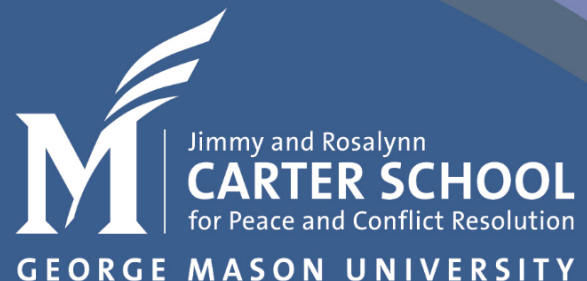


# **Risks, Dangers, and Threat Models: Evaluating Security Analysis for Conflict Practitioners**

AUGUST 2021

**Prepared by Dr. Michael Loadenthal,  
with contributions from  
Peyton Nielsen and Devin McCarthy**

**Better Evidence Project**  
*Center for Peacemaking  
Practice*



# Table of Contents

<b>Executive Summary .....</b>	<b>4</b>
<b>Guiding Security Principles for Practitioners .....</b>	<b>5</b>
<b>Introduction .....</b>	<b>6</b>
Why Should Peacemakers Care About Security? .....	6
<b>Stage 1: Understanding Security, Risk, and Threat.....</b>	<b>7</b>
Establishing ‘Security’ as Human Security .....	7
Security for Whom? .....	9
Threat Modeling Best Practices .....	10
Threat Modeling as Harm Reduction.....	12
Threat Modeling as Intersectional .....	13
Frameworks Not Prescriptions.....	15
A Risk-Centric Threat Modeling Approach.....	16
Weaknesses, Vulnerabilities, Exploits, and Risks .....	16
Threat Typologies, Motives, and Archetypes .....	18
Developing Risk Management Strategies .....	21
<b>Stage 2: Surveying the Field at Large.....</b>	<b>25</b>
Surveying Academics: Contemporary literature .....	25
Background Literature .....	25
Recent Trend Literature .....	27
Current Security Strategies and Policy Literature .....	28
Recommendations from the Literature.....	29
Further Research and Literature Limitations .....	30
Surveying Practitioners: Educational-Training Materials.....	32
Research Design.....	32
Methodology .....	33
Findings.....	35
Comparing Our Findings .....	36
<b>Future Directions .....</b>	<b>37</b>
<b>Conclusion .....</b>	<b>38</b>
<b>Appendices.....</b>	<b>39</b>
Appendix 1: ‘Threat to journalist’ continuum (NYT) .....	39
Appendix 2: Risk, Danger, and Threat Mind Map for Conflict Practitioners (Loadenthal) .....	40
Appendix 3: Initial Respondent Pool .....	41
Appendix 4: Field Survey Results .....	42
Appendix 5: Guides, Reports, and Educational Training Materials Reviewed .....	43

<b>Appendix 6: Complete Coding Table for Responsive Organizations .....</b>	<b>45</b>
<b>Appendix 7: Findings Table Restricted to Responsive Organizations .....</b>	<b>47</b>
<b>Appendix 8: Research Brief #1 .....</b>	<b>48</b>
<b>Appendix 9: Research Brief #2 .....</b>	<b>50</b>
<b>Appendix 10: Research Brief #3 .....</b>	<b>53</b>
<b>Appendix 11: Research Brief #4 .....</b>	<b>55</b>
<b>Appendix 12: Research Brief #5 .....</b>	<b>57</b>
<b>Appendix 13: Threat Modeling Worksheet (EFF) .....</b>	<b>59</b>
<b><i>Acknowledgements .....</i></b>	<b>63</b>
<b><i>Notes on contributors .....</i></b>	<b>63</b>
<b><i>References.....</i></b>	<b>64</b>

## Executive Summary

The risks to conflict practitioners, peacemakers, humanitarian aid workers, and others serving 'in the field' are diverse, deeply contextual, and ever-changing. While ample literature exists focused around documenting and evaluating the history of these dangers, far fewer resources have been authored to promote a comprehensive, proactive, and agile framework for predicting, observing, and understanding risks and threats to one's safety and security. While it is true that many organizations provide their employees with carefully-written guides containing security 'dos and don'ts,' what are practitioners meant to do when the conditions on the ground change? Instead of providing fixed solutions to emergent problems, this paper argues for a flexible framework to understand security and risk, and as a result, facilitates the development of a sustained, adaptable security posture and risk balance.

The first portion of the paper draws upon a broad review of the relevant research in Critical Security Studies, threat assessment, risk management, and threat modeling to offer guidance to conflict practitioners, with the aim of building an understanding of relevant threats, methods of analysis, and means of mitigation. This engagement explores broad frameworks for understanding security, risk, and threat, as well as contextualizing and situating the role of (technical) threat modeling within a conflict practitioner's agenda. The themes of interdependent, intersectional conflict, as well as the contributions of the harm reduction framework is central to this approach. Building on these themes, this paper embraces a risk and attack-centric, proactive approach to security including a focus on threat types and attacker motives. The goal of this portion is not to tell practitioners *what* to protect against, but rather to teach them *how* to think in security terms, and in doing so, make each individual the best active architect of their own security.

In the second portion of the paper, through a broad survey of contemporary academic and practitioner literature, we assess the present state of the field's readiness to mitigate insecurity and risk. This is accomplished through two pursuits: a formal review of the current academic literature and a systematic review of existing educational-training resources provided to practitioners by their employers, measured through a multi-variable qualitative coding schema. This literature review, in combination with the assessment of educational-training materials, provides a clear picture of the 'state of the field' in terms of both scholars and practitioners.

While this paper has begun the inquiry into these key areas of danger for our field, this is not the end but rather a starting point. Beyond this investigation, this study will be continued into the future through a practitioner-focused working group made up of engaged scholars. This working group will be the first set of individuals invited to review this paper, and their engagement will help to shape and guide the next stages, as led by the Better Evidence Project. Since the Better Evidence Project is chiefly focused on providing evidence-based guidance to make peacemaking efforts more effective, facilitating the increased safety of those engaged on the ground is a necessary early step, and essential for long-term, sustained deployments.

**Keywords:** security; safety; risk; conflict practitioners; threat modeling; risk analysis

## Guiding Security Principles for Practitioners

1. Rather than teach practitioners special means of protecting themselves (e.g., device hardening, defensive driving), organizations should aim to teach reasoned, analytical thinking, focused on threat mapping and risk mitigation, so that individuals can be active agents in establishing their personal and organizational security postures.
2. Security should be planned for *prior* to a practitioners' deployment, at the 'design' stage, and *not* understood as a burdensome feature to be added in at the end.
3. Practitioners should engage routinely with the formal practice of threat modeling and risk analysis, guided by leaders in the field<sup>1</sup>, and following the example of communities engaged in digital security.
4. Security management plans should aim to *mitigate* risks while also acknowledging their ever-presence and unavoidable nature (i.e., harm reduction approach).
5. Planning for security must take into account situational contexts, local realities, the individual positionalities and identities of practitioners, and the inherently intersectional nature of threat environments and attack vectors.
6. Any analysis, prediction, and planning should be understood as *temporary*—a snapshot in time—and as such, security planning should prioritize those approaches which are agile, adaptable, and suited to persistent refinement and adaptation.
7. Digital operational security (e.g., secure communications, anti/counter-surveillance) must feature as a central comment of any skills-based training, with the acknowledgement that any specific mitigations and technological solutions are temporary fixes in an ever-present, ongoing, electronic arms race.
8. A standardized set of tools can help form the basis of a first stage analysis to be used in identifying risks, dangers, and insecurities. Such a toolkit should include standard approaches (e.g., mind maps, SWOT analyses, risk matrices), as well as more closely-tailored tools, such as those driven by user archetype, motive, and capability assessment.

---

<sup>1</sup> For example, begin with: Electronic Frontier Foundation, "Threat Modeling," 2020, <https://ssd.eff.org/>; Electronic Frontier Foundation, "Your Security Plan," Surveillance Self-Defense, February 2, 2021, <https://ssd.eff.org/en/module/your-security-plan>.

## Introduction

Existing literature provides ample evidence of the physical and psychological dangers faced by those working in conflict, post-conflict, and disaster environments.<sup>2</sup> Despite the richness of these materials, many of these valuable insights do not aim to offer solutions. Although the risks, dangers, and threats facing practitioners are understood, this literature often lacks proposals for comprehensive, proactive, and agile-adaptive frameworks for predicting, observing, and understanding threats to safety and security. The growth in literature focused on the risks facing conflict practitioners (especially humanitarian aid workers) has not translated to focused attention towards *preventing* violence, as such research remains scant.<sup>3</sup>

The following paper draws on a broad review of relevant research to offer guidance to practitioners and policy makers to identify and mitigate the threats they face, and to provide a framework to help routinize that process. This paper will proceed in two distinct stages. In the first stage we will review foundational concepts in security theory, risk assessment, and management, as well as threat modeling. In the second stage, we will take stock of our field, both in terms of how practitioner organizations are preparing individuals in the field, as well as the broader state of the academic discourse on the topic.

## Why Should Peacemakers Care About Security?

It is instructive to begin with the question above, namely, ‘Why should peacemakers care about security?’ Depending on your individual positionality and work setting, in conjunction with other identity-based and environmental factors, it may be more or less apparent why this is a relevant topic. For many of us deployed in the field, we are well-versed in the litany of insecurities we may encounter—from those seeking to abduct our colleagues (e.g., armed political groups), to those who may wish to interject disruption into our inter-agency communications (e.g., hackers). Regardless of the nature of the threat, from the annoying to the lethal, we all need to consider security in our planning.

For those engaged in peacemaking, there are several key reasons why this knowledge is essential, and how security is a precursor to effective engagement. In general, one needs to feel secure to be effective. This understanding is a foundational basis of human needs theory used throughout Conflict Analysis,<sup>4</sup> and can be extended to the broader theory of self-actualization

---

<sup>2</sup> For example, see: Dennis King, “Chronology of Humanitarian Aid Workers Killed in 1997–2001” (Geneva: UN Office for the Coordination of Humanitarian Affairs, January 15, 2002), <http://reliefweb.int/symposium/NewChron1997-2001.html>; Elizabeth A. Rowley, Byron L. Crape, and Gilbert M. Burnham, “Violence-Related Mortality and Morbidity of Humanitarian Workers,” *American Journal of Disaster Medicine* 3, no. 1 (February 2008): 39–45; Abby Stoddard, Adele Harmer, and Victoria DiDomenico, “Providing Aid in Insecure Environments: 2009 Update” (London, UK: Humanitarian Outcomes, April 2009), <https://www.humanitarianoutcomes.org/publications/providing-aid-insecure-environments-2009-update>; Victoria Metcalfe, Ellen Martin, and Sara Pantuliano, “Risk in Humanitarian Action: Towards a Common Approach?” (Denmark: Ministry of Foreign Affairs, November 2010), [https://www.who.int/hac/techguidance/tools/risk\\_in\\_humanitarian\\_action.pdf](https://www.who.int/hac/techguidance/tools/risk_in_humanitarian_action.pdf); Larissa A. Fast, “Mind the Gap: Documenting and Explaining Violence Against Aid Workers,” *European Journal of International Relations* 16, no. 3 (September 1, 2010): 365–89.

<sup>3</sup> Larissa Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*, Pennsylvania Studies in Human Rights (Philadelphia, PA: University of Pennsylvania Press, 2014), 1.

