the question of monitoring and/or auditing may be the acceptance by the SSMWG of the statement that indeed an auditing function on the status of security management within a CO is a requirement.

If the SSMWG agrees to this statement, a second step is to agree as to who is best positioned to take such an auditing role (accepting that a line manager should never audit a CO for which he/she is responsible). This may lead to the conclusion that CISSU is a logical actor to perform this role, but other solutions remain possible.

II. On output

With the security framework as developed, CISSU has contributed significantly to building a proper foundation for a robust safety and security management system throughout the confederation. The next priority (for all staff working on safety and security within LM's and CISSU) must be on the implementation of this system, and their related procedure in the respective CO's worldwide.

A need identified is the need for further *guidance* material. More emphasis must be given to issues of *safety* (car fleet management, staff issues, site selection etc) in addition to *security* issues.

A second important need is the need for a standard *auditing* tool. This CI specific tool should have the CI safety and security standards (MSSS) as a basis. It is recommended to give this tool the form of a "facilitated self-assessment". The background to this recommendation is that the form of a *facilitated self-assessment* might be more acceptable to those that oppose CISSU to take any type of audit role.

A third priority must be the creation of an on-line data base where all safety and security related material, policies, guidance material and resource material, is made easily accessible for Country Offices and CARE-members, both LM and Non LM's. The existing www.careemergencytoolkit.org may serve as an example.

CISSU should take a lead role in defining the respective *training needs* for safety and security for the different stakeholders groups within CI. Which safety and security skills should a CD be trained in, which skills should team members possess, what is needed for new staff, local staff member etc. Such a defined set of skills, in line with the existing security roles and responsibilities as allocated to each staff member will greatly help in developing a common safety and security culture within the CO's. CISSU itself should not be responsible for performing these trainings.

CISSU, in close cooperation with the members of the SSMWG, should write a discussion paper on its foreseen role during critical incidents. This document should define which situations would constitute an *institutional* critical incident for CI as well as the expected roles of the different partners within the confederation during such a critical incident. In a second step, CISSU should define minimum standards to be applied to the response of a LM towards such an incident. The objective must be to harmonise and standardise the responses of the respective LM's towards critical incidents where possible, allowing differences caused by the different legal realities.

III. On structure

A direct link with, and resorting under the International Secretariat, being supervised by the Secretary General, remains to be most logical position within the CI organogram¹ for the unit.

The connection with the board (and with the LM's) need to be strengthened by inserting more operational knowledge and insight in the Human Resources Safety and Security Committee (HRSSC). This can be achieved by inviting a representative of one of the LM's, preferably CARE-US, to take seat in the HRSSC. It must be observed that this will reflect the situation as described in the original May 2006 proposal.

IV. On Finances

The present financial support system for CISSU should be reconsidered. It is proposed to shift to the logic that all CI members benefit from the existence of the unit, and that therefore all CI-members contribute (in proportion). The same contribution key that determines the annual contribution to the International Secretariat can be copied, although other contribution keys can be considered.

Simultaneously, an investigation into the feasibility of *external* funding for CISSU should be made.

¹ Available via International Secretariat

Introduction

The Human Resources Safety and Security Committee (HRSSC) of CARE-International's (CI) board commissioned a review of CI's Safety and Security Unit (CISSU).

An external reviewer was invited to execute this task during April and May 2011.

The results of the review are intended to provide information to the CI board for further decision taking on the future mandate, composition and expected output of the unit.

For details, see the Terms of Reference² as drawn up on April 7th 2011.

The reviewer (Mr. Wouter Kok) started his activities in early April with a visit to the International Secretariat of CI in Geneva.

He was supplied with a number of essential background documents. In close cooperation with the secretariat, he selected a number of CARE staff that formed a representative cross section of stakeholders in safety and security within the organisation.

Amongst the interviewees, representatives of the following CARE entities are represented

International Secretariat
Safety and Security Working Group
CI National Directors
HR Safety and Security Committee
CARE members Safety and Security Focal Points
Country Directors
Regional Emergency Coordinators

To complement the information, an external observer was invited to share his impressions about CISSU with the reviewer.

Each of these persons is asked for two contributions:

1. To fill out a questionnaire on CISSU mandate, place and output in the past years
2. To be available for an interview with the reviewer on the answers as provided in the questionnaire.

For an example of the questionnaire, see footnote ² at bottom of page.

Interviews were held throughout April and May 2011,
Please find a complete list of the interviewees in annex to this report on page 28.

The findings of the review are compiled in this final report in which the valuable comments on a draft version by a selection of involved CI staff are incorporated.

The reviewer wants to express his appreciation for the excellent support and facilitation

² For reasons of readability the TOR and the (example) questionnaire are not part of the report. Both documents are available upon request via vdmolten@careinternational.org

he received during this exercise from Hilde van der Molen, Safety and Security Desk Officer for CI in Geneva.

1. Standard³ for - and history of security management within NGO's

CI is an important player in the global network of Non Governmental Organisations (NGO's) and other humanitarian actors that operate in the sector of relief and development worldwide. It is therefore relevant for CI to realise that it does not operate in a vacuum.

It is for this reason that before touching on the contribution of CISSU to the overall effort to augment safety and security management systems within CI, it is helpful to consider both the history of "safety and security" as well as the standards that exist within the humanitarian sector for the institutional management of safety and security.

It was the dramatic increase in sheer number as well as intensity of security incidents worldwide in the nineties of last century as well as the first decade of this century that forced all humanitarian and relief NGO's to devote substantially more time and resources to this subject than they did in the decades before.

Some statistics⁴ serve to illustrate this trend.

The number of "aid workers" involved in humanitarian relief operations more than doubled in the period 1997 - 2008 from some 136.000 to around 290.000 individuals worldwide. Inevitably also the number of victims went up. Not only in absolute numbers, but also in relative numbers. In 1997, an NGO worker would run a risk of 4/10.000/year to become a victim of a violent incident. In 2008, the chance of such a mishap occurring to him/her had risen to 9/10.000/year.

Global causes, all beyond the control of individual organisations, have contributed to this trend. Some of these causes are: not only did the number of staff go up, also crime and banditry worldwide increased. Monopolisation of aid by military forces of all sides became an issue, as did the visibility of these monopolies due to the technical advances allowing a worldwide audience to witness these changes.

In some of the more insecure settings as Iraq, Afghanistan, Somalia and other parts of Africa the status can only be described as anarchic for -often- prolonged periods of time during these two decades.

At the same time a loss of the perception that aid and relief agencies are neutral, impartial and non-political occurred. The operational choices of aid/relief organisations, sometimes siding with military forces in order to reach populations in need, further contributed to the erosion of a neutral image of organisations. At the same time do the perceptions of organisations as "wealthy" and at the same time "soft" targets further aggravate the situation. No longer are they untouchable simply because they are assumed to be doing "good".

And as said before, all these developments are beyond control of an individual NGO. The only response this individual NGO can offer their staff are internal adjustments to their own security related rules and regulations.

