Training workshop on Physical Protection and digital security of human rights defenders, activists and journalists working in most at risk regions of Cameroon

HRDs Security Training Facilitation Guide

Module 2

By

DR. KELLY NGYAH

CEO OF MAHSRA

Module 2:

Evaluation of Security Incidents and Establishment of Individual and Organizational Security Plans

Objective:

Educate HRDs and journalists on security incidents and build their capacities to plan and manage their individual and organizational security issues.

Expectations:

1. Participants gain knowledge and are able to avoid undue activity limitations, arrests and arbitrary detentions .
2. Participants gain knowledge and are able predict and manage security incidents at individual and organizational levels.
3. Participants gain knowledge and are able to build and manage individual and organizational security plans.
4. Participants gain preliminary knowledge on individual and organizational security concerns in armed conflict zones.

Working against Undue Activity Limitations, Arrests and Arbitrary Detention

Arrest and arbitrary detention of HRDs and journalists, in the case of Cameroon, mostly occur because these actors do not pay close attention to the potential threats and other security warnings in the course of their work. In the course of our activities, we need to pay close attention on our workspace and those who do not share our aims and goals, and our adversaries or those who oppose our works. Those against our activities will always strive to limit or end them through various forms including, having access to resources, freedom of expression, surveillance and censorship, and judicial, administrative and bureaucratic harassments. If they try to limit us and do not succeed they will proceed with manoeuvres for arrests and arbitrary detentions.

As HRDs and journalists at risk, we need to expand our workspace and places and build on communication base intractability. Workspace and places could include physical places such as public squares and offices or homes; social spaces such as social gatherings; technological spaces such as the internet; and legal spaces such as administrative procedures. While matters of intractability of our workspaces could help in preventing eventual attacks, there is further need to develop and adopt practices, tools and tactics that can encourage others to accept our works, deter those against us and as well protect us during workspace expansion processes. Some measures may include but are not limited to:

Working against Undue Activity Limitations, Arrests and Arbitrary Detention. *Continues...*

- ❖Conduct friendly human rights education and sensitisation talks with family members, friends, civil society organisations and other interested parties.
- ❖Assess third parties' individual interests, fears and anxiety levels with regards to our works and discuss when and where necessary the issues at stake, in order to assess their support.
- ❖Conduct third party investigations in order to understand our adversaries and their reasons for such opposition.
- ❖Understand the relations and connections of people who show much interest to our works in general or to particular human rights crisis situations.
- ❖Share our work ideologies and request for institutional backup support from diplomatic and other international bodies, national human rights institutions and human rights civil society networks;
- ❖Avoid unauthorised access to our work places and spaces and completely understand the motives and reasons for all authorised accesses.
- ❖Assure that there are always effective backup mechanisms to safeguard individual security and sensitive human rights information storages especially during an ongoing denunciation process.
- ❖Know confidential hiding places or escape routes and how to leave your work place and/or space for a while if necessary.

A good assessment on the above points will help us understand the possible angles of threats that can push us to sudden situations of arrests. When we assess that such risks are high, we need to take time out to draft out a lifestyle adjustment plan in order to avoid places and positions where we could easily get arrested depending on our local contexts. (30MINS)

Discussions: participants propose and make a list of lifestyle adjustment factors according to their individual contexts. (30MINS)

How to Manage Arbitrary Arrests and Detentions

In the case of arbitrary arrest or detention, the first issue in place is situational notification. This works in line with a security plan that oversees the work of the HRD or the journalist. Options to consider here include:

- Your ability to build and stay accountable with strong human rights and media networks that are aware of your local situation and ready to intervene.
- Trusted colleagues or friends who understand and are regularly in touch with you and your activities.
- A list of influential contacts that can be used by your trusted colleagues or friends in case you are unduly arrested or detained.
- A standby lawyer to be contacted by your trusted friends and colleagues.

(10MINS)

Participants discuss their experiences and options they took to remedy their situation. (20MINS)

The Security Incident

A security incident refers to an event that may indicate that our work has been compromised or there has been a breach to our organization's management parameters. Simply, a security incident can be defined as any fact or event which you think could affect your personal or organizational security. It therefore draws in the need to minimize impacts from such breaches or compromises.

Managing security incidents imply that you notice an issue; you realise in might be a security incident; you register it and discuss or analyse it with your colleagues; you establish the fact that it is a security incident, and then you react accordingly.

Approaches to manage security incidents and mitigate impacts include:

1) **Information control**. This relies on the management of both digital and analogue forms of data communications which are means for compromising HRDs' and journalists' work security.

   ✓Ability to identify sensitive data, its source of origin and who else has access to such data before processing communication.

   ✓Ability to monitor and follow-up information storage and communication channels.

   ✓Ability to replicate information storage and communication from other anonymous centres that are different from one's original work place and space.

   ✓Ability to store and communicate in coded languages or code sensitive information that is targeted to particular third parties only.

The Security Incident. Continues...

Approaches to manage security incidents and mitigate impacts *continues...*

2) **Resilience and Agility**. With respect to resilience and agility, it is important as human rights defenders and journalist to understand that due to the unexpected events that may befall us at any point in time in the course of our work, we need to develop the necessary emotional and mental flexibility to cope up with situations. This implies cultivating a strong sense of mental and emotional centeredness to face and cope with security incidents and as well as risks and threats that are largely unpredictable. In fact, it is our own vulnerability that keeps us connected to the experiences of others whose rights are being violated; therefore, it becomes impracticable to keep ourselves completely safe. With this mind-frame, we now need to build resilience that will help us recover quickly from set-backs, and agility to improve on our flexibility in developing and adopting new security practices or responding to emerging risks. (30MINS)

Participants propose resilience and agility measures that apply to their individual situations (10MINS)

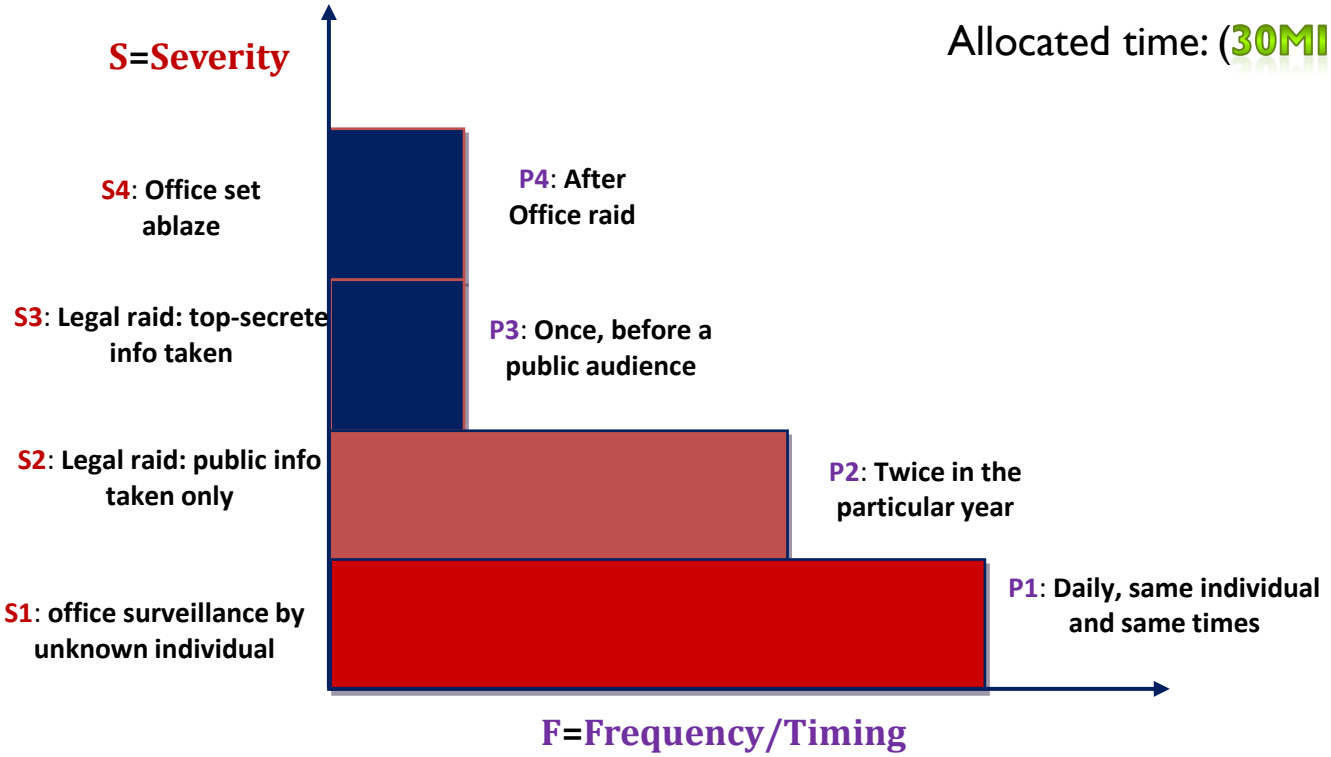
Assessing Security Incidents

Classifying security incidents and threats may help to analyse and make it possible to anticipate them at specific moments. For example, if they are records of reported security incidents around pre-electoral periods, it is likely that such may occur again at the following pre-electoral period. The records can also help assess the likeness of an action happening against the HRD or journalist by the potential aggressor or; in case of security incidents due to his/her carelessness; and can also contribute to assess how security is being managed by HRDs and journalists themselves.

@protection international. See sample security assessment chart on the following slide.

Assessing Security Incidents. continues...

Allocated time: (30MINS)



P: Probability of imminent more severe action against HRD or journalist from a potential aggressor

P1: VERY LOW (***S1***: office surveillance by unknown individual + ***P1***: daily, same individual at same times)

P2: LOW: (***S2***: legal office raid: public information only taken + ***P2***: twice in the concerned year at no specific moments)

P3: HIGH: (***S3***: legal office raid: top secret information taken (classified witnesses names taken) + ***P3***: Once just before a public audience)

P4: VERY HIGH: (***S4***: Office set ablaze + ***P4***: after office raid at ***P4***)

Creating Individual and Organisational Security Plan

In building a security plan for HRDs and journalists and/or their organisations, Frontline proposes three approaches to security for consideration. It is for the individual or organisation to chose that which best suite their context of activity. These include the acceptance, the protection and the deterrence strategies.

The **acceptance strategy** involves liaising with all actors including local community level leaders and administrative authorities in order to gain acceptance and total support for your work.

The **protection strategy** is an approach that focuses on procedures and protective measures such as in minimising vulnerabilities.

The **deterrence strategy** is that which uses counter threats to ascertain protection. For example, when you feel threatened, you decide to return the threats with counter-threats such as through lawsuits or promising to go public with the issues at-stake.

Allocated time: (5MINS)

What to consider when creating individual and organisational security plan

- Bear in mind the aim of mitigating risks which involves: reducing the level of threat you are experiencing; reducing your vulnerabilities; and improving your capacities.
- Include a day-to-day policy, measures and protocols for managing specific situations.
- Include a day-to-day policy and measures for routine work.
- Include permanent advocacy, networking, codes of ethics, culture of security, security management, etc.
- Ensure that permanent measures are made to ensure that routine works are done in accordance with security standards.
- Ensure preventive protocols: for example on how to prepare a press conference or travelling to remote and risky areas.
- Prepare emergency protocols for reacting to specific contingency issues, such as detention or disappearance.

Allocated time: (15MINS)

Creating an Individual Security Plan

From the general considerations mentioned in the previous slide, the individual should be able to draft a tabulated structure for assessing his/her risks.

For example, If the risk you face is **KIDNAP** your table will consist of the following:

- ✓ The probability or likelihood of being kidnapped.
- ✓ The impact of the kidnap with reflections on what may happen to you while in the hands of the kidnappers.
- ✓ Assessments on the level of threats you have previously noticed from different persons or groups depending on the area of your activity. Armed or unarmed groups are perceived differently.
- ✓ Assessment on your vulnerabilities in case you need to adjust your lifestyle in order not to be identified at zones of high risks.
- ✓ Considerations on your capacities whether you have resources for security and the ability to plan well. This should help you design an action plan and with consideration of all the actors.
- ✓ Preparations on your contingency plan which is majorly your reflection on the what to do in case you are eventually kidnapped. This includes, how to stay safe in the hands of the kidnappers, keeping busy in trying to memorise details, and also having an understanding on whom or what will negotiate for your release.

Allocated time: (10MINS)

Creating an Organisational Security Plan

This needs cross-sectional reflections on all the risks your organisation may be facing and should be discussed with the staff or concerned colleagues within the organisation. Depending on the level of risks as assessed by the risk matrix, your organisation may decide to focus at the level which it deems fit for its use. Some major factors to consider include:

- ✓ Discussing and agreeing on group risks.
- ✓ Agreeing on the procedures to follow which should reflect security approach content and policies.
- ✓ Identifying material and psychological issues for building your organisations' security concerns.
- ✓ Allocating responsibilities for drafting and finalising risk management plans.
- ✓ Communicating the organisational security plans to those in need of it.
- ✓ Ensuring that there is a leadership for monitoring the implementation of the security plan.
- ✓ Develop and regularly upgrade on the organisation's crises management plans for unanticipated emergencies and contingency needs. (10MINS)

Participants discuss items or issues that can improve their individual and organisational security (15MINS)

Security in Armed Conflict Areas

HRDs and journalist face special risks during armed conflict or war situations wherein indiscriminate and target killings of civilians are a recurrent issue. Though it may be very difficult to control the politically motivated killings by the military and those of the opposing armed militia, if you are resident within any of such armed conflict areas, you should have a priority in keep you and your family save. On the contrary, if you are not resident but have to work in the armed conflict zones, you should make the following reflections:

- What is the level of risk, you and/or your organisation are willing to tolerate?
- How does your benefits and risks analyses reflect your long-term human rights works?
- Are you beware of the possibilities of finding yourself under a mortar or sniper attack?

In an armed conflict area, you may never know whether you are being targeted or not, so, you should give concern to reducing your vulnerabilities by:

- Avoiding dangerous places.
- Finding adequate protection from attacks such as window shields, sandbags, identified organisational vehicles when such is respected etc.
- Beware of landmines, booby traps and unexploded ordinances. (15MINS)

END OF SESSION

ABOUT:

This training guide (Module 1 & Module 2) for human rights defenders (HRDs) and journalists security has been researched and written by Dr. Kelly NGYAH, Chief Executive Officer (CEO) of Modern Advocacy Humanitarian Social and Rehabilitation Association (MAHSRA).

It can be copied or downloaded freely when and where necessary for the benefit of HDRs and journalists at risk so long as the source/authors are acknowledged.

For additional usages other the purpose mentioned above, the source/authors should be contacted with the following address:

The Chief Executive Officer,
Modern Advocacy Humanitarian Social and
Rehabilitation Association (MAHSRA),
Commercial Avenue,
PO Box 1091, Bamenda – Cameroon,
Tel: **+237654904225; +237662504497**
Email: books@mahsra.org

ACKNOWLEDGEMENTS:

- Pair Educateurs et Promoteurs (PEP) Sans Frontières for organizing the "Training workshop on physical and digital security protection for human rights defenders , activists and journalists working in most at risk regions of Cameroon"
- Frontline Defenders Ireland for their security workbook: practical steps for human rights defenders.
- Protection International for their new protection manual for human rights defenders.