<sup>4</sup> John W. Burton, *Conflict: Human Needs Theory* (New York, NY: St. Martin’s Press, 1990).

popularized by the psychologist Abraham Maslow and his hierarchy of psycho-social needs. Individuals can not engage in their work effectively if they feel at risk, in danger, or otherwise unable to provide their own basic security. The goal of the Better Evidence Project is to make peacemaking more effective, and in this manner, security should be understood as a paramount, prerequisite feature. The paper that follows seeks to first promote this security by providing insights into how we understand it, and in the second stage, evaluate how widespread such an approach is within the academic and practitioner-based communities we are emersed within.

## Stage 1: Understanding Security, Risk, and Threat

While traditional threat modeling frameworks are designed to secure *digital* systems,<sup>5</sup> these same principles can be applied to conflict practitioners. The goal of promoting frameworks for practitioners is to encourage proactive thinking in regards to safety and security. The carpenter's motto of 'measure twice, cut once' should be applied when designing engagements by practitioners, especially considering that much of our work occurs in precarious, hostile, or otherwise dangerous environments, and with a catalogue of opponents, malicious actors, and uncertainty.

In establishing a community of stakeholders in this exploration, it should be noted that throughout this paper, the use of terms such as "practitioner/conflict practitioner," "aid worker," "human rights activist/defender," "peace worker," "organizational staff," etc. should be understood as imprecise labels *not* meant to draw meaningful operational distinctions. The varied use of terminology is meant to encourage wide adoption. These terms are used interchangeably and in doing so, seek to encompass individuals working in a paid or volunteer capacity, in areas and communities experiencing conflict, post-conflict, disaster, and other forms of instability. While many readers will likely evoke images of Afghanistan, Somalia, Chechnya, Darfur, Syria, the Gaza Strip, and other 'hot' conflict zones, situational awareness as it pertains to safety and security can apply to any environment, foreign or domestic (including digital spaces and communities<sup>6</sup>), whether experiencing active violence or not.

## Establishing 'Security' as Human Security

The increasingly militarized and securitized manner through which conflict-centered work is carried out serves to frame interventions as elements of national security, and the subject matter experts, as military commanders.<sup>7</sup> This trend is troubling for those seeking to *transform*

---

<sup>5</sup> For example, see: Adam Shostack, *Threat Modeling: Designing for Security*, 1st edition (Indianapolis, IN: Wiley, 2014); Brook S.E. Schoenfield, *Securing Systems: Applied Security Architecture and Threat Models* (Boca Raton, FL: CRC Press/Taylor & Francis, 2015); Tony UcedaVelez and Marco M. Morana, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis* (Hoboken, New Jersey: Wiley, 2015); Izar Tarandach and Matthew J. Coles, *Threat Modeling: A Practical Guide for Development Teams*, 1st edition (Sebastopol, CA: O'Reilly Media, 2020).

<sup>6</sup> Monica J Barratt and Alexia Maddox, "Active Engagement with Stigmatised Communities through Digital Ethnography," *Qualitative Research* 16, no. 6 (December 1, 2016): 701–19; Maura Conway, "Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines," *Terrorism and Political Violence* 33, no. 2 (February 17, 2021): 367–80.

<sup>7</sup> Fast, 120–21, 175–76.

violence conflicts and not simply end them (i.e., foster a negative peace<sup>8</sup>) and creates additional challenges for conflict workers. Although often thought of in terms of military might, physical safety, or avoiding violence, what actually constitutes *security* is a contested term as demonstrated by a host of scholars in *Critical Security Studies*<sup>9</sup> and related areas including *Feminist Security Studies*.<sup>10</sup> Others security theorists have sought to ‘widen sectors’<sup>11</sup> of the security foci, challenging a military-state fixation for the multi-leveled.<sup>12</sup> Many of these thinkers seek to de-center the state—its militaries, borders, functionaries, and capital—as the focus of security,<sup>13</sup> and instead advocate for an embedded notion, which seeks to provide for *human security*,<sup>14</sup> *environmental security*,<sup>15</sup> and other approaches which center the community’s needs while recognizing the inherent power imbalance. Security throughout the present paper points to *human security*, not the security of the institution, its host nation-state, or its technocrats, and employees.

---

<sup>8</sup> Johan Galtung, “An Editorial,” *Journal of Peace Research* 1, no. 1 (March 1, 1964): 2.

<sup>9</sup> For example, see: Ronald Paris, “Human Security: Paradigm Shift or Hot Air?,” *International Security* 26, no. 2 (2001): 87–102; Ken Booth, ed., *Critical Security Studies And World Politics* (Boulder, CO: Lynne Rienner Pub, 2005); Peoples and Vaughan-Williams, *Critical Security Studies*; Mark B. Salter and Can E. Mutlu, eds., *Research Methods in Critical Security Studies: An Introduction* (New York, NY: Routledge, 2012); Laura J. Shepherd, ed., *Critical Approaches to Security: An Introduction to Theories and Methods* (New York, NY: Routledge, 2013).

<sup>10</sup> For example, see: Wibben, *Feminist Security Studies*; Wendy Stokes, “Feminist Security Studies,” in *International Security Studies: Theory and Practice*, ed. Peter Hough et al. (London, UK: Routledge, 2015), 44–56; Annick T. R. Wibben, ed., *Researching War: Feminist Methods, Ethics and Politics* (New York, NY: Routledge, 2016).

<sup>11</sup> Buzan, Waever, and de Wilde, *Security: A New Framework for Analysis*.

<sup>12</sup> For example, see: Richard Ullman, “Redefining Security,” *International Security* 8, no. 1 (1983): 129–53; Joseph S. Nye Jr. and Sean M. Lynn-Jones, “International Security Studies,” *International Security* 12, no. 4 (1988): 5–27; Jessica Tuchman Matthews, “Redefining Security,” *Foreign Affairs* 68, no. 2 (1989): 162–77; Helga Haftendorn, “The Security Puzzle: Theory-Building and Discipline Building in International Security,” *International Studies Quarterly* 35, no. 1 (1991): 3–17; Neta C. Crawford, “Once and Future Security Studies,” *Security Studies* 1, no. 2 (1991): 283–316; J. Ann Tickner, *Gender in International Relations: Feminist Perspectives on Achieving Global Security* (New York, NY: Columbia University Press, 1992); Ken Booth, *Theory of World Security* (Cambridge, UK: Cambridge University Press, 2008).

<sup>13</sup> Lee Jarvis and Jack Holland, *Security: A Critical Introduction* (London, UK: Palgrave Macmillan, 2015), 98–104.

<sup>14</sup> Mary Kaldor, *Human Security* (Oxford, UK: Polity, 2007); Shahrbanou Tadjbakhsh and Anuradha Chenoy, *Human Security: Concepts and Implications* (New York, NY: Routledge, 2007); Marc G. Doucet and Miguel de Larrinaga, “Human Security and the Securing of Human Life: Tracing Global Sovereign and Biopolitical Rule,” in *Critical Perspectives on Human Security: Rethinking Emancipation and Power in International Relations*, ed. David Chandler and Nik Hynek (New York, NY: Routledge, 2012), 129–43.

<sup>15</sup> For example, see: Jessica Tuchman Matthews, “Redefining Security,” *Foreign Affairs* 68, no. 2 (Spring 1989): 162–77; Simon Dalby, “Climate Change and Environmental Security,” in *Security Studies: An Introduction*, ed. Paul D. Williams, 2nd edition (London ; New York: Routledge, 2012), 311–23; Peter Hough, “Environmental Security,” in *International Security Studies: Theory and Practice*, by Peter Hough et al. (New York, NY: Routledge, 2015), 211–24; J. Jackson Ewing, “Environmental Security,” in *An Introduction to Non-Traditional Security Studies: A Transnational Approach*, ed. Mely Caballero-Anthon (Los Angeles, CA: SAGE Publications Ltd, 2016), 95–113; Marcus Dubois King, “Water Security,” in *An Introduction to Non-Traditional Security Studies: A Transnational Approach*, ed. Mely Caballero-Anthon (Los Angeles, CA: SAGE Publications Ltd, 2016), 154–73.



The introduction of a *human-centered* security discourse is often historicized within the 1994 UN Development Program's Human Development Report which began the shift away from state centrism.<sup>16</sup> As the authors of the report write:

The concept of security has for too long been interpreted narrowly: as security of territory from external aggression, or as protection of national interests in foreign policy or as global security...It has been related more to nation-states than to people...Forgotten were the legitimate concerns of ordinary people who sought security in their daily lives. For many of them, security symbolized protection from the threat of disease, hunger, unemployment, crime, social conflict, political repression and environmental hazards.<sup>17</sup>

This focus on the human seeks to return *agency* to the securitized subject and challenge the state/security conflation.<sup>18</sup> The so-called *critical* turn in Security Studies<sup>19</sup> seeks to refocus and uplift individuals' experience and situational knowledge;<sup>20</sup> and approach which is foundational for on-the-ground practitioners developing *their* security posture through a review of prior institutional memory and its history of *insecurity*. Existential threats presented by climate change, health pandemics, mass migration, civil unrest, etc. will impact both state and the non-state, as they do not acknowledge national borders, ethnic divisions, employment status, and other human-created distinctions.

### Security for Whom?

If individuals can agree on the general *lack of* security in diverse locales, certainly many fail to agree on a definition of what constitutes a safe and secure environment. The US government for example, offers the following definition, authored by the US Institute for Peace:

A safe and secure environment is one in which the population has the freedom to pursue daily activities without fear of politically motivated, persistent, or large-scale violence. Such an environment is characterized by an end to large-scale fighting; an adequate level of public order; the subordination of accountable security forces to legitimate state authority; the protection of key individuals, communities, sites, and infrastructure; and the freedom for people and goods to move about the country and across borders without fear of undue harm to life and limb.<sup>21</sup>

---

<sup>16</sup> "Human Development Report 1994" (New York, NY: United Nations Development Programme, 1994), chap. 2, [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf).

<sup>17</sup> "Human Development Report 1994," 22.

<sup>18</sup> Jarvis and Holland, *Security: A Critical Introduction*, 100, 104.

<sup>19</sup> For example, see: Booth, *Critical Security Studies And World Politics*; Peoples and Vaughan-Williams, *Critical Security Studies*; Salter and Mutlu, *Research Methods in Critical Security Studies*; Jarvis and Holland, *Security: A Critical Introduction*; Mely Caballero-Anthon, ed., *An Introduction to Non-Traditional Security Studies: A Transnational Approach* (Los Angeles, CA: SAGE Publications Ltd, 2016).

<sup>20</sup> Jarvis and Holland, *Security: A Critical Introduction*, 107.

<sup>21</sup> United States Institute of Peace, "Guiding Principles for Stabilization and Reconstruction: Safe and Secure Environment," United States Institute of Peace, n.d., sec. 6.0, <https://www.usip.org/guiding-principles-stabilization-and-reconstruction-the-web-version/safe-and-secure-environment>.

Although overly ambitious, this “safe and secure environment...which the population has the freedom to pursue daily activities” is precisely the goal at hand. While the daily activities may be observing, intervening, transforming, and ending conflict, the goal for functional security remains the same.

