Operational Security Management in Violent Environments

Koenraad Van Brabant

This is the outcome of a training-oriented research and research-oriented training project, in collaboration with a wide range of individuals from the main types of humanitarian organisations (UN, Red Cross movement, NGOs, think-tanks). Its primary target audience are field-level aid agency managers responsible for security of staff and assets, for whom the GPR should serve as a practical reference tool. It offers a systematic step-by-step approach to security management starting from context analysis and threat and risk assessment, to security strategy choice and security planning. It reviews major types of threats (battlefield survival, vehicle safety, site security, sexual assault, abduction and kidnapping, etc), measures to try and prevent them, and guidelines on how to survive and manage an incident if it occurs. It also stresses the importance of incident analysis and better exchange of security information between agencies. Finally, a number of crosscutting themes are explored that are relevant to risk control such as personal and team competency, clarity towards national staff, good communications, briefing and training, etc. The annexes provide additional information, for example, on legal protection of aid workers, private security companies, the UN security management system, and insurance cover. The arguments in the GPR are illustrated with case material drawn from all over the world.

This Good Practice Review is supported by:

OFDA/USAID

Netherlands Ministerie van Buitenlandse Zaken/Ministry of Foreign Affairs

Sida

Danida

Department of Foreign Affairs, Ireland

ISBN 0 85003 457 4

£14.95

Published by the Humanitarian Practice Network at the Overseas Development Institute

June 2000
About the Author
Koenraad Van Brabant, like many others, was given responsibility for staff and asset security in various international programmes without any formal training—notably in Afghanistan, east Ethiopia and Sri Lanka. He therefore had to learn ‘on the job’. Dissatisfaction with such dangerous and sometimes tragic practices provided an initial motivation for research and training on better security practice. For the past three years he has been working at the ODI with the HPN (former RRN), and as a research fellow.
Operational Security Management in Violent Environments

A Field Manual for Aid Agencies

by Koenraad Van Brabant

Good Practice Review 8

Humanitarian Practice Network (HPN)
Overseas Development Institute, London
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Sexual Aggression</td>
<td>155</td>
</tr>
<tr>
<td>12.1</td>
<td>Definitions and Scope</td>
<td>156</td>
</tr>
<tr>
<td>12.2</td>
<td>Risk Reduction</td>
<td>157</td>
</tr>
<tr>
<td>12.3</td>
<td>Surviving Sexual Assault and Rape</td>
<td>161</td>
</tr>
<tr>
<td>12.4</td>
<td>Crisis Management</td>
<td>164</td>
</tr>
<tr>
<td>12.5</td>
<td>Recovering</td>
<td>174</td>
</tr>
<tr>
<td>12.6</td>
<td>Cultural Differences</td>
<td>175</td>
</tr>
<tr>
<td>12.7</td>
<td>Preparation and Training</td>
<td>175</td>
</tr>
<tr>
<td>13</td>
<td>Detention, Arrest, Abduction, Kidnapping and Hostage Taking</td>
<td>178</td>
</tr>
<tr>
<td>13.1</td>
<td>What Sort of Disappearance?</td>
<td>179</td>
</tr>
<tr>
<td>13.2</td>
<td>Risk Reduction</td>
<td>181</td>
</tr>
<tr>
<td>13.3</td>
<td>Crisis Management: Detention, Arrest, Abduction</td>
<td>185</td>
</tr>
<tr>
<td>13.4</td>
<td>Crisis Management: Kidnapping</td>
<td>187</td>
</tr>
<tr>
<td>13.5</td>
<td>A Hostage/Siege Situation</td>
<td>203</td>
</tr>
<tr>
<td>13.6</td>
<td>Managing the Return of the Abducted/Kidnapped</td>
<td>204</td>
</tr>
<tr>
<td>13.7</td>
<td>Preparation and Training</td>
<td>205</td>
</tr>
<tr>
<td>14</td>
<td>Withdrawal and Hibernation</td>
<td>208</td>
</tr>
<tr>
<td>14.1</td>
<td>Planning</td>
<td>209</td>
</tr>
<tr>
<td>14.2</td>
<td>Preparedness: Management and Practical Steps</td>
<td>214</td>
</tr>
<tr>
<td>14.3</td>
<td>Preparedness: Staff Policy</td>
<td>219</td>
</tr>
<tr>
<td>14.4</td>
<td>Programme Continuation</td>
<td>222</td>
</tr>
<tr>
<td>14.5</td>
<td>Crisis Management</td>
<td>223</td>
</tr>
<tr>
<td>14.6</td>
<td>Hibernation</td>
<td>226</td>
</tr>
<tr>
<td>14.7</td>
<td>Post-evacuation Steps</td>
<td>227</td>
</tr>
<tr>
<td>14.8</td>
<td>Exploring Return</td>
<td>228</td>
</tr>
<tr>
<td>14.9</td>
<td>Preparation and Training</td>
<td>228</td>
</tr>
</tbody>
</table>