It is important to realise that no formal standard describing how an (I)NGO should shape its safety and security management systems exists. This is because no international authoritative body, be it under UN or other flag, has formal authority to enforce such a standard. The only legislation that an (I)NGO has to abide by is the legislation that is prescribed by the (labour) law of the country under which jurisdiction it is registered. In the situation of CI, this implies that a total of minimally twelve country specific laws are applicable (in addition to the relevant labour law of the respective

³ The summary of a standard for a NGO security framework is here provided as general background information for a CI audience. It may also allow the reader to make his/her own comparison with the state of CI's security framework.

⁴ From: HPG policy brief 34, April 2009

host countries!), but not one of them has an overriding jurisdiction over all CI-bodies. Each CARE-member is accountable via the (labour) law of his own country of residence.

The bottom-line of all these respective labour laws is that an organisation does have a formal responsibility as an employer towards the safety and security of its staff. The organisation must be able to demonstrate its ability to live up to this responsibility. In this way, it is able to show that it is worthy of the trust of staff and (institutional as well as private) donors.

However, there is more to it than "just" the formal responsibility. A practice has grown overtime, and an informal set of minimal standards has evolved. Much of this practice is based on the ideas as laid down in the handbook titled "Operational Security Management in Violent Environments" by Koenraad van Brabant. This handbook⁵, first published in June 2000, offers an outline of a standard for a security management system as described below.

An organisation will institutionalise its security related responsibilities by adopting a formal "Security Policy". Such basic document will outline the security principals on which the organisation builds its (security) practices. Next to this basic document, a set of "Security Instruments" will be developed. These instruments together form a "toolkit" that staff has at its disposal to implement activities in an optimal safe manner. Such a toolkit will entail a wide variety of documents (=instruments). It will range from important protocols as Briefing- and Training Protocols (so as to assure the staff to be able to exercise "informed consent", i.e. to accept a degree of risk after having been made aware of the extent of the risk) to "light" guidance material on e.g. site selection.

The volume of the "toolkit" will vary enormously from one organisation to the other. It will even vary within an organisation, surely if the organisation is multi-mandated and works in a variety of different contexts (as CI does).

An additional level will be introduced by making it mandatory for field offices to develop a context specific Field Security Plan. Such security plans will vary tremendously in intensity and volume from one setting to another. Think of the difference in risks that exist between working in a war zone as to working in a relatively safe and peaceful environment where e.g. poverty reduction is the main *raison d'être*.

Apart from the three levels mentioned above, some more elements can be identified:

- Institutional capacity to manage serious incidents, both locally and on corporate level.
- Institutional capacity to register, document and analyse safety and security incidents.

The total set of safety and security related documents, procedures and guidance material that exist within an organisation is usually referred to as the organisational Security Framework.

In summary

Any responsible organisation working globally in the fields of emergency aid, relief and/or development will have developed a security framework with (minimum) the following elements:

➤ **Security policy**

Outlines the fundamental views of the organisation of security. It allocates responsibilities, and describes expectations and obligations, both for HQ- as well as for field staff. A *code of conduct* will be part of this policy.

➤ **Security protocols and standard procedures**

This set of documents introduces standard procedures to be followed by all staff of the organisation. This will include obligatory rules and procedures as well as guidance material. The total set can be regarded as a Tool kit.

➤ **Mandatory Field Security Plan**

Following a standard, recognisable format, the security plan will describe the locally applicable rules and regulations that all staff in this country/project is subject to. Developed under responsibility of the Country Office.

⁵ For this report, the new edition number 8, December 2010 is consulted

- Organisational and institutionalised capacity to manage one or multiple crises and to analyse and learn from safety and security incidents.

2. History, Mandate and Place of CISSU

The trends and developments observed above have had their impact on CI as well. As a confederation of (at the time of installation of CISSU twelve) independent members, amongst which several (initially three) with operational responsibilities for a great number of Country and Regional Offices also CI had its period of operational growth and its increasing share of incidents.

The individual CI (lead) members had undoubtedly taken up their responsibility in order to minimise risks by the establishment of functions to deal with "security". See the CSU within CARE-USA and comparable capacities within CARE-Australia and CARE-Canada.

In May 2006, a joint meeting of the National Directors and the CI Board agreed that steps should be taken to strengthen the capacity within CI to support staff Safety and Security, and to ensure that related policies and practices were consistently applied across the confederation.

The CI Safety and Security Unit (CISSU) was established as a result of a decision of the CI-board.

A short document called "Proposal for a CARE-International Safety and Security Unit (CISSU)" formalises its establishment in May 2006.⁶

The mandate is captured under the heading of "CISSU responsibilities", and details eight tasks:

1. *Advise the CI Secretary General on all matters pertaining to safety and security.*
2. *Stay current on developments in security practice and thinking within the sector, and also in respect of security crises in areas where CI is operational.*
3. *Develop and maintain CI safety and security policy and standards.*
4. *Support and guide CI members in their implementation of safety and security policy, including planning and training.*
5. *Monitor CI member and country office compliance with safety and security policy.*
6. *Directly support members' safety and security operations in the field during periods of crisis. Consistent with the earlier decision of the National Directors and CI Board, when deployed in the field in support of an operational member, CISSU personnel would come under the day-to-day management of that member.*
7. *Keep CI's Secretary General and governance advised of staff safety and security developments.*
8. *Activate an appeal mechanism when required (If a CO was considered as creating insufficient provisions for staff safety and security).*

In fact, CISSU is asked to create a security framework for the CARE confederation that allows the CO's to build a proportionate and robust safety and security practice and at the same time is able to withstand the scrutiny of any legal or other challenge of CI' safety and security practices.

In the reading of the reviewer, CISSU is asked to perform a role of the *internal auditor* to the system as well: See bullet 3, *maintain standards*, bullet 4, *guide members* and bullet 5, *compliance*. The detail of how to perform such auditing task is however not defined in any sort of detail, and interpretation differences over this point have hampered the cooperation between the major parties involved (LM's and CISSU). See below page 12, monitoring versus auditing.

Much of the rest of the institutionalising document interestingly emphasises what CISSU is **NOT** supposed to do or to be. It is explicitly mentioned (on at least four places) within the document that the responsibility of the individual CI members will not and cannot be touched. If it is felt at the time that this aspect deserves such an emphasis, it is reasonable to assume this must have been a point of primary concern in the minds of those that contributed to the formulation of this

⁶ Available upon request (in hard copy only) via vdmolen@careinternational.org

mandate. This also strengthens the impression that the unit is from the onset perceived as an instrument of the non-operational members and the International Secretariat to get a grip on the security management of the LM's.

Eventually, in September 2007, after a period of discussion on its mandate, its place within the confederations organogram and after its two staff members are recruited, the unit formally starts its activities.