The above definition maintains that security is to be established by those holding a state-mandated monopoly on violence<sup>22</sup> (i.e., “the subordination of accountable security forces to legitimate state authority”), which appears in conflict with a non-state-centric notion of human security. This is especially true for practitioners working in locales wherein their goals exist at odds with those of the nation-state where they reside. For example, an international volunteer engaging in protective accompaniment in the Occupied Palestinian Territories would not likely be able to rely on Israeli military authorities to provide for their safety and security, nor could the Palestinian security forces (e.g., Preventative Security Service) or militias (e.g., the Al Aqsa Martyrs Brigade) provide such comprehensive protections. In order for field-based practitioners to place their faith in their host organization, they must assume that the organization can do a better job of security than the individual can achieve on their own.<sup>23</sup>

### Threat Modeling Best Practices

In developing a security posture, this paper builds upon the approach commonly referred to as *threat modeling*, a methodology constructed around three central questions,<sup>24</sup> recurrent through the literature, namely:

1. What am I trying to protect?
2. What do I need to protect against?
3. How much time, effort, money, decreased functionality, additional steps, etc. am I willing to expend to obtain adequate protections?

Using these guiding questions, individuals and organizations can begin understating their security environment, and establishing a framework for what to protect, how, and to what end. Threat modeling can help practitioners understand local risks and dangers, and like other security thinking, should “derive from a sound analysis of the context, vulnerabilities, threat levels...[and] risk threshold.”<sup>25</sup> To help this process, practitioner-focused organizations have developed threat modeling aids, including a ‘personal threat model help desk’ maintained by

---

<sup>22</sup> Max Weber, “Politik als Beruf (Politics as a Vocation)” (Lecture, Free Students Union, Munich University, January 1919), [http://www.ne.jp/asahi/moriyuki/abukuma/weber/lecture/politics\\_vocation.html](http://www.ne.jp/asahi/moriyuki/abukuma/weber/lecture/politics_vocation.html).

<sup>23</sup> Eleanor Gordon, *Conflict, Security and Justice: Practice and Challenges in Peacebuilding* (London, UK: Macmillan International/Red Globe Press, 2019), 43.

<sup>24</sup> As adapted from: Simson Garfinkel and Gene Spafford, *Practical Unix & Internet Security, 3rd Edition*, 2nd edition (Sebastopol, CA: O’Reilly Media, 1996), 27.

<sup>25</sup> Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*, 173.

Reporters Without Borders<sup>26</sup>, and numerous platforms for digital modeling including those maintained by digitally-focused organizations such as OWASP<sup>27</sup> and Irius Risk,<sup>28</sup> both of whom offer free, online threat modeling platforms. There are also preexisting learning aids which are well-suited for practitioners seeking to engage with threat modeling.<sup>29</sup> An example of such a learning aid, developed by the Electronic Frontier Foundation, is included as the final appendix to this paper.

The threat modeling questions above serve to help us determine what to focus on, and can be used to identify assets, threats, and risks, and develop appropriate measures to respond. These factors are enumerated in the table below:

*Table: Assets, Threats, and Risks*

<b>Assets</b>	Staff, property, vehicles, staff credentials, brand reputation, client goodwill, money and other financial instruments, protected intellectual property (i.e., data), other organizational resources
<b>Threats</b>	Criminal organizations, unorganized opportunistic criminals, rival nation-states, non-state armed actors, militia
<b>Risks</b>	Injury to staff, death of staff, kidnapping/abduction, disease, theft, disruption of services...

Threat modeling is a continually-reflective process wherein findings are reintegrated and subsequently reevaluated on an ongoing and near-constant basis. As practices, laws, political landscapes, and attackers' capabilities change, so do our models and the mitigation strategies they lead us towards. This continuous process—as opposed to a one time or interval-paced approach—allows us to develop models of increasing accuracy, and with growing utility for the end user. Unfortunately, this also means that observations, determinations, and conclusions established are temporary, likely to change, and serve as a basis for analysis and adaptation, and not permanent realities.

In 2020, a group of leading thinkers focused on technical threat modeling collaboratively authored the Threat Modeling Manifesto<sup>30</sup>, which laid out guidelines for the approach. In this key text, the authors note:

<sup>26</sup> Reporters Without Borders, “Training: Your Threat Model,” Helpdesk - Digital Security for Journalists, 2021, <https://helpdesk.rsf.org/training/your-threat-model/>.

<sup>27</sup> OWASP, “OWASP Threat Dragon,” 2021, <https://threatdragon.org/login>.

<sup>28</sup> IriusRisk, “IriusRisk Threat Modeling Platform: Community Edition,” 2021, <https://community.iriusrisk.com/ui#!login>.

<sup>29</sup> For example, see: MobLab, “Stay Safe out There: Threat Modeling for Campaigners,” MobLab, August 12, 2015, <https://mobilisationlab.org/stories/threat-modeling-for-campaigners-and-activists/>; Kit O’Connell, “Threat Modeling For Activists: Tips For Secure Organizing & Activism,” *Kit O’Connell: Approximately 8,000 Words* (blog), October 22, 2018, <https://kitoconnell.com/2018/10/22/threat-modeling/>; Daniel Moßbrucker, “Threat Modeling Guide: How to Identify Digital Risks in International Development Projects” (Berlin, Germany: Akademie/German Federal Ministry for Economic Cooperation and Development, September 2020), [https://akademie.dw.com/docs/Handbook\\_Threat\\_Modeling\\_Guide.pdf](https://akademie.dw.com/docs/Handbook_Threat_Modeling_Guide.pdf); Electronic Frontier Foundation, “Your Security Plan.”

<sup>30</sup> Zoe Braiterman et al., “Threat Modeling Manifesto” (Threat Modeling Manifesto Working Group, November 17, 2020), <https://www.threatmodelingmanifesto.org/>.

1. Threat modeling should *not* be done by a sole individual working in isolation (i.e., the hero threat modeler), nor does its success depend on that individual's abilities or mindset. Instead, the modeling process must be collaborative, community-led, interactive, and involve a variety of individuals working at all levels of the project.
2. Threat modeling should *not* over focus on the minutia, but maintain a broad, wide eyed perspective. Adversaries' strengths should not be exaggerated nor should their actions be shown as coordinated or sharing a common goal.
3. The goal is creating a single, stable model is undesirable as it is more useful to develop multiple models through multiple formats as these can reveal different risks and vulnerabilities, and provide information useful to different types of individuals.

This manifesto represents current thinking from the industry's leaders in digital threat modeling, and its recommendations should be seen as representative of agreed upon best practices. On this advice, conflict practitioners and peacemakers deployed in the field should work in teams, focus on the broad, and aim to create deeply contextual, individually-tailored models and resulting mitigation strategies.

### Threat Modeling as Harm Reduction

Threat models and risk assessments examine facts on the ground as they exist at a given time and place. The structures, relationships, and power differentials of a given locale can be mapped and studied, but they represent *at best* a contextualized snapshot—a situational awareness frozen at the time of analysis—and often times, something far less precise. An analyst must be able to distinguish between information and data points which are factual, static (i.e., will not change over time), and dynamic (i.e., can change over time).<sup>31</sup>

Understanding risks, dangers, and threats to one's safety and security is an ongoing and dynamic process of assessment—a measured evaluation of intersecting interests.<sup>32</sup> One element of developing such as assessment is the creation of a threat model to reduce potential harm.

Threat modeling is not simply a means to detect insecurity, but more also a means of securely *designing* our deployments, engagements, and ventures into situations where risk is present. As a prominent technical (i.e., software and computer system) threat modeling scholar explains:

We threat model to anticipate problems when it's inexpensive to deal with them...When we're thinking through what it is that we're going to build and how we're going to arrange the components, we have this infinite ability to make changes quickly and

---

<sup>31</sup> Bram B. Van Der Meer and Margaret L. Diekhuis, "Collecting and Assessing Information for Threat Assessment," in *International Handbook of Threat Assessment*, ed. J. Reid Meloy and Jens Hoffmann (New York, NY: Oxford University Press, 2014), 64.

<sup>32</sup> Van Der Meer and Diekhuis, 56.

easily. Threat modeling is a set of methods that allow us to think about security at that point so that the thing we build is as secure as we need it to be.<sup>33</sup>

Conflict practitioners need not accept the “seemingly inevitable consequence of new environments”<sup>34</sup> and their accompanying insecurities, but rather, through the use of an intersectional threat model which aims to reduce harm, practitioners can identify areas of concern and their potential mitigations. The use of the terms *harm reduction* and *intersectional* are explicit and intentional. *Harm reduction*, as a medical approach, seeks to acknowledge and accept the unavoidable persistence of risk, while still seeking to minimize its likelihood and consequential impact. Harm reduction rests upon the notion that we all deserve security, without stigma or the need for justification (e.g., I deserve security because of X).<sup>35</sup> Security is part of a complex ecosystem of concerns with some approaches better than others. It is with this acknowledged risk that we continue to engage in our work, and though we seek to reduce the likelihood and impact of dangers, we proceed with the knowledge that such risks are ever-present and persistent.

It should go without saying that risk—including security risks, frequency of exposure to disease, vulnerability in disaster situations, etc.—is *not* experienced by all people evenly, or with equal likelihood and consequence.<sup>36</sup> Factors including (but not limited to) gender, race, ethnicity, class, citizenship, nationality, physical ability, sexuality, age, employment status, political views, and religion will fundamentally impact an individual’s risk and threat models. This acknowledgement has appeared regularly in academic<sup>37</sup> and government-authored<sup>38</sup> studies, and should certainly inform an analyst’s approach.

### Threat Modeling as Intersectional

*Intersectional* is used here not as a nod to decades of critical scholarship on identity, power, and marginalization,<sup>39</sup> but rather to point towards the need for a multi-leveled, interdependent, nested approach to understanding security which acknowledges the social, political, economic,

---

<sup>33</sup> Adam Shostack, *Why Threat Model?*, Streaming video (Adam Shostack & friends, 2021), <https://adam.shostack.org/blog/2021/06/why-threat-model/>.

<sup>34</sup> Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*, 51.

<sup>35</sup> Electronic Frontier Foundation, “The Harm Reduction Approach,” Security Education Companion, 2021, <https://sec.eff.org/articles/harm-reduction>.

<sup>36</sup> Conway, “Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines,” 370.

<sup>37</sup> Daniel Chaplin, John Twigg, and Emma Lovell, “Intersectional Approaches to Vulnerability Reduction and Resilience-Building” (UK: BRACED, April 12, 2019), <https://cdn.odi.org/media/documents/12651.pdf>; Christian Henrik Alexander Kuran et al., “Vulnerability and Vulnerable Groups from an Intersectionality Perspective,” *International Journal of Disaster Risk Reduction* 50 (November 1, 2020): 101826; Musabber Ali Chisty et al., “Intersectionality, Vulnerability and Resilience: Why It Is Important to Review the Diversifications Within Groups at Risk to Achieve a Resilient Community,” *Continuity & Resilience Review*, January 1, 2021.

<sup>38</sup> Kristen Vinyeta, Kyle Powys Whyte, and Kathy Lynn, “Climate Change Through an Intersectional Lens: Gendered Vulnerability and Resilience in Indigenous Communities in the United States” (Washington, DC: United States Department of Agriculture, Forest Service, December 2015), [https://www.fs.fed.us/pnw/pubs/pnw\\_gtr923.pdf](https://www.fs.fed.us/pnw/pubs/pnw_gtr923.pdf).

