5

Improving the Positive Impact of Your Security Measures and Reducing Possible Negative Impact: The Do-No-Harm Approach

Changing our practices regarding security can have both positive and negative impacts. As we build new security practices, it is worthwhile considering how we can enhance the positive impact on security for ourselves and others, while at the same time monitoring and attempting to reduce any negative impacts that these might cause.

We must begin from the perspective that as human rights defenders at risk, we are often operating in a context characterised by conflict. This conflict may be armed or unarmed and the violence to which we are subjected may be direct physical or armed violence, or may be economic, gender-based, institutional, structural, economic, psychological, etc. At times, activist communities are affected by conflicts within organisations, communities or movements. At the very least, we are rarely free from dynamics of privilege (related to gender identity, sexual orientation, race, religion, ethnicity, language, socio-economic status, etc.) and other forms of structural violence.

When we begin to adopt new behaviours relating to security, there can be some unintended negative consequences which affect these conflicts as a result. This doesn't mean that changing our practices is a bad idea – rather, it's just a good idea to be aware of these potential negative consequences, so that we can make truly informed decisions.

To achieve this, it is useful to engage with the **Do No Harm (DNH) Approach**.[21] It assumes that all our actions and behaviours lead to consequences, both positive and negative.

Actions + Behaviours = Consequences.

In the context of conflicts both internal and external to the group, our actions and behaviours can create additional **division** between people (hence worsening the conflict) or additional **connection** between people (relieving the conflict). Below, we consider some of the ways in which our actions and behaviours can have positive or negative effects on these conflicts when we implement changes to our security practices.

Actions and resources

We understand actions as everything we do and bring into an existing situation, including the resources obtained, used, and transferred in the course of your work and while implementing your security practices. Resources for security and well-being are often considered to be valuable and access to them may be limited. As you expand the actions and resources you engage with for security within your group or organisation, what might be the impact of these resource transfers on yourself, your allies and your opponents?

There are some potentially negative consequences to be aware of here, and these could easily develop into serious security issues. Four ways in which this can happen are:

---

21 For more, see CDA Collaborative, Do No Harm http://www.cdacollaborative.orgprograms/do-no-harm/

1 **Competition vs. inclusivity**

Supplying resources (such as training, computer hardware or well-being resources) only to selected individuals within a group might increase already existing tensions or create new ones. On the other hand, being inclusive about using and sharing your resources might help to connect people and strengthen feelings of inclusivity. If resources cannot be shared among all members of the group, it's important to have open communication as to why this is the case (perhaps due to higher risk levels of the individuals in question) and obtain the support of the group for this decision.

2 **Substitution vs. appreciation**

Adopting new practices or implementing new resources can mean that old practices, traditions or even people's roles are replaced or pushed aside. It is important that existing strategies and resources be recognised and replaced only when justified and in a way which respects the efforts which were put into them.

3 **Selectivity and power relations**

The members of the group who receive any extra training, attention, responsibilities, etc., can, through their access to new knowledge and resources, also gain more informal or formal 'power' or influence within the group, which can aggravate existing tensions or lead to new ones. By contrast, where possible, including the whole group or organisation can enhance acceptance of security measures and reinforce a sense of unity in the whole team.

4 **Standard of living and working**

This is particularly relevant in the case of staff members and volunteers. Who gets which training? Who gets paid for which activities? Who benefits more from security practices or suffers more burdens in everyday life and work? Who has what access to communication due to living in rural or urban settings? How can these dividing differences be bridged?

Behaviours and implicit ethical messages

When building our capacities and adopting new practices, we ought to also be aware of our behaviours, how they change, and how this may impact others. Our behaviours send non-verbal, implicit messages to our fellow activists, colleagues, team, organisation, allies and adversaries. The interpretation of these messages can, like with our actions, lead to further connection or division within the group.

It is good to consider each of our new practices and the potential messages they send to those around us, and where possible, seek to verify them. Below, we explore four common ways in which our behaviours can lead to increased connection or division within the group.

1 **Cultural characteristics**

One 'lens' through which others interpret our behaviours is, of course, culture. In multi-cultural environments, it's a good idea to consider how new security practices may be interpreted through this filter. For example, notions such as privacy, or the value of certain resources or social traditions, or a means of decision-making often vary greatly between different cultures. Be sensitive to your cultural surroundings and check whether the new security measures you take are being interpreted in a way that doesn't cause offence or division.

2 **Different values for different lives**

This can be especially relevant in groups and organisations which are of mixed nationality or background and wherein differing levels of 'expertise' – occasionally reflective of social class structures – are present. If certain groups or members are not included in the emergency plan of their organisation, they might interpret this as a sign that the organisation does not care as much about their security. Some international organisations, for example, do not reflect and plan for an evacuation of their local staff in an emergency, and focus only on their international staff. This can send a message that the well-being of some staff is more valuable than that of others. Furthermore, the importance of security awareness among administrative staff, cleaners and so on is often overlooked: consider who will pick up the telephone in order to receive an emergency call, or is most likely to recognise potential security indicators in the building? An inclusive approach not only allows for more cohesion and ownership of security measures in teams, but also to improved security for everybody.