2.1. Opinions and remarks from respondents on CISSU's mandate

The respondents are asked in the questionnaire to rank the tasks of CISSU in order of priority, indicating which four are seen as most prominent. This gives an indication as to how this cross section of CI's workforce views the mandate of the unit. This aspect of CISSU's functioning is extensively elaborated upon during the individual interviews.

The inventory of opinions from the respondents reveals that development (and maintenance) of safety and security policies, safety and security standards and safety and security related guidance material is still seen as the top-priority for the unit. Most people are satisfied with the quality of the material that is produced, and several of the documents have found their way into the operations and the daily procedures of the organisation. They are used on a daily basis without people realising that it is CISSU that developed this material. The use of the travel guide and SSIMS are examples of this. Also the safety and security standards, though not yet officially approved do have the function of providing a benchmark that people use to steer the practices on a day-to-day level.

So, CISSU needs to write policies, write guidelines.

A recurrent observation of respondents on regional and CO level is that a need for more practical material is needed. The focus must (no longer) be on policy development but rather on the creation of practical guidance material. The focus can also shift towards safety rather than only on security.

Having made an inventory of the production of CISSU in the past years, the reviewer can only subscribe to this observation. Rightly, the emphasis in the first years has been on the creation of the security framework. In the second phase, the priorities can and must shift gradually towards the needs as they present themselves through the interviews during this review.

Recommendation

CISSU's priorities can shift from policy development towards development of guidance material as site selection, drivers management etc.

The aspect of availability of the material produced is mentioned often. The material that is produced needs to be made available to all. At this moment this aspect is seen as under-developed and weak. What is missing is a central place, an on-line database that all CO's have easy access to. Several efforts have been made to create such a platform (see e.g. Nirvana, Minerva), but none has managed to become the central, CI-broad place that is needed.

Recommendation

The creation of an on-line data base where all safety and security related material, policies, guidance material and resource material, is made easily accessible for Country Offices and CARE-members, both LM and Non LM's must be an explicit task of CISSU-II. The existing www.careemergencytoolkit.org may serve as an example.

Monitoring versus Auditing

Another crucial task is perceived to be the monitoring role; staying current on developments in safety and security thinking and practices within the sector. In other words, the representation role of the unit within the international NGO community. Sharing of the findings throughout the CI network is seen as important in assuring all members to stay informed and up to date.

The real divergence of opinions start to arise at the moment that CISSU starts to have (any perceived pretences of) operational involvement. In practice, at the moment it starts to exercise its audit role. The points 3, 4 and 5 of the mandate "*maintain standards*"(3), "*support CI members and Country Offices in their implementation with safety and security policy*" (4) and "*monitor CI*

members and CO's compliance with safety and security policy" (5) have led in the past years increasingly to tensions as a result of different interpretations as how these tasks are to be exercised by CISSU.

Are the CISSU staff allowed to contact CO's unilaterally in order to monitor the safety and security practices of any given CO or not. Obviously the CISSU would reason that it has to be able to do so, while the LM would just as obvious reason that all communications need to be channelled via the (security section) of that specific LM.

In practice, it has proven impossible for both sides (CISSU and LM's) to arrive at a sort of logical middle ground that allow both sides to perform their tasks in relatively good harmony, with respect for each others positions and roles. The resulting conflicts have at times obstructed an optimal functioning of the unit. It has surely prevented CISSU from exercising its audit function as effectively as it had wanted to do.

Recommendation

An approach can be to ask the SSMWG to subscribe to a general statement that indeed an auditing function on the status/quality of security management within a CO is a requirement.

If the SSMWG agrees on this statement, a second step could be to agree on who is best positioned to perform such an audit (accepting that a line manager should never audit his/her own CO). This process may lead to the conclusion that CISSU is a logical actor to perform this role, but other solutions remain possible.

Regardless of the outcome of this discussion the first step in this process however is the development of a CI auditing tool.

It is therefore recommended that (in close cooperation with the SSMWG) this tool is developed by CISSU. The basis for such an auditing tool can be no other than the Safety and Security Standards as developed (but not yet approved!).

It is recommended to give this tool the form of a "facilitated self-assessment". The background to this recommendation is that the form of a *facilitated self-assessment* might be more acceptable to those that oppose CISSU to take any type of audit role.

Recommendation

CISSU, within the context of the SSMWG, is recommended to develop an auditing tool based on the CI Safety and Security Standards. This tool should have the form of a *facilitated self-assessment*⁷ to be used on the level of the CO's.

A common appreciation is that the present mandate is too broad and too full. Either an adjustment of the mandate or a serious extension of the resources available for the unit is needed. In combination with the ongoing discussion on the role of CISSU (monitoring versus auditing) this leads most people to consider it more logical to limit the activities rather than increasing the resources of the unit.

Recommendation

In order to create more realism on the expectations of the unit, a reduction of the tasks of CISSU is recommended.

2.2. Observations on the mandate of CISSU

Scrutiny of the eight tasks that CISSU is expected to fulfil (see above) and getting a picture on how these tasks have been shaped in the past years, show that in several of them, inevitably, CISSU is to exercise (at least partly) a type of an operational line management role. If the Unit indeed is to "*support members safety and security operations in the field during periods of crisis*" (task # 6), a form of authority to do so is required. Also "*activating an appeal mechanism when required*" (task

⁷ Advice should be looked for at CEG, who uses this tool to audit the level of emergency preparedness of a CO

8) implicitly leads to exercising authority. Both functions, if properly exercised have characteristics of a line function.

But also some of the other functions pre-suppose an authority that only comes with an auditing role. How else can CISSU shape its tasks to "*Monitoring CI members and CO's compliance*" or to "*support implementation of security and safety policies*" (see task # 4 and 5).

As signalled above, the different interpretations of HOW these tasks are to be exercised have resulted in an increasingly blurred relation between CISSU and most notable CARE-US.

All this to say that at moment of its establishment, CISSU is constructed with some built-in weaknesses. These built-in weaknesses may not have been prominent in the beginning but they have surfaced over time, and they need to be dealt with.

This, in combination with some other factors as distance, financial- and general institutional asymmetry, cultural differences and different levels of involvement in operations caused CISSU to become less productive than one would have liked it to be.

Recommendation

It is for the combination of reasons described above that the reviewer recommends the mandate of the unit to be adjusted. An example of such adjusted *Terms of Reference* is given in under "Recommendations".

It is important to observe however that at the same time nobody questions the need for the shared, the common CI safety and security approach. The need for an independent audit function within CI in order to ensure this common approach to be complied with is understood. It is on the level of *how* this is done that tensions have emerged.

2.3 Place of CISSU within CARE-International

An explicit choice is made to bring the unit under the direct supervision of the Secretary General⁸.

Periodic reports to a *security oversight committee*⁹ must assure the board to be well informed on issues of safety and security. The proposal mentions the oversight committee to consist (next to the CI Chair and the SG) of two CI board members from the three main operational members of CI selected on rotation basis.