<sup>39</sup> Most notably, see: Patricia Hill Collins, *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment* (New York, NY: Routledge, 1991); Kimberlé Crenshaw, *On Intersectionality: The Essential Writings of Kimberle Crenshaw* (New Press, The, 2012).

cultural, legal, and technical.<sup>40</sup> To this list, one could add foci on the military, and those related to the environment,<sup>41</sup> especially due to the trans-border, deterritorialized nature of climate-related crises including human migration, resource scarcity, and increasingly violent weather events which constitute an existential danger.<sup>42</sup> I have attempted to develop and promote such an intersectional approach amongst technical (i.e., digital and information security)<sup>43</sup> and social movement communities alike,<sup>44</sup> paying particular attention to the legal, political, social, and technical risks. Such a focus helps to develop, engage, and promote a new narrative of security—advocating for alternatives to the question of *security for whom*.<sup>45</sup>

To construct a single example to demonstrate the need for intersectional modeling, we can imagine a team developing medical, educational, technical, or infrastructural services in a conflict, post-conflict, or disaster zone. Assuming the conflict involves non-state actors as a main belligerent party (e.g., Hamas in the Gaza Strip), the delivery of services in this contested space could only be understood through an intersectional framework, as the non-state actor would be central in the provision of social services including schools, religious sites, medical facilities, job training, childcare, financial assistance, prisoner support, etc.<sup>46</sup> To *only* understand these armed actors from a securitized, military, or political framework would fail to account for the key role they play in the social, religious, ethnic, and economic reality for many residents—engendering popular support for their wider goals.<sup>47</sup> This is especially important in a range of conflicts, where non-state and quasi-state actors engage in a “demonstration of potency [through] meeting the needs of the people through an administrative apparatus” such as those maintained by Salafi Jihadists operating in poorly-governed areas (e.g., the Taliban in Afghanistan, or various, Al Qaeda factions in Mali, Somalia, Nigeria, the Egyptian Sinai, Yemen and elsewhere), or other locales where armed actors control and govern territory (e.g., Zapatista-controlled Mexico, or Kurdish-controlled Rojava/northeastern Syria) .

---

<sup>40</sup> This approach is informed by the theory of “nested conflict” as explored by: Marie Dugan, “A Nested Theory of Conflict,” *Leadership Journal: Women in Leadership* 1 (1996): 9–19.

<sup>41</sup> Barry Buzan, Ole Waever, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Pub, 1998), 6–8.

<sup>42</sup> Columba Peoples and Nick Vaughan-Williams, *Critical Security Studies: An Introduction* (Taylor & Francis, 2010), 81.

<sup>43</sup> For example, see: Michael Loadenthal, “Legal-Centric Risk and Threat Modeling for Itme, a Solid Provider,” White paper series (Cincinnati, OH: Off the Page Consulting, February 2021); Michael Loadenthal, “Political-Centric Risk and Threat Modeling for Itme, a Solid Provider,” White paper series (Cincinnati, OH: Off the Page Consulting, February 2021); Michael Loadenthal, “Social-Centric Risk and Threat Modeling for Itme, a Solid Provider,” White paper series (Cincinnati, OH: Off the Page Consulting, February 2021); Michael Loadenthal, “Technical Risk and Threat Modeling for Itme, a Solid Provider,” White paper series (Cincinnati, OH: Off the Page Consulting, February 2021).

<sup>44</sup> For example, see: Michael Loadenthal, “Advanced Threat Modeling and Key Points of InfoSec & OPSEC for Activists” (Institute for Advanced Troublemaking, Cincinnati, OH: IAT, 2020); Michael Loadenthal, “Web Security and Intersectional Threat Modeling for Activists and Organizers” (Working Securely From Home, San Francisco, CA: CoLab Cooperative, 2020); Michael Loadenthal, “Understanding Repression and Building Resilience” (Institute for Advanced Troublemaking, Worcester, MA: IAT, 2018); Michael Loadenthal, “Understanding Contemporary Repression: Psychologically, Legally, Politically and Discursively” (Earth First! Round River Rendezvous, Southeast Ohio: Earth First!, 2018).

<sup>45</sup> Annick T. R. Wibben, *Feminist Security Studies: A Narrative Approach* (New York, NY: Routledge, 2011), 65.

<sup>46</sup> Bard E. O’Neill, *Insurgency & Terrorism* (Dulles, VA: Potomac Books, 2001), 82–84.

<sup>47</sup> O’Neill, chap. 5.

This layered, contextual understanding is especially key in areas where armed actors are well-integrated into everyday social life, as in such cases, providing services (i.e., medical, transportation, sanitation), “sanctuary,” or even logistical coordination can amount to *unintended* material support with legal or military consequences for the conflict practitioner.<sup>48</sup> Working amongst, and potentially coordinating *with* these armed actors should be preceded by analysis which takes into account political, cultural, social, and especially legal concerns. Not only could a US-based organization run afoul of domestic law, for example, by unintentionally providing material support<sup>49</sup> to a designated Foreign Terrorist Organization,<sup>50</sup> but even superficial contact with armed actors could expose individuals to violent responses from military, police, militia, and other security forces.

### Frameworks Not Prescriptions

Because it is impossible to design a single set of security practices that reflect the multi-layered risks of innumerable and diverse environmental locales, the aim of this paper is to promote a *method* for identifying, contextualizing, measuring, and mitigating danger. This approach follows trends in the fields of intelligence analysis<sup>51</sup> and threat modeling<sup>52</sup> which encourage “multidimensional” thinking, and reaching beyond the traditional, technical focus. This framework is not an edict to be universally applied, but rather promotes a *framework and methodology* to be shaped by local conditions, and refocused by whatever locally-situated insecurity is the most relevant and pressing.

This framework approach—as weighed against a more prescriptive guideline approach<sup>53</sup>—is key to *not* isolate the practitioner from their environment and its externalities. Instead of promoting the hardening and securitization of sites and persons, we understand the individual to be an *active* agent in their own security and risk assessment. The use of high walls and armed guards can serve to promote fear by identifying the practitioner as isolated and vulnerable spectators to their own situations, and their protection as a passive act.<sup>54</sup> In such an understanding, the violence and risks associated with work is understood to be something *they*

---

<sup>48</sup> O’Neill, 116–19.

<sup>49</sup> Legal Information Institute, Cornell Law, “18 U.S. Code § 2339A - Providing Material Support to Terrorists,” LII / Legal Information Institute, 2009, <https://www.law.cornell.edu/uscode/text/18/2339A>; Legal Information Institute, Cornell Law, “18 U.S. Code § 2339B - Providing Material Support or Resources to Designated Foreign Terrorist Organizations,” LII / Legal Information Institute, 2015, <https://www.law.cornell.edu/uscode/text/18/2339B>.

<sup>50</sup> U.S. Department of State, Bureau of Counterterrorism, “Foreign Terrorist Organizations,” *United States Department of State* (blog), January 10, 2020, <https://www.state.gov/foreign-terrorist-organizations/>.

<sup>51</sup> Noel Hendrickson, *Reasoning for Intelligence Analysts: A Multidimensional Approach of Traits, Techniques, and Targets* (Lanham, MD: Rowman & Littlefield Publishers, 2018), chaps. 5, 13, 18, 23, 28.

<sup>52</sup> For example, see: Jon Pincus, “Social Threat Modeling,” Medium, May 11, 2018, <https://medium.com/a-change-is-coming/social-threat-modeling-the-winds-of-change-are-in-the-air-8dc330479a50>; Adam Shostack, Threat Modeling for Social Issues, interview by Anna Delaney, Video, January 28, 2021, <https://www.databreachtoday.com/threat-modeling-for-social-issues-a-15854>; Michael Loadenthal, “Intersectional, Risk-Centric, Threat Modeling for Web 3.0,” White paper series (Cincinnati, OH: Off the Page Consulting, February 2021).

<sup>53</sup> For an excellent example of a more practice-centric, guideline approach, see: Shaun Bickley, “SAFETY FIRST: A Safety and Security Handbook for Aid Workers” (London, UK: Save the Children, 2010).

<sup>54</sup> Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*, 216.



do to *me*. The present effort reflects a nascent trend of interdisciplinary scholarship promoting an intersectional, and “relational”<sup>55</sup> analysis—one which incorporates a range of conflict actors, motives, and “the multiplicity of factors that contribute to a security incident.”<sup>56</sup> This multiplicity framework understands conflict practitioners to be embedded within often immutable, interdependent institutions, embedded with conflict systems, situated within wider geopolitical realities.

### A Risk-Centric Threat Modeling Approach

While there are a variety of approaches to threat modeling, this paper advocates for an attack-driven, risk-centric, and intersectional approach which seeks to balance the diverse areas of *possible* threats with the individual’s need for simplicity and security. Unmitigated risks which map atop known attack vectors represent viable threats against personnel, their assets, and the networks which they support.<sup>57</sup> After these risks are named and understood, risk management strategies can be developed, and mitigations (e.g., policies, practices, technologies) developed and put in place. Not all risks will have the same likelihood, or require the same level of preparation, resources, and sophistication, nor will all types of risk carry with them the same potentiality for damage. It is this calculation—attack requirements, scope, and impact, likelihood, and risk remediation costs—that undergirds a risk-centric approach and the policies that emanate from it.

A risk-centric approach begins with the acknowledgement that risk *cannot* be eliminated. This approach is shared by harm reduction practices, such as those applied on intravenous drugs users.<sup>58</sup> While risks can be enumerated and guarded against to reduce their likelihood and impact, risk is ever-present.

### Weaknesses, Vulnerabilities, Exploits, and Risks

The task of risk-centric and attack-driven threat modeling is to identify and respond to risk, though how this is understood requires some familiarity with the language of modeling risk. While in their more general usage, words such as “weakness”, “vulnerability”, “exploits”, “risks”, and “threats” may appear to point to the same things, within threat modeling, they indicate key differences. It is therefore helpful to briefly clarify these often-conflated terms.<sup>59</sup>

---

<sup>55</sup> Charles Tilly, *The Politics of Collective Violence* (Cambridge University Press, 2003).

<sup>56</sup> Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*, 58.

<sup>57</sup> UcedaVelez and Morana, *Risk Centric Threat Modeling*, 57.

<sup>58</sup> For example, see: UNAIDS, “Harm Reduction Saves Lives” (Geneva: Joint United Nations Programme on HIV/AIDS, 2017), [https://www.unaids.org/sites/default/files/media\\_asset/harm-reduction-saves-lives\\_en.pdf](https://www.unaids.org/sites/default/files/media_asset/harm-reduction-saves-lives_en.pdf); Azores-Gococo Nicole M. and Fridberg Daniel J., “Harm-Reduction Strategies for Injection Drug Use,” *Psychiatric Annals* 47, no. 1 (January 1, 2017): 45–48; National Harm Reduction Coalition, “Safe(r) Drug Use 101,” *National Harm Reduction Coalition* (blog), 2021, <https://harmreduction.org/issues/safer-drug-use/facts/>.

<sup>59</sup> These conceptual definitions were adapted from: UcedaVelez and Morana, *Risk Centric Threat Modeling*, 1–3; Tarandach and Coles, *Threat Modeling*, xxviii–xxx; Liz Rice, *Container Security: Fundamental Technology Concepts That Protect Containerized Applications*, 1st edition (Sebastopol, CA: O’Reilly Media, 2020), 2.



