SECURITY CHALLENGE: NON-STATE ARMED GROUPS

Recommendations for work in the DRC in the context of the Ebola emergency response 2019-20

In March, suspected ADF forces burnt down a health clinic and several houses during an attack on Lubwasi town. Six civilians were also killed by guns or machetes, and several houses in the area were burnt down.

CONTEXT AND KEY CHALLENGES

Using open sources, key informant interviews and data shared by response actors, **Insecurity Insight** has identified the following contextual challenges relating to the presence and involvement of non-state armed groups in response areas of operation that have impacted both response actors' security and their access to affected communities.

- During the first six months of 2019, armed groups carried out over 550 attacks on civilians. In some of these attacks **healthcare facilities were burnt down or staff members were killed or abducted**.
- Some attacks directly targeted healthcare workers or facilities. Other attacks targeted a whole town and, therefore, healthcare workers were among the affected civilians and healthcare facilities among the looted properties.
- Over 100 armed groups, including Mai Mai militia and ADF forces, operate in Ebola-outbreak areas. There are tensions and competitions between the various armed groups.
- Boundaries between armed groups and state actors can be fluid and motives are not always clear. Soldiers serving with the state's armed forces can also be active armed group members. Criminal acts can be perpetrated by both armed groups and soldiers. Medical equipment or drugs may be looted to supply an armed group with needed medical care.
- Armed groups can be embedded within local communities or have close relations with them, and may share community perceptions that the Ebola crisis was artificially created to profit elites.
- Armed groups tend to have economic interests to sustain themselves.

SECURITY STRATEGY

While every organisation should adopt a combination of security strategies in accordance with the contextual dynamics of the area in which it operates, in terms of the DRC Ebola response evidence gathered by Insecurity Insight from open sources, key informant interviews and data from response actors **suggests that a strong emphasis should be placed on adopting an acceptance approach to security.**

This approach should aim to encourage non-state armed groups to accept the presence and work of response actors. An acceptance strategy can be successful in engaging armed groups to provide constructive support. Some non-state armed groups have been known to intervene with local communities on behalf of response actors, and to facilitate access to these communities when they (i.e. the armed groups) have accepted the response actors' presence and work.

Geneva Call's Deed of Commitment

In the Deed of Commitment, armed groups publicly commit to maintaining and providing access for affected populations to essential healthcare facilities, goods and services, without adverse distinction, and to facilitating the provision of healthcare by impartial and neutral humanitarian organisations. Current signees: **Alliance of Patriots for a Free and Sovereign Congo (APCLS)**.

SECURITY STRATEGY

To effectively implement an acceptance strategy, the following points apply:

- Adherence to the principles of neutrality, impartiality and independence is key.
- Response actors who appear biased towards one group can inflame a volatile situation.
- Transparency and open dialogue are important to avoid the perception by non-state armed groups that response actors are spying or otherwise trying to undermine their authority in the operational context in which these groups operate.
- Any practices that could be perceived as profiting from the delivery of healthcare services or other humanitarian activities should be avoided.
- The use of armed escorts should be carefully considered. In some contexts, using them can increase security risks and may incite attacks or cause response actors to be distrusted.

Response organisations can use three security strategies in humanitarian settings:

- **Acceptance** involves building a safe operating environment through the approval, consent and cooperation of communities, local authorities and other stakeholders in the operational area.
- **Protection** involves reducing risk by reducing the vulnerability of the organisation and its employees, e.g. through the use of walls, fences and armoured vehicles..
- **Deterrence** involves reducing risk by containing external threats through the use of counter-threats, e.g. obtaining armed protection and exercising diplomatic/political leverage.

Most response organisations will adopt a combination of these approaches, based on what they perceive as being appropriate to a particular setting. However, it is important to remember that the behaviour and approach of a response actor will impact future efforts to develop community acceptance, e.g. the use of armed protection.[1]

SECURITY RISK MANAGEMENT MEASURES

In the DRC Ebola response, response actors are encouraged to consider the following when developing their security plans and implementing security measures to deal with threats posed by non-state armed groups:

- Carry out regular contextual analysis and map the actors in each operational area. This is particularly important in eastern DRC, where rival armed groups and shifting power dynamics have a significant effect on response actors' security and access to communities.
- Be aware of how responders' activities are perceived and adopt a strategy of proactively influencing perceptions. This can be achieved, for example, through adhering to joint principles of engagement, adhering to humanitarian principles, and clearly and assertively communicating the role and objectives of response actors.
- Explore and develop interventions that are specific to the operational area. The needs and understandings of one non-state armed group can vary from that of another. This is true for community members as well. Avoid copying strategies blindly from other contexts.
- Develop strategic partnerships and/or positive relationships with other response actors, local communities, and state security forces and non-state armed groups.
- Establish and maintain transparent and consistent relations with armed actors. Long-term presence in the community, reach and communication are key.
- Where necessary, distance a health programme or other humanitarian activity from actors not perceived as neutral, in order to strengthen reach and independence.
- Be contactable.

SECURITY RISK MANAGEMENT MEASURES

- Coordinate with other response actors to overcome challenges to community access. Adherence to joint principles of community engagement can improve communities' and non-state armed groups' perception of response actors. Failure by one response actor to collaborate and adhere to principles can have knock-on effects on all response actors and severely curtail community access and staff security.
- Adopt a clearly defined vision of what health and other humanitarian interventions are working to achieve and clearly communicate the objectives and priorities of interventions in a way that it is well understood.
- Ensure that stakeholders from the local community, the government and non-state actors are engaged before commencing outreach work. There are examples in the DRC of non-state armed groups positively engaging with local communities on response issues on behalf of response actors.
- Be transparent about funding sources and objectives. Where this is possible and appropriate, maintain an open dialogue with armed groups about the organisation's activities and objectives, especially in areas where organisations work simultaneously with multiple rival armed groups.
- Conduct staff training to develop staff skills and capacity, especially in the areas of communication and negotiation with armed groups.
- Learn from security incidents. A strong security incident information management system can help organisations to understand the circumstances surrounding security incidents and support them with ongoing context analyses and risk assessments. For example, a robust incident report following an incident involving an armed group can support in-depth analysis of the cause and consequences of the incident and inform future engagement in the area and/or with that armed group.

Security risk management process

To improve the security of response actors and their access to affected communities, organisations should follow a security risk management process that involves the identification of risks and implementation of mitigating measures. Broadly, this involves:

- carrying out a contextual analysis and mapping the actors in each operational area;
- assessing the risks that response actors will face in each operational area (i.e. by carrying out a risk assessment);
- identifying possible risk management measures to mitigate identified risks. These include:
  - measures that prevent the risk altogether (e.g. not operating in a given context);
  - measures that reduce the likelihood of risks occurring (e.g. implementing a curfew for healthcare responders);
  - measures that reduce the impact should an event happen (e.g. evacuation and emergency medical support);
- developing a security plan that incorporates these identified measures and provides guidance for staff on how to implement them through detailed standard operating procedures and contingency plans;
- implementing a security incident information management system through which security incidents are reported, analysed and used to inform improved security risk management measures.

FURTHER READING

Geneva Call: www.genevacall.org/wp-content/uploads/2019/07/GC-Negotiation-of-humanitarian-access-in-NK_EN2.pdf
ICRC: www.icrc.org/en/doc/assets/files/review/2011/irrc-883-schneckener.pdf
International Law: www.armedgroups-internationallaw.org/2019/02/18/engaging-armed-non-state-actors-on-the-protection-of-health-care-some-promising-steps/
RefWorld: https://www.refworld.org/pdfid/57e92e4d4.pdf
CSIS: htthttps://www.csis.org/analysis/north-kivus-ebola-outbreak-day-90-what-be-done
CSIS: :/www.csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/120125_Rubenstein_ProtectionOfHealth_Web.pdf
https://acceptanceresearch.files.wordpress.com/2012/01/acceptance-toolkit-final-for-print-with-notes.pdf
AWSD: www.aidworkersecurity.org/sites/default/files/AidWorkerSecurityReport_2013_web.pdf
EISF: www.eisf.eu/news/community-mistrust-why-the-drcs-ebola-epidemic/

OTHER DOCUMENTS IN THE SERIES

1. *Introduction* **to delivering aid and emergency healthcare in insecure settings**
2. **Introduction to** *Security Risk Management*
3. **Security challenge:** *Non-state armed groups*
4. **Security challenge:** *Community resistance and mistrust*
5. **Security challenge:** *Arson attacks on healthcare facilities*
6. **Security challenge:** *Abduction of health workers*
7. **Security challenge:** *Sexual violence and abuse*

RESOURCES OFFERED BY INSECURITY INSIGHT

Mailing list

- Sign up to receive all the *latest news and resources* from Insecurity Insight.

Reports

- *Monthly News Briefs*: These provide briefings on safety, security and access incidents that affect healthcare workers, infrastructure and services around the world. They are compiled from open sources with links to the original information where possible, and provide a summary of WHO SSA-reported events.
- *Attacks on Health Care in the Context of the Ebola Response*: This provides an overview of reported verified submissions from Insecurity Insight partner agencies and open-source incidents affecting the delivery of healthcare in the DRC in 2019.

Datasets

- *Attacks on Health Care in the DRC during the Ebola Response*: This dataset contains verified submissions from Aid in Danger partner agencies and open-source data on incidents affecting the delivery of healthcare in the DRC between January 2018 and November 2019.

Podcasts

- *Humanitarian Incidents podcasts*: These constitute a series of conversations with experts discussing how to understand, manage and use information on incidents, and how this can improve organisations' risk management procedures and access to crisis-affected populations. Developed together with EISF and RedR UK.

Handbook

- *Security Incident Information Management (SIIM):* This guidance handbook and tool kit shares best practice, guidelines, tools and recommendations to enhance organisational security incident information management. Developed together with EISF and RedR UK.

This document was produced by **Insecurity Insight** as part of the **H2H Network** DR Congo Ebola response activation and has been funded by the H2H Fund, which is supported by aid from the UK government. This information is part of the general data collection activities carried out by Insecurity Insight in support of the **Safeguarding Health in Conflict Coalition (SHCC)** and the **Researching the Impacts of Attacks on Healthcare Project (RIAH)**. It is supported by the **Department for International Development (DFID)** of the UK government. Image: Goran Tomasevic/REUTERS