It is important to notice that the committee as foreseen in the proposal has never been formed. In practice, the unit reports via the existing HR Safety and Security Committee (HRSSC).

Seemingly a detail, in reality this situation caused the three most prominent Lead members (US, Canada and Australia) not to be included in the oversight committee. The reason why the original plan never materialised is unclear to the reviewer. But this situation will have fed the impression on the side of the LM's that the unit is primarily an instrument for the benefit of the non-operational members of CI. On board level, it may have contributed to a feeling within the LM's that the unit is not "theirs". It may have (contributed) to prevention of a sense of ownership, of connectedness to the unit to be developed by LM's.

During the interviews as well as in the reactions via the questionnaires, no serious challenges to the status quo or alternatives are presented. The only point of discussion is whether the CISSU should report via the ExCom or via the HRSSC. Pro and cons of this are elaborated below under the heading 4.1, HRSSC, page 18 and 8.1, Future of CI, page 24.

For some further information on the functioning of the HRSSC, please see under 4.1 (page 15).

⁸ See for details the organigram of the International Secretariat, available upon request via the secretariat

⁹ Available upon request (in hard copy only) via vdmolen@careinternational.org

3. Output of CISSU in the past years

CISSU has been active on a great many sub-terrains of the broad field of Safety and Security.

In this short overview, it will not be possible to mention all activities, but following compilation highlights the main achievements of CISSU in the review period.

CISSU developed

A. Safety and Security Management Framework applicable to all Country Offices (CO's) regardless of the Lead Member (LM) involved. The framework explains the security approach taken by CARE. A number of supporting documents that guide the CO's in making this framework operational are part and parcel of the framework. It consists of:

- Safety and Security Management Plan (Manual); a handbook that helps the CD and his/her team to compile a locally applicable and relevant Security Plan.
 - Safety and Security Management Protocol (Quick reference Guide). A short version of CARE International's Safety and Security Management Manual. It is intended to be a reference guide.
 - Safety and Security Management Protocol (Template). Is intended as the basis for the development of a recognisable CI country and location-specific Safety and Security Management Protocol. It also provides links to more extensive instructions and examples.
- B. Safety and Security Incidents Monitoring System (SSIMS)

This on-line database allows all CO's to report incidents to a central point.

CISSU developed a relation with "Insecurity Insight", a non-for-profit NGO that supports CARE in the analysis of incident related data since February 2009.

Observation by the reviewer:

The importance of a proper system of incident reporting, analysis and adjustment of safety and security procedures and practises on CO level cannot be over emphasised. The fact that CISSU choose to develop this aspect as a priority shows that it has a well-developed understanding for the priorities for CI. As such, SSIMS must be considered as one of the most important contributions so far of the unit. By the time the system will be utilised till its full potential, it will be an important tool for CO's to analyse the context they find themselves in, and implement a relevant security management system accordingly. Unfortunately, at present too many CO's fail to see the importance of a systematic reporting via SSIMS of all incidents.

In a sense, this is a strong illustration of the difficult position CISSU finds itself in.

CISSU (together with the SSMWG, see below) has further developed and maintained this system, and sees the importance and potential of its use. If it were to be in a line management position in its relation with the CO's it would be able to enforce a more systematic use of SSIMS than at the moment is the practice. However, because CISSU is not in a position to take this role, often even not allowed to take direct contact with the CO's, it becomes impossible to enforce maximum use. The result is that the system is under-used, not living up to the expectations. This in return has a demotivating effect on the CO's, and the system gets even less attention. A vicious circle results.

If CISSU had more leverage towards the CO's (or to the LM's to assure them taking appropriate

action) in order to enforce full compliance, it would optimise the use of the system. This catch-22 situation is here elaborated because it strongly illustrates a fundamental problem with the present set-up of CISSU within CI.

C. A set of general Guides and Tools comprising (a.o.) of:

➤ Policy Framework on Civil-Military relations¹⁰

CARE realised the importance of the humanitarian challenges represented by the integration of humanitarian responses into an overall military and security concept. Inappropriate interaction or even the perception thereof may undermine CARE's acceptance amongst local populations and increase the level of insecurity. It is for this reason that a policy framework is developed that guides the CO's through the difficulties of defining where and when lines are crossed.

➤ Safety and Security Risk Rating System

This security and safety rating system intends to enable CO's to systematically map different risk profiles of its operations. By comparing and ranking risk profiles against a defined set of criteria, it is ensured that the risk profile ranking is carried out in a more or less objective and methodical manner. It allows linking the risk levels to a set of defined mitigation measures.

➤ Sensitive Information Management Protocol

The reviewer could not trace this document. It is nevertheless mentioned as an example of one of the more practical guidance documents that has been worked on by CISSU during the review period.

➤ Minimum Safety and Security Standards (yet to be approved)

As a logical extension of the *CI Safety and Security Principles* as adopted in November 2008 by the CI board, CISSU undertook to define standards that form the benchmark for safety and security behaviour and culture within CI. The standards contribute towards accountability of CARE members for the safety and security of their staff and associated personnel. All CARE members will be asked to conform to these standards and hold themselves accountable to them¹¹.

D. Training aspects

CISSU developed a Standard Training session for Non-lead members on CI's security approach. This one-day introduction to CI's security approach was conducted several times, amongst others to the benefit of CARE-Nederland, CARE-France, CARE-Deutschland/Luxembourg and CARE UK.

This instruction session has a general nature and does not teach security skills to participants.

Also a Crisis Management Training module is under development, a test run of it was performed in cooperation with the Asia Regional Management Unit in Bangkok.

Throughout the years CISSU participated in several Regional/Country Offices Training sessions, as well as in thinking with the LM's on the needs throughout CI on the training needs of the different staff groups within the organisation.

¹⁰ Although this subject has important security aspects, it has the character of general CI policy formulation. As such, cooperation with project staff rather than with security experts during its compilation is assumed.

¹¹ A speedy process of adopting these standards for CI by all members is an urgent pre-condition for further steps to be taken. The development of a CI specific auditing tool is dependent on this step to be made.

It is relevant at this junction to differentiate between training of specific safety and security skills on one hand and providing more general information on concepts and management approaches for safety and security on the other hand. It is argued that CISSU should limit its involvement (as it did so far) to general security training. The teaching of specific safety and security skills is an area for more professional trainers. CISSU should not engage in to this direction (as is suggested by some interviewees)

Recommendation

CISSU should take a lead role in *defining* respective training needs on safety and security for the different stakeholders groups within CO's. (CD's, Security Officers etc). This is part of the effort of CISSU to implement/introduce the common and coherent security management system that CI requires.

Performing these trainings should not be within the mandate and capabilities of the unit.

E. Other activities

A major step was taken in August 2008 with the establishment of the *safety and Security Management Working Group*, comprising of security staff of the Lead members and CISSU staff. In the following years, this Working Group proved vital in agenda setting for CI where and when it concerns safety and security issues relevant for all CARE Lead members.

Throughout its existence CISSU either conducted, or was involved in a number of country/area risk assessments. A (incomplete) listing shows that in following settings the assessments were carried out: Nairobi, Jerusalem, Yemen, West Bank/Gaza, Kenya, Liberia, Sudan and Pakistan.

Via CISSU, CI became member of a number of international security oriented networks as the European Interagency Security Forum (EISF, since March 2008), the UN Interagency Standing Committee Steering Group on Security (February 2009), the International Security Association and other relevant bodies. CISSU contributed to the HPN Good Practice Review 8, a follow-up study on the standard setting study on Operational Security Management in Insecure Environments, first published on 2000.

These memberships, and the opportunities they provided to present the CI achievements in its internal security approach has given CI a high profile and a position of authority within the INGO community.

The fact that the former CISSU Director is perceived as highly credible and respectable because of his experience and background plays an important role in gaining this authority for CI.

According to a spokesperson outside CI, this position allowed CI to contribute significantly in softening UNDSS approach to security in 2009 and equally contributed to influence donors to support security strategies based on acceptance. It may have helped that CISSU hosted a number of sector wide security events. All in all it is fair to say that CISSU has managed to give CI a profile as a constant, reliable and active partner in the field of security in the different networks it engaged with.

Throughout the 3.5 years of functioning, CISSU published a steady flow of in total twenty-seven *newsletters/updates*. This is an average of one newsletter every 6 weeks during the 43 months that the Unit functioned so far (September 2007 – March 2011).

These documents highlighted the sensitive operational areas, identified potential new threats and gave advice on possible risk mitigating measures. Every edition provided an overview of the incidents recorded via CI's Security and Safety Incident Monitoring System.

A last regular product distributed via (not by) CISSU is the *travel advises* that are issued by the respective lead members for the CO's under the responsibility of that LM.

Conclusion/Recommendation

With the security framework as developed, CISSU has contributed significantly to building a proper foundation for a robust safety and security management system throughout the confederation. The next priority (for all staff working on safety and

security within LM's and CISSU) must be on the implementation of this system, and its related procedures in the respective CO's worldwide.

4. CI entities related to CISSU

CISSU does not function within a vacuum.

It is placed within the International Secretariat, and reports directly to the Secretary General.

Its link to the board is guaranteed through the obligation to report to the Board's Human Resources Safety and Security Committee (HRSSC).

Its linkage to the (security sections) of the Lead members is organised via the establishment of a working group (started in August 2008), the Safety and Security Management Working Group (SSMWG).

Within the Secretariat, the CISSU is given a similar status as the CI's Emergency Group, the CEG.

Below, please find some details on the functioning of the HRSSC, SSMWG and CEG.

4.1. Human Resources Safety and Security Committee

It is through the Human Resources Safety and Security Committee (HRSSC) that CISSU is to assure the CI board to remain involved with and informed on the activities and findings of CISSU.

Following a governance reform in 2008, the HRSSC is one of four standing committees of the CI board. The other ones being the Finance, Audit and Risk committee, the Executive Committee and the Governance and Nominations Committee.

The HR SSC is composed of maximum seven members of the board, being the CI Chairperson, CI board members as appointed by the CI chairperson and the CI Secretary General as non-voting member. It meets twice annually in person. Furthermore, it meets via a number of conference calls throughout the year to assure acceptable level of functioning of the committee. Contrary to the ExCom, the HR SSC does not have sub-committees.

Since the governance reform is evaluated as being a successful one, it must be assumed that this structure will remain in place for the foreseeable future. The relation of CISSU with HR SSC is one of accountability. Twice a year, CISSU reports to the HR SSC on its activities and its findings via a written report that allows the committee to take note of the progress of the developments. It also elaborates on the incidents, the causes thereof and resulting actions.

A point raised is the "political weight" that this committee has in comparison with other board committees. Some argue that it might be better to have CISSU report to the executive committee. This is seen as giving the work of the CISSU a greater weight because it would underline the operational linkages and importance that is attached to the subject of security (within a broad field of competing priorities). The expected result would be more "political leverage" within CI.

A contra argument is that the ExCom is felt to be stretched to, and beyond, its limits and would find it difficult to raise the attention required for a highly contentious subject as security is.

Another suggestion, one favoured by the author of this report, is to reconsider the composition of the HRSSC. At present there is no representation of lead members in the committee. This implies that on board level, there is no platform where the often-opposing opinions on the limits of the mandate and authority of CISSU can be discussed between members with full knowledge and insight of all relevant information.

It is for this reason that it is strongly recommended to appoint one senior representative of a Lead Member (preferably CARE-USA) in the HR SSC. This would allow the committee, and thus the board to be better informed on security matters. The practical day-to-day struggle that comes with carrying safety and security responsibilities for field staff can be brought into the equation.

For some further thoughts and observations on the relation between CISSU and the board, see

under 8. Future of CI.

4.2. SSMWG

The Safety and Security Management Working Group is institutionalised in August 2008. This forum has proven itself from the start as an important vehicle for all staff within the CARE confederation that is tasked with safety and security to assure issues of common interest to be discussed and decided.

To quote one of the respondents in an interview:

"Even if CISSU ceased to exist today, we will maintain this working group".

All respondents that are involved in the SSMWG echo this opinion.

The fact that the working group foresees in a gap is illustrated by the increasing intensity of contacts between the members.

In 2008, two conference calls were conducted. This number rose in 2009 to four, and in 2010 to five regular phone meetings. The minutes of these meetings show that the quality of the discussion increases overtime, and that the number as well as the type of subjects increases.

A series of workshops are organised by CISSU in order to create a common agenda as well as a common work plan for implementation. The workshops (2/3 days each) are held annually.

A total of four workshops have taken place in respectively Geneva (2008), Amman (2009), Geneva (2010) and Washington (2010).

A point raised is that the Director of CISSU must take a more outspoken leadership role within this platform. The reviewer very much supports this suggestion. The SSMWG, intended or not, has proven to be the single most positive development for the staff involved in safety and security within CI.

It brought the group together around one table, creating a sense of being a group.

Recommendation

More outspoken than so far, the CISSU Director should assume ownership over the SSMWG. He/she should be the chair, set the agenda, follow-up and oversee the implementation of decisions taken by the SSMWG. An important development as new members taking on operational responsibility (CARE-Fr and CARE- Deutschland) must be anticipated, and membership of these new lead members of the SSMWG must be compulsory. These new lead members are in need of strong guidance by the CISSU, as they do not yet have the experience that is a pre-condition to building an acceptable safety and security culture within an organisation.

4.3 CI's Emergency Group (CEG)

The CEG is a CI-entity that finds itself in a very comparable position as CISSU.

The CEG is to assure CO's to provide an acceptable emergency response if required. This pre-supposes a level of emergency preparedness to be in place within the CO. CEG is to advice on the do's and don'ts of this process without having a line responsibility over a CO.

Both CEG and CISSU have to work via Lead members in their relation with the CO's. Both cannot use the strength of authority, but have to prove the value and importance of "their subject" (emergency and security respectively) through the strength of arguments, goodwill and conviction. Both face therefore a very comparable set of challenges.

It must have been considered in the past to merge the two entities. Also in several conversations,

the possibility of a merger is discussed. In the end however, it is not recommended to do this for several reasons:

- It would diminish the visibility of CISSU as an independent entity making it harder to convince an already sceptical audience of its importance.
- It would enforce an already existing association of CEG with security issues, an image the CEG staff is struggling against already.

5. **Financial considerations**

A decision is taken in 2006 to share the costs of the unit between those members that have field staff based in CO's. The underlying logic at the time is that these are the members that are going to benefit most of all of the work of the unit. The division key is based on the number of personnel employed in their respective country offices of the lead members. See table below for realisation.

	Costs (in €)	CARE-US (in %)	CARE-Can. (in %)	CARE-Aust. (in %)	CARE-UK (in %)	Other (in %)
2007	255.000	70.6 %	19 %	6 %	0.1 %	4.3 % (MERMU)
2008	362.000	75.6 %	16 %	8 %	0.4 %	
2009	364.000	73.8 %	16 %	10 %	0.2 %	0.04 % (CARE-Denmark)
2010	300.000	65.6 %	17.6 %	15.6 %	0.03 %	0.62 % by C-France
2011 (till March 31)	267.000	70.4 %	15%	13 %	0.03 %	0.04 % - C-Denmark 0.37 % - C-Germany 0.64 % - C-France

The cost sharing for CISSU obviously follows the division of (operational, financial, staffing) strength between the partners, with CARE-USA taking the lion share of the costs (just over 70%)

This would be fully acceptable if the benefits of CISSU were also felt by CARE-US as a benefit. Unfortunately, this is not the case, and increasingly the staff of the security unit in Atlanta feels to subsidize other CI members, without getting value for their money. With the financial contribution of CARE-US being in the range of less than 0.1 % of the CARE-US annual budget, the financial argument is obviously not the heart of the matter. The real problem is the perception that CARE-US is subsidizing the rest of the confederation, without getting value for money. This perception is difficult to argue against, as these are feelings, not facts. The people that harbour this perception will at the same time subscribe to the need for a uniform and recognisable safety and security approach of all CARE members. So, although there are here elements of "caricature" thinking in the arguments, undeniable is the fact that an asymmetry exists in the financial support for the unit.

It is therefore recommended to examine alternative support models.

The present base for funding of the unit is the "bodies in the field" logic. Every (lead) member contributes in proportion to the number of staff it has positioned anywhere in, or via a CO in the field.

An alternative suggestion made during the review is to change from this "bodies in the field" logic to "it's a shared CI interest" logic. In such logic, it is only fair that all CI members contribute to CISSU.

Such a new approach would help to increase the sense of ownership of the smaller CI-members over the unit, and diminish the perception of the bigger LM's to contribute disproportionately to the unit. It would bring more equality, more balance in the relation between the different members.

Recommendations on finances

The present logic used to define the financial contribution to CISSU is based on the number of people positioned in "the field". A new formula must be considered. This

formula should have the logic that all CI members benefit from the existence of the unit, and that thus all CI-members contribute. The same contribution key that determines the contribution to the International Secretariat could be introduced.

A longer-term effort can be made simultaneously to identify external parties to CI that may have an interest in sponsoring the unit.

6. **CISSU role during critical incidents**

In order to fully appreciate the sensitivities of this specific aspect of CISSU's mandate, it is inevitable to take an historical perspective. CISSU came into existence following an episode of a serious critical incident.

An internal reflection recognised the importance of a common approach, and shared communications during such a situation, both prior to the event as well as during it. It testifies to the strength of CI that this resulted in an explicit effort to improve the internal dynamics, and create a common mechanism for this purpose. The establishment of CISSU is therefore, apart from all other objectives, also an effort to create more coherence amongst CI during critical incidents.

Two elements of the mandate of CISSU have been introduced to guarantee CISSU to take this role. Both the task number 6: "*direct support to members during periods of crisis*" and task number 8 "*activate an appeal mechanism when required*" must be read as the way to prevent when possible, and react when needed, in a common and coherent manner as confederation to critical incidents.

In the past years, during the existence of CISSU, this function has not properly been tested.

Though positive it may be that no major critical incident has hit the organisation during this timeframe, it also means that there has been no opportunity to properly "field-test" this aspect. Therefore the reviewer looked at the level of preparation as well as to the expectations of different actors within CI.

The interviews give a wide variety of different opinions as to what this "support role" might entail. This varies literally from "no role whatsoever, apart from sending out communications to the periphery of the organisation" to "taking a central role in handling of the incident at hand".

Unsurprisingly, representatives of the lead members have strong opinions as to the foreseen approach of a critical incident. Each lead member, driven by legal as well as moral responsibilities, have their own, individually defined way of preparation. In these preparedness scenarios, no role is allocated to CISSU. In the conversations no indication is received that CISSU is expected or encouraged to take a role other than as a "communication-dispatcher" during an incident.

The further away the respondent is from direct operational support, the higher the expectations as to the role that is allocated to CISSU¹². This coincides with the overall expectations that respondents have from CISSU. Those with operational responsibilities are exclusively oriented to exercise these responsibilities, doing so from the respective LM's view of the world, while more distant (or more central) positioned CI staff takes a different perspective, expecting stronger contribution from CISSU, in general a stronger role from the International Secretariat.

At the moment of writing, no signs can be seen that an effort is made to bridge this expectation gap. This implies a great potential for misunderstanding, frustration and confusing communications if a critical incident would occur.

Adding to this unfortunate situation is that in the documentation reviewed, hardly any reference is found to pro-active, prior thinking on the subject. No policies or document of any status as to what sort of role CISSU itself foresees to take has been seen. No scenario's, no (proposed) policies, no blue prints for lines of actions to be taken in case of a kidnap, mass casualties amongst CI staff or any other scenario.

It is the conclusion of the reviewer that CI *on the level of the International Secretariat* is as ill prepared for the occurrence of a critical incident at this moment as it was in 2004. If the situation is any better on the level of the individual LM's is beyond the scope of this review, and thus not

¹² With notable exceptions; one respondent expects his/her government to take full control over such a situation

considered.

Recommendation

CISSU must play a pivotal role in times of critical incidents within CI. The concrete nature of this role is to be further defined by the CISSU Director, in close cooperation with the SSMWG.

7. The “appeal” mechanism

An important aspect of CISSU’s mandate is the so-called “appeal mechanism”. It is worded in the mandate as CISSU having the right to “*activate an appeal mechanism when required (If a CO was considered as creating insufficient provisions for staff safety and security)*”.