Table: Distinguishing Weakness, Exploitability, Vulnerability, Risk and Threat

	Definition	Example
<b>Weakness</b>	A known, underlying defect in the system, the result of not following best practices, standards, or conventions	A practitioner is deployed in a conflict zone, helping to set up mobile clinics, and is readily-identifiable as an outsider, and employed by a multinational agency.
<b>Exploitability</b>	The measure of how easily an attacker can utilize a weakness to cause harm, disruption, etc.	The practitioner is easily identifiable with their employer and has weak ties to the local community outside of those with the Ministry of Health.
<b>Vulnerability</b>	A known weakness which is exploitable and used a means for an attacker to strike	The practitioner's employer mandates the individual to wear a uniform, travel via a known mode of transportation (e.g., armored, designated car) <sup>60</sup> , and live in shared housing reserved for foreign nationals.
<b>Risk</b>	Calculation based on the probability and potential impact resulting from the successful exploitation of a weakness. Risk is relative to the system, the assets it contains, degree of skill required to exploit, and its potential impact	The practitioner faces a high risk of kidnapping, direct violence, unintentional violence from local factional fighting, and potential exposure to disease.
<b>Threat</b>	The path to the risk occurring; the means for its actualization	Because the practitioner is easily identifiable, not tied to the local community, lacks optimal situational awareness, the potential for malicious individuals' causing them harm is ever-present.

The preceding examples are meant to represent generic attack vectors which are obvious and require low degrees of sophistication or reasoning. These can often be understood as crimes of opportunity, fundamentally different from sustained, targeted, well-scouted attacks from a dedicated and sophisticated attacker.

To tie these terms together, we can say that the underlying *weakness* is embedded within a particular *vulnerability*, which requires a means to *exploit*, and thus represents a *risk* to the practitioner. The *weakness* does not inherently lead to a systemic *threat*. If the *vulnerability*

<sup>60</sup> The prevalence of threats to practitioners at their sites of transportation is well documented in a variety of inquiries including: King, "Chronology of Humanitarian Aid Workers Killed in 1997– 2001"; Abby Stoddard and Adele Harmer, "Little Room to Maneuver: The Challenges to Humanitarian Action in the New Global Security Environment," *Journal of Human Development* 7, no. 1 (March 1, 2006): 23–41; Rowley, Crape, and Burnham, "Violence-Related Mortality and Morbidity of Humanitarian Workers"; Stoddard, Harmer, and DiDomenico, "Providing Aid in Insecure Environments: 2009 Update."

it creates can be mitigated, the *risk* is eliminated while the *weakness* persists. A comprehensive security framework balances the persistence of internal vulnerabilities, external threats, and the operational functionality of the task at hand. For example, it would be short-sighted to focus on external threats from malicious actors (i.e., kidnappers, militia) while ignoring or accepting risks embedded within internal mechanisms (i.e., insider threats)<sup>61</sup> in training staff or planning daily operations. This is precisely why the present analysis adopts a *risk-centric* approach to understanding threats, which aims to enumerate the widest universe of potential risks across a range of possible environments.<sup>62</sup>

### Threat Typologies, Motives, and Archetypes

Understanding likely threats from an attack-driven perspective can be enhanced by focusing on actors' motives. By better understanding an individuals' motives, we can more accurately predict and estimate attack scenarios, their aspirational aims, likely level of sophistication, and as a result, possible countermeasures.<sup>63</sup> While many threat types share motivations (e.g., financial gain, political contestation), to assume a single motive across multiple actors can lead to a limited mitigation and defensive strategy. By understanding an actors' varied motives, we can better approximate their plans and potential defense measures.

One way to understand and group attackers is through the perspective of user archetypes—typical behaviors grouped around shared attributes.<sup>64</sup> Such archetypes should be constructed around attackers' behavioral patterns, preferences, psyche, background, emotions, attitudes, and presumed personality traits.<sup>65</sup> These archetypes can be differentiated and shown relationally through typology trees, such as the one below which identifies and distinguishes six types of individuals who issue threats:

---

<sup>61</sup> Eleanor E. Thompson, *The Insider Threat: Assessment and Mitigation of Risks* (Boca Raton, FL: CRC Press/Taylor & Francis, 2019), chap. 4.

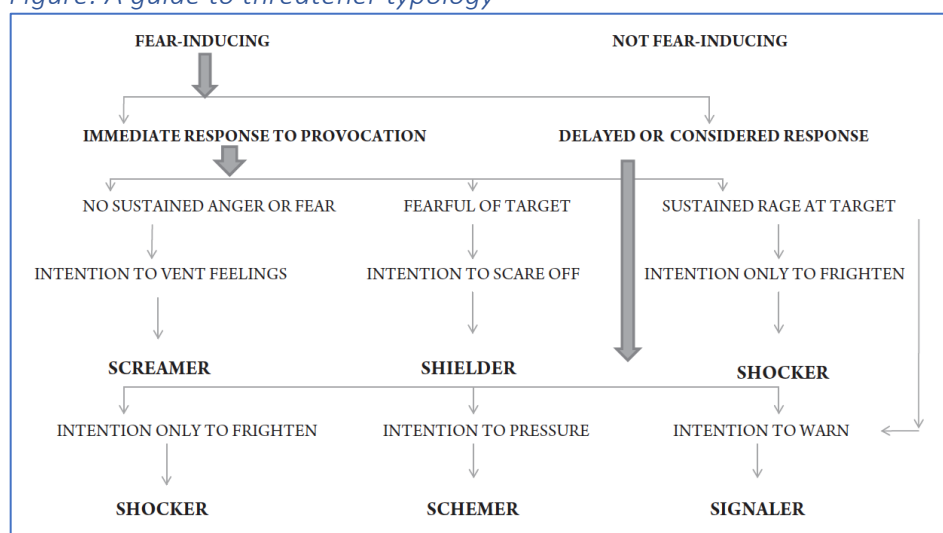
<sup>62</sup> An example of this widest universe approach can be seen in Appendix 2: Risk, Danger, and Threat Mind Map for Conflict Practitioners.

<sup>63</sup> UcedaVelez and Morana, *Risk Centric Threat Modeling*, 12–13.

<sup>64</sup> Further mapping of archetypes can be accomplished using organizational/situational risk matrices and expanded upon through the use of archetype-driven matrices. These tools and their application are the focus of a forthcoming publication from this paper's principal investigator.

<sup>65</sup> Nancy R. Mead et al., "A Hybrid Threat Modeling Method" (Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute, March 2018), 3.

Figure: A guide to threatener typology<sup>66</sup>



The ‘threateners’ mapped above are divided by motivation and function, specifically the likelihood they will act on their threats.<sup>67</sup> Motive is a key factor in measuring relative risk and likely attack vectors. An attacker seeking to covertly surveil an institution or individual for potential opportunities for blackmail will have a very different approach to pre-attack reconnaissance than someone seeking to disrupt or disable a site for political theater.

While motive is not a *perfect* predictor of an attackers’ strategies and goals, it can provide key context for estimating an attacker’s aims and capabilities. Below is a table estimating three typical and relevant threat types, as well as their associated targets, motive category, and likely attacker type.<sup>68</sup>

<sup>66</sup> Lisa J. Warren, Paul E. Mullien, and Troy E. Mcewan, “Explicit Threats of Violence,” in *International Handbook of Threat Assessment*, ed. J. Reid Meloy and Jens Hoffmann (New York, NY: Oxford University Press, 2014), fig. 2.1.

<sup>67</sup> Warren, Mullien, and Mcewan, 19.

<sup>68</sup> This basic table can be expanded with additional columns enumerating actors’ goals, common tools/exploits/methods used, history of past activities, relationship to other identified actors, etc.

Table: Targets, Motives, and Likely Attackers

	Target Examples	Motive Examples	Likely Attackers
<b>Theft, or unintentional disclosure</b>	Intellectual property (e.g., data), validated credentials (e.g., badges, keys), communications systems, vehicles, personal property (e.g., smartphone, jewelry)	Financial gain, competitive advantage, intimidation, bragging rights, curiosity, political speech, service disruption	Governments, militaries, corporations, organized crime, opportunistic criminals,
<b>Kidnapping, abduction, assault, or other violent, physical attack</b>	Personnel associated with the institution or organization, its volunteers, employees, contractors, external partners, constituents, community stakeholders	Financial gain, political speech or action, inter-factional bargaining, demonstrating dissent and discontent to power elites, bragging rights	competitors, hackers, activists, religious groups, terrorist organizations and other armed non-state actors (e.g.,
<b>Misuse or misrepresentation</b>	Intellectual property, physical resources, credentials, financial instruments, critical infrastructure, personnel, other resources owned or utilized by the target	Financial gain, defamation, access to restricted materials, service disruption, political speech	militia, 'warlords'), security state factions, governmental defectors...

While such an analysis is far from specific or prescriptive, it is meant to illuminate the relationship between attack type (e.g., theft v. misuse) and an attackers' motive and actions. In doing so, it is easy to notice that a single attacker type (e.g., organized crime) can have multiple motivations and means of attack.

Each attacker type will have a different path towards their goals situated in their motive. The field of threat assessment offers a model for such a progressive path, for example:

Grievance → ideation → research/planning → preparation → breach → attack<sup>69</sup>

In a scenario such as this, the original grievance motivates the desire to act (i.e., ideation), and the steps follow from there. Understanding motive can tell us a great deal about how an attacker may strike. An attacker motivated by anger or ideology is likely to follow a path similar to the one above, whereas one motivated by financial gain may present *no grievance* and a *lengthier* period of research, planning, and preparation. Beyond the categorical motives outlined above (e.g., financial gain, defamation, etc.) there are many impetuses for those who wish us harm, ranging from those seeking an exciting challenge (i.e., 'thrill seekers'), to those motivated by patriotism or state-sanctioning of attacks.

<sup>69</sup> Adapted from: Frederick S. Calhoun and Stephen W. Weston, *Threat Assessment and Management Strategies: Identifying the Howlers and Hunters, Second Edition*, 2nd edition (Boca Raton, FL: CRC Press/Taylor & Francis, 2016), 119.

### Developing Risk Management Strategies

Having identified motivations and typical paths towards risk for practitioners, a next step involves negotiating a strategy to help manage and mitigate these dangers. Building from classic texts in the field of risk management, in order to develop a strategy to manage risk, “risk factors must be systematically identified, assessed and provided for.”<sup>70</sup> In developing strategy, there are several ways in which threats, can be addressed. Given a risk, threat, or vulnerabilities, these insecurities can be dealt with through four distinct approaches—mitigate, eliminate, transfer, or accept—detailed in the table below.

*Table: Dealing with Threats—Mitigate, Eliminate, Transfer, and/or Accept*

Approach	Definition	Example
<b>Mitigate</b>	Take steps to make it more difficult to exploit a given threat.	Because insecurity of staff requires <i>identifying</i> employees, steps to decrease this can be taken such as eliminating uniforms, keeping credentials on site, varying travel routes and modes of transportation, distributing workers’ living arrangements through a given area, etc.
<b>Eliminate</b>	Take steps to remove opportunity for a given threat often by removing the vulnerable aspect.	Medical staff could eliminate their community deployment and only see patients in a secured facility, within a controlled perimeter, reducing the opportunity for abduction/violence. Staff can be prevented from traveling outside of their hardened facility and prevented from wearing uniforms or identifiable marking outside of the facility.
<b>Transfer</b>	Take steps to make the securing of a given threat someone else’s responsibility.	Staff are assigned escorts or protective accompaniment from the host government or a private security firm.
<b>Accept</b>	Be aware of a given threat, but by acknowledging that the cost of a proper mitigation would be too high, the system continues with the ever-present risk of the identified threat.	Inform staff of the risks, provide adequate training and support, but continue to operate within the conflict zone aiming to reduce the likelihood of harm (i.e., a harm reduction approach) whenever possible.

In general, when considering strategies, these can be thought of as hierarchical options: begin with mitigation, if that is not possible, proceed to elimination, then transfer, and if nothing is possible, then acceptance. Mitigation should always be the aim as it allows the system to maintain functionality (unlike with elimination), while avoiding having to externalize the threat (i.e., transfer). While deciding which path to pursue, one preliminary consideration is the rate of

<sup>70</sup> D.V. Pym, “Risk Management,” *PM Network* 1, no. 3 (August 1987): 33–36.

success for similar ventures.<sup>71</sup> For example, when considering how to deal with persistent abductions of staff, an organization can examine the past histories of organizations' efforts to mitigate, eliminate, transfer, or (as undesirable as it may be) accept this threat.<sup>72</sup> In considering the recommendations, one must also consider alternative approaches. For example, some solutions identified as mitigations may best be handled through an approach closer to elimination—removing the risky component rather than salvaging it. Therefore, despite suggestions provided for reducing the impact of identified risks, when deciding upon a strategy, counter-conclusions should be considered as well.

The risk assessment and management perspective advocated throughout broadly follows a series of stages derived from widely-accepted, technological standards, and can be understood as a simplified series of steps, namely:

1. **Establish context** (e.g., understanding of the organization and conflict 'in country' and establishing situational awareness)
2. **Identify risks** (e.g., group brainstorm, mind mapping, attack trees)
3. **Analyze risks** (e.g., SWOT/PEST analysis, risk matrices)<sup>73</sup>
4. **Evaluate risks** (e.g., determining likelihood, frequency, and potential consequences)
5. **Mitigate risks** (e.g., creating risk treatment policies, procedures, technologies, workflows)

While a host of factors are carefully balanced in assessing risk, calculations are grounded in an analysis of probability and severity,<sup>74</sup> or to use the preceding language, likelihood and impact.

Risks and potential sites of insecurity need to be predicted, identified, observed, and understood prior to designing a management or mitigation plan. Risks need to be classified (i.e., risk taxonomy) and threat actors grouped together to both tailor the analysis and provide a generalizable solution. Additional frameworks exist at the ready for assessing and measuring risk and can be consulted in tandem. For example, the US Department of Homeland Security (DHS) has authored and recently revised their own Threat and Hazard Identification and Risk Assessment (THIRA) which is based around the aforementioned threat modeling framework. The DHS framework centers upon identifying, contextualizing, and determining the capability of risk-threats, broadly categorizing them into natural (e.g., epidemic, flood), technological (e.g.,

---

<sup>71</sup> Robert M. Clark, ed., *Intelligence Analysis; A Target-Centric Approach Fifth Edition*, 5th edition (Los Angeles, CA: CQ Press, 2016), 169.

<sup>72</sup> This manner of analysis, informed by past histories, can be supported through the use of a Security Products Review—not unlike a literature review of relevant prior assessments. This tool and its application is the focus of a forthcoming publication from this paper's principal investigator.

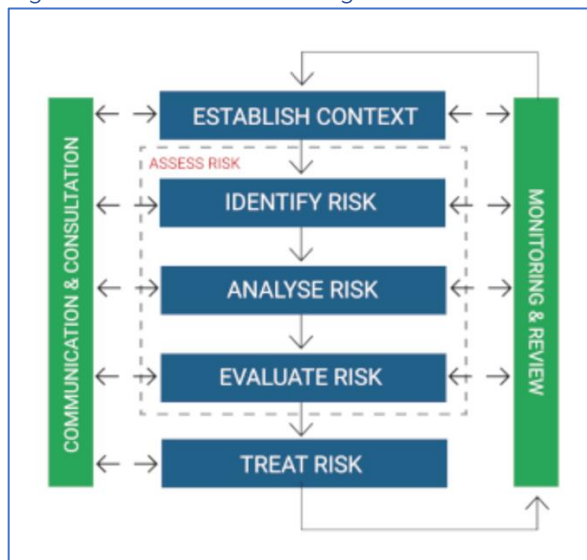
<sup>73</sup> An example of a continuum (Appendix 1) as well as a mind map (Appendix 2) focused on articulating risks, threats, and dangers for conflict practitioners are included as appendices to this paper, and expanded upon as the focus of a forthcoming publication from this paper's principal investigator. This forthcoming work will expand upon the use of the abovementioned tool set for risk analysis, namely the use of SWOT analyses, risk matrices, archetype-driven matrices, and mind maps, attack trees, and fishbone diagrams.

<sup>74</sup> Carl L. Pritchard, *Risk Management Concepts and Guidance*, 5th ed. (Boca Raton, FL: CRC Press, 2015), 7.

pipeline explosion, utility disruption), and human-caused categories (e.g., active shooter, cyber attack).<sup>75</sup>

The aforementioned staged approach—establish context before identifying, analyzing, evaluating, and mitigating risks—is mirrored in the technical literature as well, such as the Generic Risk Management Process published by the International Organization for Standardization (i.e., ISO 27005), and included below:

*Figure: Generic Risk Management Process<sup>76</sup>*

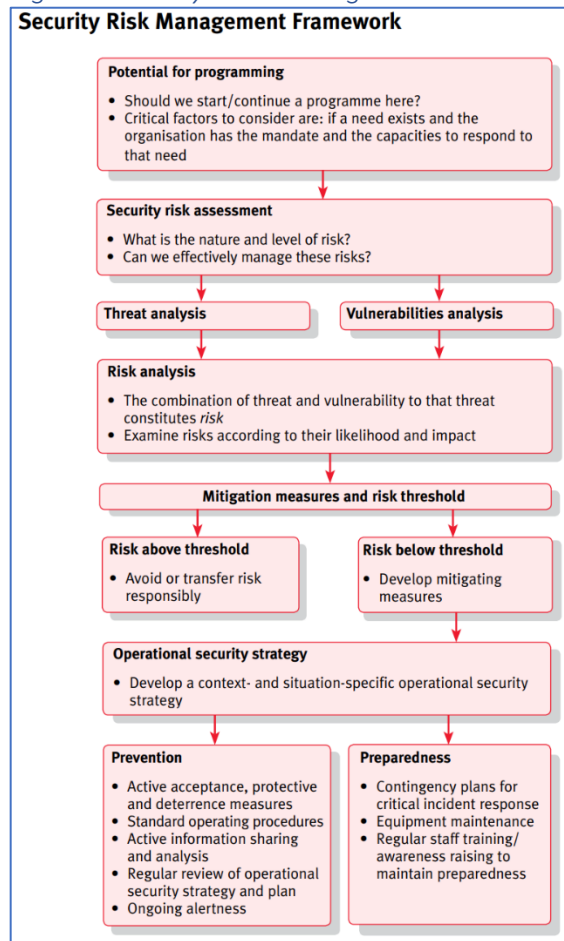


This generic risk management strategy is a helpful starting point and has been expanded upon by conflict practitioners to integrate risk assessment, threat analysis (i.e., externals), vulnerability analysis (i.e., internals), and mitigation measures. The Humanitarian Practice Network features an exemplary diagram in its 2010 report, and included below:

<sup>75</sup> United States Department of Homeland Security, “Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide (3rd Ed.)” (Washington, DC: United States Department of Homeland Security, May 2018), 12, <https://www.fema.gov/sites/default/files/2020-04/CPG201Final20180525.pdf>.

<sup>76</sup> IT Governance USA, “ISO 27005,” 2020, <https://itgovernanceusa.com/cyber-security-solutions/iso27001/iso-27005>.

Figure: Security Risk Management Framework<sup>77</sup>



The framework promoted in this paper is meant to guide an analyst through this flow, beginning with establishing context, and ending at the start of a reflexive loop mitigating risks. This process of understanding risks aims to promote system design-level concerns and strategies. In a practitioners' final stage of analysis—the mitigating risks stage—we can return to the preceding mitigate, eliminate, transfer, accept framework. This is akin to “treat[ing] risk” as outlined above, and takes into account the intersectional, and deeply contextual position of conflict practitioners deployed in diverse zones of insecurity.

The preceding pages are an attempt to develop and promote a manner of understanding security and risk which is embedded and responsive without being stoic and galvanized. In seeking to identify key considerations—for example, whose security is being promoted, what are the typical experiences of your constituents, what are your potential attackers' motives, etc.—the goal is to identify best practices, and to critique those that fall short. This constitutes the first stage of the present engagement. In the remainder of this paper, we will examine the broader field of conflict practitioners as informed by the training

<sup>77</sup> Humanitarian Practice Network, “Operational Security Management in Violent Environments (Revised Edition)” (London, UK: Overseas Development Institute, Humanitarian Practice Network, December 2010), 9, <https://odihpn.org/resources/operational-security-management-in-violent-environments-revised-edition/>.



and educational materials they receive. The focus of this second stage is to determine how adequately our field is seeking to prepare field-based practitioners to understand dangers, risks, and threats. In the pages that follow we will review a systematic survey of the field of conflict practitioners, the current state of academic literature on this topic, and examine the findings and future recommendations for such a pursuit.

## Stage 2: Surveying the Field at Large

When our team developed this study, we began from a position of ignorance, not knowing the state of affairs of the field, but estimating that it fell short of a desired aim. In order to advance such an assessment, the team sought to survey a broad range of conflict practitioners, and to assess whether or not security featured centrally in organization's thinking. Early on, we located the work of Larissa Fast, whose work *Aid In Danger* focused on the risks facing humanitarian aid workers. This book was central to researchers' foundational basis as according to Fast's assessment:

Few if any [humanitarian aid] agencies devoted systemic attention to security management, protecting their staff, or ensuring that programming and services could continue in the midst of violence and chaos. Instead, many seemed to operate under an assumption of altruistic immunity, an aura of invincibility rooted in the supposition that no one would intentionally attack someone there to help. The idea that an aid worker, providing much needed assistance, could be purposely attacked supervenes such inviolability. Security, in short, does not feature prominently in this image; rather, risk was just part of the job.<sup>78</sup>

Keeping Fast's assessment in prime focus, it was obvious that a wider exploration of the field was warranted to confirm or contest these findings. Therefore, this paper in its second stage surveys relevant field leaders—both academic-based and practitioner-based—whose work could benefit from the development of risk-centric security materials.

## Surveying Academics: Contemporary literature

### Background Literature

There is a general consensus held by both scholars and practitioners that aid workers' safety and security has been increasingly at risk throughout the past several decades.<sup>79</sup> Over the past

---

<sup>78</sup> Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*, 156–57.

<sup>79</sup> For example, see: Mark Cutts and Alan Dingle, *Safety First: Protecting NGO Employees Who Work in Areas of Conflict (2nd Ed.)* (London, UK: Save the Children, 1998); Charles Rogers and Brian Sytsma, "World Vision Security Manual: Safety Awareness for Aid Workers" (Geneva: World Vision, 1999), <https://fmwm.org/wp-content/uploads/2016/02/WV-Security-Manual-amended.pdf>; King, "Chronology of Humanitarian Aid Workers Killed in 1997–2001"; Bickley, "SAFETY FIRST: A Safety and Security Handbook for Aid Workers"; Fast, "Mind the Gap: Documenting and Explaining Violence Against Aid Workers"; Elizabeth Rowley, Lauren Burns, and Gilbert Burnham, "Research Review of Nongovernmental Organizations' Security Policies for Humanitarian Programs in War, Conflict, and Postconflict Environments," *Disaster Medicine and Public Health Preparedness* 7, no. 3 (June 2013): 241–50; Kristian Hoelscher, Jason Miklian, and Havard Mokliev Nygard, "Understanding Attacks on Humanitarian Aid Workers" (Oslo, Norway: Peace Research Institute Oslo, June 2015),

two decades, violence against aid workers specially has risen significantly. In just 2012, a high point for such incidents, these dangers resulted in 274 aid workers kidnapped, killed, or injured.<sup>80</sup> Scholar Larissa Fast, who has written extensively on this subject, notes:

The humanitarian impulse to provide lifesaving assistance is under fire, literally and figuratively: literally, as aid workers from Afghanistan to Zimbabwe are attacked, injured, kidnapped, and killed, and aid agencies are prevented from accessing vulnerable populations; and figuratively, as the essence of humanitarian action—to provide life-sustaining assistance to those suffering as a result of war or natural disaster—is compromised by those who link such assistance to foreign policy or security goals.<sup>81</sup>

Concern over aid worker security and the potential of workers to provide aid is by no means a new concept, but worries have intensified in the wake of the 9/11 terrorist attacks and the so-called Global War on Terror which followed. Fast touches on this concern noting that many attacks against aid workers have occurred in the midst of conflicts that began in the wake of 9/11.<sup>82</sup> Fast writes that this “raises questions about how to ensure physical security for humanitarians in a post-9/11 world,” bemoaning that, “the response to security concerns across the humanitarian community has been somewhat schizophrenic.”<sup>83</sup> According to Fast, there has not been a unified response to the increasing insecurities that humanitarian aid and other conflict-adjacent workers face. While some practitioner-centric organizations have looked to practices of deterrence and other protective measures, other organizations operate without any sort of risk assessment or security management strategy.<sup>84</sup>

There are several arguments against prioritizing security management that appear to be preventing organizations from adopting improved strategies. Common arguments include the notion that risk is an unavoidable part of conflict work, that the organization has been managing risk for years or decades without adopting new policies, or that the organization does not operate in conflict zones.<sup>85</sup> These arguments contain several flaws. Not only do they fail to

---

<https://www.prio.org/utility/DownloadFile.ashx?id=101&type=publicationfile>; Emma Jones et al., “Managing the Security of Aid Workers with Diverse Profiles,” European Interagency Security Forum Research Paper (London, UK: European Interagency Security Forum, 2018); Jeffrey Alan Sluka, “Too Dangerous for Fieldwork? The Challenge of Institutional Risk-Management in Primary Research on Conflict, Violence and ‘Terrorism,’” *Contemporary Social Science* 0, no. 0 (July 16, 2018): 1–17.

<sup>80</sup> Adele Harmer, Abby Stoddard, and Kate Toth, “Aid Worker Security Report 2013 - The New Normal: Coping with the Kidnapping Threat” (Washington, DC: Humanitarian Outcomes, October 2013), [https://aidworkersecurity.org/sites/default/files/2020-08/AidWorkerSecurityReport\\_2013\\_web.pdf](https://aidworkersecurity.org/sites/default/files/2020-08/AidWorkerSecurityReport_2013_web.pdf).

<sup>81</sup> Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*, 1.

<sup>82</sup> Throughout the literature, and especially that which tracks violent incidents, the use of the term “aid worker” and “humanitarian aid worker” is extremely common and encompasses a variety of categories of conflict practitioners operating in conflict, post-conflict, and disaster zones.

<sup>83</sup> Fast, “Mind the Gap: Documenting and Explaining Violence Against Aid Workers,” 366.

<sup>84</sup> Fast, 366.

<sup>85</sup> Koenraad Van Brabant, “Mainstreaming the Organisational Management of Safety and Security,” HPG report (London, UK: Overseas Development Institute, Humanitarian Policy Group, March 2001), 5, <https://gisf.ngo/wp-content/uploads/2014/09/0598-Van-Brabant-2001-Mainstreaming-the-Organisational-Management-of-Safety-and-Security.pdf>.

recognize the increasing danger that practitioners face, but they assume that risk is only inherent to violent conflict zones and that said risk cannot be reduced through individual and organizational measures.<sup>86</sup> These assumptions are not in line with the evidence gathered over the last several decades of research. In 2011, “86 aid workers died, 127 were severely injured, and 95 were kidnapped in 151 incidents worldwide,” which at the time had represented the highest number of incidents since researchers began to track in the mid-1990s.<sup>87</sup> Many organizations have noted this alarming increase and have worked on building up their safety and security policies and resources during the last decade. While acknowledgment of the dangers faced is needed, a unified approach to security across the field is still nonexistent, as is a fully comprehensive framework of risk assessment and security management.

### Recent Trend Literature

Recent trends in practitioner security further demonstrate the need for improved approaches. The organization Humanitarian Outcomes released a 2020 security report stating that “casualties in 2019 exceeded all past years recorded,” with a total of 125 individuals murdered, 234 wounded, and 124 who were the victims of kidnapping.<sup>88</sup> These incidents disproportionately involved humanitarian health care workers. 42% of humanitarian aid fatalities in 2019 were healthcare workers, which constituted a higher percentage than any previous year recorded.<sup>89</sup> The report, *Understanding Attacks on Humanitarian Aid Workers* provides additional insights into these trends. The authors note, “the increased number of total attacks are driven by a small number of countries that register many more aid worker attacks than what is commonly seen, led by, in particular, Afghanistan and Syria.”<sup>90</sup> These specific conflicts have been violent enough to contribute to the aggregate increase in attacks and fatalities. The authors cite the impact of environmental features in their assessment, noting that “aid organizations are working much more extensively in remote field settings, doing more sophisticated work, and undertaking a much wider variety of development tasks than just a decade ago.”<sup>91</sup> One of the authors’ primary conclusions is that the less developed a nation-state is, the more likely it is that aid workers will be attacked.

Conflict practitioners’ approaches to security and risk management have changed over the past several decades in order to adapt to evolving challenges. According to Christine Persaud, in the past few decades, “there are more dedicated headquarters, regional and field positions for security.... Enhanced [training] to reflect the needs of governance, operational security management and personal security...[and] interagency security forums and opportunities for collaboration have been created.”<sup>92</sup> Unfortunately, this enhanced security

---

<sup>86</sup> Van Brabant, 5.

<sup>87</sup> Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*, 1.

<sup>88</sup> Abby Stoddard et al., “Aid Worker Security Report 2020” (London, UK: Humanitarian Outcomes, August 2020), 2, [https://www.humanitarianoutcomes.org/sites/default/files/publications/awsr2020\\_0\\_0.pdf](https://www.humanitarianoutcomes.org/sites/default/files/publications/awsr2020_0_0.pdf).

<sup>89</sup> Stoddard et al., 2.

<sup>90</sup> Hoelscher, Miklian, and Nygard, “Understanding Attacks on Humanitarian Aid Workers,” 2.

<sup>91</sup> Hoelscher, Miklian, and Nygard, 2.

<sup>92</sup> Christine Persaud, “NGO Safety and Security Training Project: How to Create Effective Security Training for NGOs” (The European Interagency Security Forum/InterAction, 2014), 6,

posture and risk management practices have not led to noticeable improvements in workers' safety. Persaud argues, "in practice, cost and access still remain important factors in how training is implemented and sustained,"<sup>93</sup> concluding that comprehensive security training is not a priority for many organizations. Even for those groups that *do* focus adequate resources on security and risk training, Persaud notes that topics such as conflict resolution, first aid, and development of culture and gender awareness in the field are missing from the materials that organizations provide their workers.<sup>94</sup> While some progress has been made in the field of security risk management, many in the field believe that crucial topics continue to be underrepresented in training.

#### Current Security Strategies and Policy Literature

There is currently no single, agreed-upon way for an organization to conduct security and safety management. Despite a lack of consensus, many organizations and experts in the field *have* adopted overlapping strategies. One common approach is prioritizing acceptance. According to a 2014 study by Fast:

[The strategy of acceptance] incorporates the same skill sets and tools that peacebuilders already employ in their work. It does not rely upon force or weapons but instead on building networks and relationships with a wide variety of stakeholders, especially those who benefit from violence or who are likely to undermine a peace process or peacebuilding activities.<sup>95</sup>

This approach, by emphasizing process instead of results, can build trust between partners and lead to outcomes more broadly beneficial to all parties. The drawback of the acceptance approach is that building the necessary trust in order to reach the desired outcome requires time and effort. According to Fast, those engaging in an acceptance strategy must do so in good faith for it to be successful.<sup>96</sup>

A second common strategic approach to security for organizations is prioritizing inclusion; requiring an organization to look inwards rather than outwards. Organizations that adopt the inclusion approach believe that risk assessment and management must involve everyone in the organization, from executives to program staff.<sup>97</sup> By choosing this strategy, organizations ensure that they will receive diverse perspectives, and that all staff members will be aware of the group's security policies. However, the inclusion approach is more effective for small organizations, as building internal partnerships and awareness in larger groups requires significant time and resources.<sup>98</sup> In order for this approach to work well, organizations must

---

[https://reliefweb.int/sites/reliefweb.int/files/resources/EISF%2520and%2520InterAction\\_Security%2520Training%2520Project\\_April%25202014\\_1.pdf](https://reliefweb.int/sites/reliefweb.int/files/resources/EISF%2520and%2520InterAction_Security%2520Training%2520Project_April%25202014_1.pdf).

<sup>93</sup> Persaud, 7.

<sup>94</sup> Persaud, 10.

<sup>95</sup> Larissa Fast, "Security and Risk Management for Peacebuilding Organisations" (Berlin, Germany: Berghof Foundation, 2014), 16.

<sup>96</sup> Fast, 16.

<sup>97</sup> Fast, 16.

<sup>98</sup> Fast, 16.

hire individuals who represent all sides of the conflicts that the organization hopes to solve, though this could potentially lead to grievances between staff members. Inclusion has clear benefits, but it is a delicate balancing act. Beyond the general values that shape their approach to risk management, many organizations share similar ideas regarding staff security training. Since staff turnover tends to be high, many groups believe that staff training has a low return on investment. Because of this, “learning-by-doing, and learning-on-the-job continue to be a major staff development path.”<sup>99</sup> The mindset that training staff in security and risk policy is not worth the time and effort is highly detrimental to the advancement of the field.

Additionally, there are broad discrepancies between international and national non-governmental organizations (NGOs), an issue explored in *Safety and Security for National Humanitarian Workers*, part of a report by the United Nations Office for the Coordination of Humanitarian Affairs. In this report, the three authors note that while a majority of international NGO staff report receiving *some form* of security training, most local staff report receiving no security training whatsoever.<sup>100</sup> This concern was also voiced in the report *NGOs and Risk: How international humanitarian actors manage uncertainty*, authored jointly by Humanitarian Outcomes and InterAction. In this report, the authors state that many international NGO staff members “understood their national NGO partners to be exposed to high levels of security risk, often without sufficient support, training, and discussion.”<sup>101</sup> While security training is often not given enough attention by smaller organizations, national and local NGOs provide their staff members with even less support in terms of safety and security management.