**PART V INFORMATION AND COMMUNICATION MANAGEMENT**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Protecting Information</td>
<td>232</td>
</tr>
<tr>
<td>15.1</td>
<td>Key Records</td>
<td>233</td>
</tr>
<tr>
<td>15.2</td>
<td>Sensitive Records</td>
<td>234</td>
</tr>
<tr>
<td>15.3</td>
<td>Discreteness and Encoding</td>
<td>235</td>
</tr>
<tr>
<td>15.4</td>
<td>Dealing with the Media</td>
<td>237</td>
</tr>
<tr>
<td>16</td>
<td>Incident Reporting and Analysis</td>
<td>239</td>
</tr>
<tr>
<td>16.1</td>
<td>Crucial Good Practice</td>
<td>240</td>
</tr>
<tr>
<td>16.2</td>
<td>Incident Reporting, Inquiry and Analysis</td>
<td>240</td>
</tr>
<tr>
<td>16.3</td>
<td>What is an ‘Incident’?</td>
<td>245</td>
</tr>
<tr>
<td>16.4</td>
<td>Interagency Collaboration on Security Information</td>
<td>245</td>
</tr>
<tr>
<td>17</td>
<td>Telecommunications</td>
<td>251</td>
</tr>
<tr>
<td>17.1</td>
<td>Telecoms and Security</td>
<td>252</td>
</tr>
<tr>
<td>17.2</td>
<td>Choosing Telecoms: Cost and Performance Criteria</td>
<td>252</td>
</tr>
<tr>
<td>17.3</td>
<td>Choosing Telecoms: Contextual Criteria</td>
<td>257</td>
</tr>
<tr>
<td>17.4</td>
<td>Operating Radios</td>
<td>261</td>
</tr>
<tr>
<td>17.5</td>
<td>Operational Discipline</td>
<td>263</td>
</tr>
<tr>
<td>17.6</td>
<td>Preparation and Training</td>
<td>265</td>
</tr>
</tbody>
</table>
### PART VI PERSONAL AND PERSONNEL DIMENSIONS OF SECURITY MANAGEMENT

18. Personal and Team Competence  
18.1 The Relevance for Security  
18.2 Personal Competence  
18.3 Team Competence  
18.4 Preparation and Training

19. Managing Stress  
19.1 The Relevance for Security  
19.2 Who is Affected by Stress  
19.3 Types of Stress  
19.4 Symptoms of Negative Stress  
19.5 Contributory Factors  
19.6 Managing Stress  
19.7 Cultural and Situational Experiences of Stress and Stress Management

20. Staffing and Personnel Management  
20.1 Differential Risks  
20.2 Staff: The Source of Problems, the Source of Solutions  
20.3 International Staff Issues  
20.4 National Staff Issues  
20.5 Gender Dimensions in Security Management  
20.6 Organisational and Individual Responsibilities

---

### PART VII SECURITY MANAGEMENT

21.1 How Appropriate and Effective is your Security Plan?  
21.2 Organisational Responsibility  
21.3 Security Planning and Documentation  
21.4 Security Management  
21.5 Maintaining Alertness, Discipline and Effectiveness

22. Security Management and the Authorities  
22.1 The Responsibility of State Authorities  
22.2 A Sensitive Relationship  
22.3 Complex Scenarios

---

### AN EXNES

Annex 1 Trends in Aid Agency Security Risks  
Annex 2 The Legal Protection of Aid Workers  
Annex 3 The UN Security Management System  
Annex 4 Who is Responsible for Security at Field Level?  
Annex 5 Private Security Companies  
Annex 6 Insurance Cover
Disclaimer

Security management is about reducing risk. It does not offer any guarantee that incidents will not occur. It is also about contextual adaptation and situational judgement. This Good Practice Review offers guidance of a general nature and does not cover all situations. The appropriateness of a specific measure will often depend on the context, and in some situations following the tips and guidelines mentioned here may not be the best course of action and could actually increase the risk. The author, the Humanitarian Practice Network and the Overseas Development Institute decline responsibility for incidents, and for loss of assets or injury or death.

Several case examples refer to specific countries and actors. They are invariably simplified and often no longer ‘current’. Their purpose is to illustrate a point. They should not be taken as an adequate or currently valid statement about threat patterns in a particular country or as a statement about the security management of one or more agencies.

Glossary

Acceptance strategy: the attempt to remove the threat or have local actors control the threat on your behalf by getting their more or less formal consent and acceptance for your presence and your work.

Battlefield survival: measures to lessen the risk of death or injury when under fire, or in an area which is under fire from any sort of weapon.

Booby trap: an improvised or custom-made explosive usually attached to or concealed under ordinary objects that acts as a mine to deter or harm people approaching the booby trap area.

Car-jacking: the stealing of a car at gun-point, ie, while the driver is in the car.

Communications tree: an arrangement to spread information rapidly such as a security alert, whereby one person/agency informs eg, three others, who each in turn then inform three pre-identified others, and so on.

Compound mentality: a tendency of aid agencies, and especially their international staff, to discuss and analyse their environment among themselves with little reference to or interaction with non-aid actors in that environment.

Counter-surveillance: watching whether you are being watched and studied by people with malicious intent, here used in the context of a threat of kidnapping or armed robbery.

Critical incident: a security incident in which life was threatened and which led to an experience of mortal danger; either of the aid worker, or of someone emotionally dear or physically close to him/her.

Danger habituation: a usually unconscious adjustment of one's threshold of acceptable risk resulting from constant exposure to danger; the result is a reduction of one's objective assessment of risk, leading possibly to increased risk-taking behaviour.

Deterrence strategy: a strategy to try and deter someone from posing or effecting a threat against you by posing a counter-threat, in its most extreme form through the use of armed protection.

Evacuation: the withdrawal of staff across an international border.
Hibernation: choosing, or being forced to stay, in the middle of a crisis and danger zone often because evacuation could not yet/no longer be effected.

Incident analysis: deeper and more critical inquiry into the structural and contextual factors that allowed a security incident to happen; questioning the effectiveness of the various dimensions and steps in the security management, and asking whether or to what degree the agency or one or more of its staff members could have been perceived to be "provoking" anger or aggression.

Incident inquiry: the collection of situational and circumstantial information about an incident that took place beyond the basic facts stated in the incident report.

Incident mapping: the visualisation, usually on a map but potentially also in a timeframe, of when and where and what type of incidents happened in an attempt to find patterns and identify high-risk areas and high-risk times.

Incident survival: what was done and/or avoided by those caught up in a security incident to minimise the harm that could be done to them.

Neighbourhood watch: a more or less formalised scheme among neighbours to keep an eye open for suspicious people and crime.

Personal sense of security: a subjective and therefore potentially misleading form of threat and risk assessment relying on one's personal impressions of a situation.

Post-traumatic stress disorder (PTSD): a psychological condition that may affect people who have suffered severe emotional trauma, and may cause sleep disturbances, flashbacks, anxiety, tiredness and depression.

Prodding: a key technique used in extraction from a (suspected) minefield whereby the soil is very carefully examined for possible mines before a foot is set on it.

Protection: used here as distinct from 'safety' and 'security' to refer to the 'protection' of civilians and non-combatants who are not aid agency staff.

Protection strategy: the use of protective procedures and devices to reduce your vulnerability; the strategy does not affect the level of threat.

Risk assessment/analysis: an attempt to consider risk more systematically in terms of the threats in your environment, your particular vulnerabilities, and your security measures to reduce the threat and/or reduce your vulnerability.

Risk reduction: the purpose of your security management, by reducing the threat and/or reducing your vulnerability.

Rules of engagement: guidelines to soldiers or armed guards regarding the conditions under which they can use force, and stipulating how much force may be used.

Safety: used here as distinct from 'protection' and 'security' to refer to 'accidents' caused by nature (e.g., avalanche) or non-violent circumstances (e.g., fire, road accidents) and to illness, injury and death resulting from medical conditions not brought about by violence, or due to lax safety guidelines and procedures in the workplace.

Scenario thinking: thinking 'forward' about how the situation may evolve in the near and medium-term future, and how the threats in your environment might develop; reviewing the assumptions in your plans and thinking about what you would do if they do not hold.

Security: used here to indicate the protection of aid personnel and aid agency assets from violence.

Security (alert) phases: a summary classification of various possible levels of risk and insecurity in your environment, each of which requires a specific set of mandatory security procedures.

Security strategies: used here to describe the three ideal-type strategies of acceptance, protection and deterrence.

Social reference: a recommendation or personal 'guarantee' about a potential recruit from someone who has not necessarily had any professional involvement with the recruit but knows his/her standing and reputation within a community.

Standard operating procedures: formally established procedures for carrying out particular operations or dealing with particular situations, here specifically to prevent an incident happening, to survive an incident, or to follow as part of the agency's incident/crisis management.
Terrain awareness: being attentive to the physical and social environment in which you are moving, where potential dangers may come from, and where you might find help or cover.

Threat: a danger in your operating environment.

Threat assessment/analysis: the attempt to examine more systematically the nature, origin, frequency and geographical concentration of threats.

Threat mapping: visualising and illustrating threats on a geographical map.

Threshold of acceptable risk: the point beyond which you consider the risk too high to continue operating so that you must withdraw yourself from the danger zone; influenced by the probability that an incident will occur, and the seriousness of the impact if it occurs.

Triangulation: cross-checking information or details by comparing the opinion or version from different sources.

Tripwire: a wire connected to the fuse of a mine or a booby trap; touching, cutting or displacing it will detonate the explosive.

Unacceptable risk: an assessment that even your security measures are not able to sufficiently reduce the likelihood and/or the impact of an incident occurring, to justify continued operations and exposure to the threat.

Unexploded ordnance (UXO): any type of munition (bullet, hand grenade, mortar shell, etc) that has been fused (prepared for firing) but not used, or that has been fired but has not gone off and is considered unstable and dangerous.

Warden/warden system: one or more focal points for security with typically a responsibility for a set of people in a defined geographical area; the warden is an important node in the communications tree and will also ensure that all those under his/her responsibility follow agreed security procedures.

Dedication

This Good Practice Review is dedicated to Smruti and Medinah, lifelong friends through security.

Acknowledgements

The list of people who one way or another have contributed to this GPR is very long. Among them special mention should be made of Lucy Brown, Jan Davis, Philippe Dind, Jonathan Dworken, David Dyck, Rob Lowe, Michael O’Neill and Lisa Schirsch, with whom I had the immense pleasure of developing and pilot testing a training curriculum on operational security management. The role of Jane Swan, who brought us together and transformed us into a ‘well-bonded’ and effective team, was crucial. Others who need mentioning include Mark Bowden, Nan Buzard, Bob Churcher, Kateri Clement, John Cosgrave, Jean Philippe Debus, Veronique de Geoffroy, Jayne Docherty, Enrique Eguren, Sue Emmott, John Fawcett, Pierre Gallien, Max Glaser, Sean Greenaway, Francois Grunewald, Andy Harris, Melissa Himes, Chris Horwood, Bernard Jacquemart, Tajma Kurt, Toby Lanzer, Nick Leader, John Logan, Sarah Longford, Richard Manlove, Randy Martin, Rae McGrath, Paul Meijis, Anita Menghetti, Jonathan Napier, Sydila Nelo, Nick Nobbs, Annemarie O’Reilly, Smruti Patel, Mike Penrose, Noël Philip, Eric Pitois, Marc Powe, Steve Penny, Moira Reddick, George Sommerwill, Arne Strand, Eric Westdorp and Jim White. I thank all of them for their input and for their patience while I was pestering them for documents or feedback. In addition, case studies and feedback from participants and resource people in several training and workshops in the US, the UK and France and in Albania, Kosovo and Indonesia, and from students at the universities of Geneva, York and Oxford Brookes, were invariably useful. I hope the participants in the workshops got as much out of them as I did as a co-facilitator. The merits of this Good Practice Review I share with them, the weaknesses and mistakes are mine. Finally I need to mention my first ‘mentors’ in appropriate security management; Philippe, Etebori and Ehsan in Afghanistan, and Mohammed Hussain, Mohammed Jibreel, Daher and Abebaw Zelleke in the Ethiopian Ogaden. Their advice in critical situations often proved invaluable.

Special thanks are due to Rachel Houghton for the challenging task of editing this GPR, to Margaret Cornell for assistance with copy-editing, and to Olivia Cheasty for patiently making on-screen changes. Also to Rebecca Lovelace for her tremendous assistance in preparing the document for publication, and to the team at DS Print & Redesign.

Invitation

This GPR should be regarded as ‘work-in-progress’. Feedback, comments and additional case material to make further editions and training more complete, relevant and appropriate are therefore very welcome.