The right to launch such an appeal is obviously a strong and in a way an ultimate instrument that is given to CISSU. Such a strong instrument can only be used in extreme situations, and only so after every other way to influence a situation has been exhausted. It is furthermore important to assure that if the appeal is used, that it happens in a discrete manner, without embarrassing CO’s, LM’s or the individuals involved in these.

In the available documentation no further specification is found as to how such an appeal should be launched, what steps are envisaged to exist within such an appeal, and how it is to be documented.

The only further reference found to how such an appeal is to be used is provided via the following stipulations

- “The CISSU will have recourse to the Secretary General if he believes that CO/lead member actions or decisions are counter to CISSU recommendations and are thus endangering CARE personnel.
- The SG in turn will take action including referring such occurrences to the CI Board.”

It must be noticed that this loose formulation has worked excellent in the past years. And maybe it did so simply because it is only loosely described. The reality is that this appeal mechanism has not been used in any formal (documented) sense, but that its existence and diplomatic use obviously did work.

In the opinion (perception) of different stakeholders within the organisation, the mechanism has been used. People differ of opinion on whether this is a formal use, or just an impression that the mechanism is used. On at least two occasions (Pakistan, Somalia) the then CISSU Director used his influence to get a correction of a situation that he considered to be posing a direct threat to the safety and security of CI staff, and he managed to achieve such a correction without having to use the mechanism, again, not in any formal way.

It is important that the use of this “nuclear option¹³” remains exercised in a diplomatic fashion in order not to exhaust its strength. Such a subtle use also implies that the ability to do so can only be limited to the Director of CISSU.

This leads to a point for further elaboration that presented itself during the review. Some security staff within LM’s is of the opinion that the use of the appeal mechanism is not, and should not be limited to the discretion of the CISSU Director. The statement is basically that everyone who observes a breach of security conditions anywhere should have the appeal mechanism available as a last resort if all other means have failed to yield a positive result.

It is the opinion of the reviewer that such a widespread and repeated use of the appeal mechanism would quickly lead to a “politicisation” of the instrument. This in turn would quickly lead to the instrument becoming obsolete. It is obvious that such a situation must be avoided.

Recommendation

It is recommended that the right to launch the appeal mechanism is (remains) a privilege for the CISSU’s Director only.

¹³ Quote from one of the interviewees

It is recommended that the new Director of CISSU will clarify the workings (and the limitations) of this instrument within the context of the Safety and Security Management Working Group as a matter of urgency.

8. Future of CARE-International

8.1 Internal considerations

At this moment in time, with the possibility to (re) structure the CISSU in any shape that is seen as appropriate, it is relevant to consider the developments within the CARE confederation. If dramatic changes can be foreseen at this junction, it makes sense to anticipate these changes in the construction of CISSU-II.

The basis for the considerations on possible future constructs has been the governance reform as implemented in November 2008, and the vision paper 2020. Some members of CI's senior management were therefore consulted.

The conclusion from these documents and consultations can only be that a development towards CI as a network organisation with strongly interconnected management and information systems is the desired way forward (at the moment of writing). Globalisation progresses fast, and the challenges this present can only be answered by coherent and global responses, so is the conclusion of CI. National approaches just will not do. The fast approaching multi-polar world, with its emerging gravity centres in Asia will not be governed by an old fashioned monopoly on power by a "North-Atlantic Alliance". Organisations that are not truly reflecting this changing world are bound to loose out¹⁴.

The CI board has subscribed to these conclusions, and describes in the vision 2020 paper the future as follows.

More and new CI-members will take a share in (a form of) operations. Not necessarily in the traditional way as C-France and C-Deutschland have done recently, but also in newly to be developed ways. CO's are expected to transform into CI members. A form of CARE presence is expected to have been established in 100 (!) developed and developing countries. The need for a uniform and recognisable approach towards safety and security is more obvious and pressing than ever before.

These CI members are likely to develop more and different forms of engagement with the civil societies within their own countries, and at times also in other countries. TH exact form and place is as yet unclear, but the vision paper and related documents do show the ambition of CI's leadership to stimulate these developments.

It is obvious that in the picture of this sort of developments and ambitions, a number of pre-conditions exist. In the field of staff Safety and Security, such a precondition is the existence of and adherence to an agreed and respected security framework as developed in recent years via CISSU. The logical next step is to assure the implementation of this framework by existing and new CI members alike.

It is only all too obvious that such a process is best guarded by a unit as CISSU on a central level, as described throughout the report.

Recommendation

CISSU needs to anticipate these changes on a strategic level, and assure the whole confederation to adopt and adhere to the CI security framework.

The trends observed above only serve to indicate that the present governance structure as set in place since 2008 is likely to remain the way the confederation will be governing itself for the foreseeable future.

The model with the board and its four sub-committees is considered as successful and will stay in place. The International Secretariat will continue to play the overseeing role it has at present.

¹⁴ These conclusions are quotations from recommendations of the external review of 2008

Safety and Security is at present a dossier that is for the board being dealt with by the HR SSC. See above. It is a possibility to consider this dossier as a more executive one, and make it part and parcel of the mandate of the Executive Committee. A recommendation to this effect can be found in the "External Review of CARE International's November 2008 Governance Reforms" (page 18)¹⁵. The reviewer (of this CISSU review) is of the opinion that

- The most crucial factor is that the board does get a direct and unhindered first hand, systematised insight and possibility to have influence on, the functioning of CISSU and all related safety and security issues concerning the whole confederation at any time it so desires. Whether this information flow runs via the HRSSC committee or the ExCom is only of secondary importance.
- An important practical argument would suggest that it is preferential to maintain the reporting line via the HRSSC. This simply because the Executive committee is already overburdened with many, many issues and dossiers¹⁶.

Recommendation

Maintain the present reporting line via the HRSSC, *but under the strict precondition that the suggested adaptation of the composition of the HRSSC is implemented* (See 4.1).

8.2 External considerations

This review has focussed mainly on CI-internal issues and realities. This is inevitable given the ToR of the exercise. However, the review would not be complete if not a few words are spent on some of the external dimensions of CI's work.

The humanitarian and development contexts within which CI works are subject to relatively fast and constant changes. An event as 9/11 has had a tremendous impact on the delivering of humanitarian aid and enforces a constant position-taking by humanitarian and relief organisations vis a vis the actors in global as well as in regional conflicts. The need to develop the policy framework for cooperation with the military is a strong example of such positioning.

A recent publication as a UN(OCHA) report titled "stay and deliver"¹⁷ argues that organisations must be organised in such a way that they are able to continue to operate, also when conflicts become more intense. CI, on confederation level, needs a function that identifies these sorts of developments, and assures that a proper translation into operational action is facilitated within the confederation. An organisation as CI needs to be able to constantly reorient itself on such developments.

Whether or not it wants to do so is not relevant; it is forced to do so by the outside world to position itself on all this sort of external developments, and translate its position in adaptation of its operational models. Safety and Security will inevitably be an important factor in these considerations. Safety and Security aspects will continue to take a prominent role in the set of potential liabilities of the organisation. Legal and moral responsibilities will continue to be felt, and will increasingly be challenged.