3 Fear, tension and mistrust

Adopting new security measures can also be interpreted as communicating a lack of trust of and among colleagues, fellow activists or other stakeholders. For example, encrypting your calls over the mobile network could be understood as stating that you mistrust your regular telephone service provider; similarly, being less readily available for certain dangerous activities can lead to increased mistrust among fellow activists. As such, it is important to simply clarify the reasons for your new security measures and the logic behind them in a frank, open and honest way. Listen to feedback and commentary from those around you to see whether there are any consequences which can be avoided or worked on, and do what you can to maintain trust in both directions. In the case of adopting radical new security measures and thereby potentially attracting negative attention from adversaries or neutral parties – such as through encrypting communications, and being noted by telephone or Internet Service Providers – consider using old or common methods in parallel to new ones in order to lower suspicion.

4 Use of resources

Any new resources – such as computer hardware or software, training, vehicles, access to psycho-social support, etc. – which are made available for increased security – should be used responsibly by those who have access to them. Group or staff members who do not have prioritised access to such resources can get the impression that they are used by their colleagues for their own personal benefit if their purpose is not shared within the group or organisation. This exclusivity can send out the message that the one who is in control of resources can use them for his or her own purposes without being held accountable.

In order to analyse your behaviour and the messages in your own security practices, it may be useful to draw a table such as the example in **Appendix F** and consider the examples given before filling it in for yourself.

We should consider our practices in light of these concepts and talk about them in a safe space with our friends, family and colleagues to try to fortify their positive effects on our relationships, and lessen their negative effects. Reflecting on our security framework in terms these questions might prevent us from producing new kinds of threats scenarios by our security set-up by creating more connecting activities and behaviours, which benefit everybody's security.

Conclusion

Through **Prepare**, **Explore** and **Strategise**, we have charted a path from defining security for ourselves and creating a space for security within our organisations, through carrying out an analysis and diagnosis of our security situation, and planning for maintaining and improving our security in the course of our work as human rights defenders.

How you will implement this idealised series of steps depends greatly on the nature of your work, and those with whom you work. It is important to keep in mind that they represent a cyclical process of evolution, and constant reassessment of our situation and updating of strategies and plans is ideal.

While the three Sections in this manual have focused on the management of a security capacity-building process in a group, the next step is to get to know particular tools and tactics which you can put into practice for increased security during different aspects of your work.

In **Section IV | Act** you can find tools and tactics sourced from a community of human rights defenders, trainers and experts on security and well-being which can be implemented in particular, high-risk activities for human rights work.

Further Reading

- **CAPACITAR Emergency Response Tool Kit**
  A response to the trauma of Hurricane Katrina, the kit includes simple basic practices taught by Capacitar to empower people to deal with the stress of challenging situations.
  http://www.capacitar.org/emergency_kits.html

- **CDA Collaborative, Do No Harm**
  A framework for analyzing the impacts of aid on conflict and for taking action to reduce negative impacts and maximize positive impacts.
  http://cdacollaborative.org/cdaproject/the-do-no-harm-project/

- **Insiste, Persiste, Resiste, Existe: Women Human Rights Defenders' Security Strategies**
  The report brings together the voices of women human rights defenders from

all over the world on combating violence and discrimination in complex contexts – in situations of overt or hidden conflict, organised armed violence as well as rising fundamentalisms.
http://kvinnatillkvinna.se/en/publication/2013/04/18/insiste-persiste-resiste-existe-2009/

- **Integrated Security: The Manual**
  This manual covers all aspects of an activists work and life, from health and personal networks to secure working spaces. This manual shows how you, a human rights defender, facilitator, international human rights organization, supporting donor or organization working in emergency and development contexts can arrange Integrated Security Workshops.
  http://integratedsecuritymanual.org

- **New Protection Manual for Human Rights Defenders**
  The purpose of this manual is to provide human rights defenders with additional knowledge and some tools that may be useful for improving their understanding of security and protection.
  http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/

- **Security in-a-Box: Tools and Tactics for your Digital Security**
  A digital security toolkit for activists and human rights defenders throughout the world.
  https://securityinabox.org

- **Security to Go: A Risk Management Toolkit for Humanitarian Aid**
  A simple, easy-to-use guide for non-security experts to quickly set up basic safety, security and risk management systems in new contexts or rapid onset emergency response situations.
  https://www.eisf.eu/library/security-to-go-a-risk-management-toolkit-for-humanitarian-aid-agencies/

- **Workbook on Security: Practical Steps for Human Rights Defenders**
  A step by step guide to producing a security plan – for yourself and/or your organisation following a systematic approach for assessing your security situation and developing risk and vulnerability reduction strategies and tactics.
  https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk