SECURITY CHALLENGE: ARSON ATTACKS

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

In February in Butembo city, where mistrust in aid workers and rumours about treatment are rampant, unidentified perpetrators set vehicles and parts of an MSF-run Ebola treatment centre on fire, destroying medical wards and equipment, and leaving four patients missing.

CONTEXT AND KEY CHALLENGES

Using open sources, key informant interviews and data shared by response actors, **Insecurity Insight** has identified a heightened risk of arson attacks against healthcare facilities in Ebola-affected areas of the DRC, with implications for response actors' security and access to affected communities.

- More than **40 reports of arson attacks on healthcare facilities** in the DRC were reported in 2019.
- The number of reported arson attacks was particularly high between February to May and in October and occurred during wider assaults on the area by armed groups and in areas characterised by community mistrust of Ebola relief efforts.
- Arson attacks are a common security threat facing healthcare facilities in Africa. In 2018, arson attacks on healthcare facilities were also reported in ten other countries, including Nigeria (by Boko Haram) and Cameroon (by Cameroonian forces).

SECURITY STRATEGY

The exact reasons for arson attacks on healthcare facilities are unclear, but they are possibly caused by community members' or other stakeholders' mistrust of and resentment towards response actors, or are part of a larger strategy by particular stakeholders to undermine response activities for political, economic or other reasons.

Preventing such attacks requires better communication and engagement with potential perpetrators, including local communities and non-state armed groups. But this is not always possible. Therefore, organisations are encouraged to adopt a combined approach to address this risk. Such an approach could include, for example, engaging in acceptance activities to improve local community and other stakeholder acceptance of and consent to response actors' presence and work. Organisations should also aim to implement protection measures to reduce the vulnerability of healthcare and other response facilities to arson attacks.

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 developing security plans and implementing security measures that prepare response actors for the threat of arson attacks on response facilities and provide guidance on how to respond in the event of an attack:

- Appoint fire warden(s) to develop and implement an evacuation plan.
- Identify an appropriate and secure alternative location to house patients and staff.
- Consider taking out insurance policies and medical coverage.
- Conduct regular inspection, monitoring, and maintenance of the site and fire-extinguishing system.
- Carry out fire evacuation and equipment training, and hold regular drills on accessing primary and secondary safe areas.
- Provide first-aid supplies to treat burns, and train staff on how to use these supplies.
- Engage and manage relations with local agencies (fire fighters, security forces) to better understand their capacity for intervention.
- Draw up a crisis management plan and pre-identify members of a crisis or incident management team that can provide support by coordinating emergency medical and psychological care for affected staff and patients, contacting and liaising with family members of affected individuals, coordinating the relocation and/or evacuation of staff, managing media and communications, and managing all the other issues relating to the incident.
- Assess the impact of the organisation's withdrawal following a severe attack and develop an appropriate and secure exit strategy should the organisation deem programme closure or temporary withdrawal necessary following a severe incident.

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

EISF: www.eisf.eu/wp-content/uploads/2017/04/EISF_Security-to-go_guide_Module-7_Security-of-facilities-2nd-ed.pdf
EISF: www.eisf.eu/library/office-closure-eisf-guide/
EISF: www.eisf.eu/library/crisis-management-of-critical-incidents/

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