For a globally working network organisation that CI ambitions to be, the need for centrally defined and globally executed policies and positions will only increase.

The organisation is obviously well prepared and aware of these and related challenges. It is in a constant process of adapting itself to meet these challenges. The installation of CISSU in 2006 and the governance restructuring of 2008 are only examples of this capacity to adapt.

Looking at CISSU's existence and performance over the past years, the conclusion can only be that CI is in need of functions such as CISSU (and CEG). They are indispensable instruments for a global network organisation as CI to cope with the challenges described above.

¹⁵ By the Berlin Civil Society Center, 16 September 2010

¹⁶ (Strong) opinion of an interviewee who has insight in the workload of Excom members

¹⁷ See "To stay and deliver"; good practice for humanitarians in complex security environments
An independent study commissioned by OCHA, March 2011

Recommendation

External developments point at an increasing need for coherence and unity in CI's approach towards safety and security. This forces the CISSU to focus on the strategical implications of the constant changes in the humanitarian landscape worldwide.

9. Overall conclusions by the reviewer

CISSU in its first years has undoubtedly had a significant and important impact on the appreciation of the dossier of safety and security within the CARE confederation. The output that it delivered helped to streamline safety and security practices. Over time, the security framework as developed by CISSU has become the standard within CI. Important to notice at this junction is that the CI framework can surely withstand critical comparisons with the policies and practices that are considered standard within the humanitarian - and development sector worldwide.

But the internal dynamic of CARE-International has its own dimensions as well. And within the confederation, different appreciations of the functioning of CISSU are inevitable.

In general, it can be concluded that those CI members that are further away from day-to-day operations have benefitted most of the existence of CISSU. Finally they discovered to have a "measuring stick" that helped them to develop an opinion and idea in how far CO's are in compliance with generally accepted standards. This helped to grow self-confidence and a critical attitude towards accepted practices of LM's that earlier could not be challenged in absence of a voice and a framework to do so. (Exceptions to this opinion exist)

Lead members also benefitted, but at a cost. For the first time, a function exists that has as a role to challenge the conventional wisdom of individual LM's and that also forced to challenge these of others. And of course, this proved painful at times, as it is generally more difficult to reach a form of consensus rather than be able just to do "your own thing".

A further institutional handicap that aggravates the pain in this process is the asymmetry that exists within the confederation. It is all too easy for the US-member to just rollersteam the others because of the operational/financial strength it has. They deserve to be applauded for not doing so. They have chosen to go the difficult road, the one of dialogue and consensus seeking rather than the one of doing things on their own. But that this process at times leads to friction and interpersonal irritations is inevitability. All involved will have to absorb the resulting frustration, and realise from time to time "what again is the common objective, why was it again that we want to work together".

And this common objective is still within the forefront of thinking of all: CI stakeholders recognise and respect the need for CI members to subscribe and adhere to a common, coherent and recognizable approach towards safety and security by all CI members.

And it is realised that in the (nearby!) future this will only become more important. New members will present themselves. Already India, Peru and Thailand exist and more are due to follow. It is only a matter of time before these new members start to have forms of operations, be it within their own countries or abroad. And at that moment the confederation will need to be able to guide these CO's on the standards that also they will need to comply with. At that moment, the need for a function as CISSU exercises at the moment is there.

This need is the cornerstone that binds CI members, both operational as well as non-operational.

But a lot of work still needs to be done. The reviewer observes underlying fundamental differences in safety and security approaches between members.

On one hand an approach with an emphasis on "hard" security strategies. Specialised staff, often with a military background that decide for the CO's where and what is acceptable and which risk minimising measures are to be put in place. On the other hand a school of thinking that wants to base its security strategies on more "softer" approaches. This thinking results in more explicit responsibilities for the CD's and their teams in identifying risks and defining the risk minimising measures.

Both approaches have their strengths and their weaknesses, both approaches can be opted for, and often a combination of these strategies will work best. The importance for CI is to have a centrally positioned function that oversees these differences, and works to bring them together.

The conclusion can only be that CI is advised to continue to invest in security through CISSU, bearing in mind the recommendations formulated throughout the report.

Annex to CISSU Review; list¹⁸ of interviewees¹⁹

CARE-International Secretariat - Geneva		
Dr. Robert GLASSER	CI Secretary General	Interview only
Marcy VIGODA	Deputy Secretary General	Interview only
Barbara JACKSON	Humanitarian Director	
Sally AUSTIN	Head of Emergency Operations (CEG)	Interview only
Jock BAKER	CI Emergency Quality Standards and Accountability Coordinator (CEG)	
Alexandre CARLE	(Former)Acting CISSU Director	Interview only
Pascal DAUDIN	Former CISSU Director	Interview only
Siw Dörte DIALLO	Former CISSU Desk Officer	
SSMWG - Safety and Security Management Working Group		
Carmen MICHIELIN	CARE USA, Atlanta. Security Director	
Rolfe BURNS	CARE USA, Atlanta. Operational Security Coordinator	
Barry STEYN	CARE USA, Cairo. Reg. Security Advisor Afr. / M.East	
Daniel ST PIERRE	CARE USA, Ghana. Reg. Security Advisor W&S Africa	
Chris WILLIAMS	CARE USA, Bangkok Reg. Security Advisor S&E Asia	
Stephen WILLIAMS	CARE AUSTRALIA, Canberra Manager Safety & Security Support / Special Projects	
Bogdan DUMITRU	CARE CANADA, Ottawa. Security Director	
Harbinder KAUR	CARE UK, London. Acting HR Director	
Peter RUNGE	CARE Deutschland-Luxembourg. Head of Programmes	
Safety and Security Focal Points		
Simone LANGENKAMP	CARE Netherlands. HR Officer Overseas Assignments	
CI National Directors		
Philippe Lévêque	CARE France – Paris	
Guus Eskens	CARE Netherlands – The Hague	
Niels Tofte	CARE Denmark – Copenhagen	
CI Country Directors		
Lex Kassenberg	CD Nepal, former CD Afghanistan	
Charles John Gondwe	Security Officer CI Pakistan (delegated to the SO by the CD)	
HR Safety and Security Committee		
Richard Greenhalgh	Chair of HR SSC	
Regional Emergency Coordinators		
Amadou Sayo	REC South and West Africa	
Hauke Hoops	REC Latin America and Caribbean	
Mohammed Khaled	REC Nairobi	
Others		
Bob McPherson	Former and Interim Security Director CISSU	
Jon MITCHELL	Head of Policy CARE USA.	Questionnaire only
Robert YALLOP	CARE Australia, Canberra Overseas Operations and Program	

¹⁸ Four CARE staff that were approached failed to respond (timely), those people are not listed above

¹⁹ Interviewees have participated both through the questionnaire and an interview unless indicated differently

Oliver Behn

Executive Coordinator
European Interagency Security Forum(EISF)