### Recommendations from the Literature

In attempting to develop recommendations for improvising on the safety of practitioners, researchers took a comprehensive look at recommendations offered for conflict practitioners, especially the international humanitarian aid worker community, for whom the literature is the most developed. In response to this rise in aid worker insecurity, agencies such as the International Committee of the Red Cross have published comprehensive sets of safety guidelines for workers in operational zones to address common dangers experienced. While many scholars and peacebuilders provide recommendations, they are scarcely described as “rules,” but rather “guidelines.”<sup>102</sup> As discussed in the Red Cross publication *Staying Alive*, since each conflict and risk analysis will require a different route of action due to differences in context, environment, and local cultural standards and rules, these guides serve more as an

---

<sup>99</sup> Van Brabant, “Mainstreaming the Organisational Management of Safety and Security,” 48–49.

<sup>100</sup> Abby Stoddard, Adele Harmer, and Katherine Haver, “Safety and Security for National Humanitarian Workers (Annex I to: To Stay and Deliver: Good Practices for Humanitarians in Complex Security Environments),” Policy and Studies Series (New York, NY: Office for the Coordination of Humanitarian Affairs Policy Development and Studies Branch, 2011), 8.

<sup>101</sup> Abby Stoddard, Katherine Haver, and Monica Czwarno, “NGOs and Risk: How International Humanitarian Actors Manage Uncertainty” (Humanitarian Outcomes/InterAction, February 2016), 17, [https://www.humanitarianoutcomes.org/sites/default/files/publications/ngo-risk\\_report\\_web.pdf](https://www.humanitarianoutcomes.org/sites/default/files/publications/ngo-risk_report_web.pdf).

<sup>102</sup> David Lloyd Roberts, “Staying Alive: Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas” (Geneva: International Committee of the Red Cross, 2005 1999), 17.

outline of *strategies*.<sup>103</sup> Many guides and texts recommend combining the materials and information with the best judgment and common sense in order to achieve maximum security and safety in the field and other situations of conflict and dangers.

Several texts claim that if a practitioner has a basic understanding of the risks faced in a conflict zone, dangers that results in insecurity can be avoided or greatly decreased. This strategy consists of recommendations such as adequate environmental adjustment, relying on one's best judgment (following Robert's "rules" versus "guidelines" approach), and understanding the organization's mission within the operational zone.<sup>104</sup> Overall, many security guides cover ground in relation to mental and physical health, effective communication, and environmental dangers (e.g., land mines, natural disasters, vehicle accidents, etc.). Moreover, other scholars discuss how adequate knowledge and understanding of context are required for effective and successful action in operational zones. This knowledge of context includes the causes and dynamics of conflict and how an organization's programs and missions interact within such context.<sup>105</sup>

While an understanding of context is important in security management, scholars are beginning to document and conduct analyses of strategies to avoid danger by integrating themselves into communities through strategies of acceptance. Through the method of field research, scholars Fast, Freeman, O'Neill, and Rowley emphasize the missed opportunities found in implementing strategies of acceptance and how they can solidify the security management of aid workers.<sup>106</sup> In many conflict zones, aid workers are often viewed as the enemy or an opposing party, which drastically changes the context of security operations.<sup>107</sup> As a result, staffers are increasingly found in the midst of violence in the field. In order to combat the rising levels of risks faced, scholars call for a monumental change in humanitarian aid practices, including the construction of a solid ethical framework and civilian and hybrid missions, backed by more research and policy analysis by scholars.

#### Further Research and Literature Limitations

Limitations in research exist when examining how practitioners identify threats and how actors perceive and interact with security. In their survey, Fast and Wiest examine some misconceptions and overlooked risks to aid staffers. While many outsiders often think the largest dangers to aid workers are high-level threats (abduction, homicide, bombing), survey respondents claimed to face low-level threats (work stress, evacuations, mobs) at a much higher rate.<sup>108</sup> The authors also break down threat perception by factors such as aid workers'

---

<sup>103</sup> Roberts, 17–18.

<sup>104</sup> Roberts, 19–21.

<sup>105</sup> Larissa Fast, "A Reflexive Approach to Risk and Intervention for Third-Party Intervenor," *Conflict Resolution Quarterly* 30, no. 4 (2013): 467–489.

<sup>106</sup> Larissa Fast et al., "The Promise of Acceptance as an NGO Security Management Approach," *Disasters* 39, no. 2 (2015): 208–31.

<sup>107</sup> Daniela Irrera, "Protecting the Protectors: Strengthening the Security of NGOs in Conflict Zones" (E-International Relations, August 25, 2020), 2–3, <https://www.e-ir.info/2020/08/25/protecting-the-protectors-strengthening-the-security-of-ngos-in-conflict-zones/>.

<sup>108</sup> Larissa Fast and Dawn Wiest, "Final Report Security Perceptions Survey" (Washington, DC: The United State Institute of Peace, August 2007), fig. 3.1, <https://gisf.ngo/wp-content/uploads/2014/09/0009-Fast-Wiest-2007-Security-Perceptions-Survey10.pdf>.

gender, security training, location, and age, further demonstrating the range in threat perception and interaction by aid staffers.<sup>109</sup> It is found that these low-level threats and identify factors are often neglected in the overall analysis of risks faced by humanitarian workers. Fast and Wiest recommend a comprehensive examination of threats faced by these actors to provide proper physical and mental care and wellbeing from various aid agencies to ensure adequate security.

While security-focused research is still in its early stages, scholars such as Larissa Fast have worked to examine the state of security management in this field.<sup>110</sup> In several of her works, Fast analyzes the causes of violence and the consequences of the strategies organizations use to protect themselves.<sup>111</sup> These approaches to security identify threats as *external* and result in the separation of practitioners from those in need, representing “both symptom and cause of the crisis in the humanitarian system.”<sup>112</sup> Fast found that internal vulnerabilities (i.e., everyday decisions, ordinary human frailties, organizational mistakes) are often missing from organizations’ analyses, and instead, she recommends an alternative framework that captures both internal *and* external factors. Fast examines the dangers faced by peacebuilders, whom she defines as “both insiders and outsiders to the conflict.”<sup>113</sup> Beyond the “humanitarian aid” community, the central focus of much of this emergent literature, Fast finds that there is very little research on the security of “peacebuilders” as well, even drastically less than that focused on aid workers.<sup>114</sup> The author develops a security framework for peacebuilders centered in education, data documentation, better access to resources, and, overall, a deeper look into the security of this dangerous profession.

At this point, it is overwhelmingly evident that there is a large gap in research pertaining to the security and safety of conflict practitioners, specifically literature which helps improve upon one’s security posture and those which promote open, adaptable frameworks for assessing risks, dangers, and threats. Although the community has experienced notable progress in the development of practical staff security guidance within the past several years, notable gaps remain. This considerable lack of literature and resources can impede an organization’s missions and efforts to assemble necessary resources, define security plans, and ensure that the personal and security needs of workers are adequately recognized and addressed. As Rowley, Burns, and Burnham have demonstrated in their report, many organizations lack a distinct security policy document, drastically limiting aid worker security within the organizations.<sup>115</sup> These scholars call for evidence-based views of security management and a common terminology and conceptualization of security management in order to create stronger efforts of aid worker security within organizations.<sup>116</sup>

---

<sup>109</sup> Fast and Wiest, fig. 3.6.

<sup>110</sup> Fast, “Security and Risk Management for Peacebuilding Organisations,” 3.

<sup>111</sup> Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*; Fast, “Mind the Gap: Documenting and Explaining Violence Against Aid Workers.”

<sup>112</sup> Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*, 2.

<sup>113</sup> Fast, “Security and Risk Management for Peacebuilding Organisations,” 3.

<sup>114</sup> Fast, 3.

<sup>115</sup> Rowley, Burns, and Burnham, “Research Review of Nongovernmental Organizations’ Security Policies for Humanitarian Programs in War, Conflict, and Postconflict Environments.”

<sup>116</sup> Rowley, Burns, and Burnham, 242–46.



## Surveying Practitioners: Educational-Training Materials

### Research Design

Following the formal review of the academic literature, the research team began a systemic review of the educational-training materials we were able to locate. In order to do accomplish a field-wide survey, two research assistants collaborating with the direction of a principal investigator<sup>117</sup> and developed a list of relevant non-governmental and multi-national organizations. After this was accomplished, a standardized coding schema was developed and tested to organize data, responses, qualitative codes, and publication/citation information. Using this schema, the researchers sought to determine if organizations provided their constituency a method for understanding and evaluating risks, threats, and security.<sup>118</sup> Through these secondary qualitative evaluation points, researchers were able to create a clearer picture of the steps that organizations are taking, organizations' priorities in terms of safety and security, and the areas where these organizations can approve and solidify the security measures taken.<sup>119</sup> Additionally, nearly forty security-themed training materials were collected using open-source digital repositories and reviewed.<sup>120</sup>

---

<sup>117</sup> This portion of the study—surveying organizations and authoring research briefs—was conducted by Peyton Nielsen and Devin McCarthy, both undergraduate students at the University of Notre Dame, serving as research interns with the Better Evidence Project for the Summer 2021 term. Michael Loadenthal served as the principal investigator and guided the researchers through a series of recurring meetings, and integrated their findings to the second stage of this paper. Nielsen and McCarthy were also responsible for reviewing the majority of the inter-academic literature, and authoring this paper's literature review.

<sup>118</sup> A separate response rate findings table, restricted to exclude nonresponsive entities, is also included as Appendix 7: Findings Table Restricted to Responsive Organizations.

<sup>119</sup> The complete results of this survey, as well as the coding schema, including both responsive and unresponsive organizations are included as appendices to this paper.

<sup>120</sup> Exemplary guides for practitioners reviewed include, but are not limited to: InterAction, Working Group on NGO Security, "Report of the Working Group on NGO Security Training Curriculum" (Washington, DC: InterAction, 1997); Bickley, "SAFETY FIRST: A Safety and Security Handbook for Aid Workers"; Charles Rogers and Brian Sytsma, *A Shield About Me: Safety Awareness for World Vision Staff* (Monrovia, CA: World Vision, 1998); Mark Cutts and Alan Dingle, *Safety First: Protecting NGO Employees Who Work in Areas of Conflict (2nd Ed.)* (London, UK: Save the Children, 1998); David Lloyd Roberts, "Staying Alive: Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas" (Geneva: International Committee of the Red Cross, 2005 1999); Charles Rogers and Brian Sytsma, "World Vision Security Manual: Safety Awareness for Aid Workers" (Geneva: World Vision, 1999), <https://fmwm.org/wp-content/uploads/2016/02/WV-Security-Manual-amended.pdf>; Koenraad Van Brabant, "Mainstreaming the Organisational Management of Safety and Security," HPG report (London, UK: Overseas Development Institute, Humanitarian Policy Group, March 2001), <https://gisf.ngo/wp-content/uploads/2014/09/0598-Van-Brabant-2001-Mainstreaming-the-Organisational-Management-of-Safety-and-Security.pdf>; Katy Barnett, "Security Report for Humanitarian Organizations" (Brussels, BE: Directorate-General for Humanitarian Aid—ECHO, European Commission, 2004); Barney Mayhew, "Generic Security Guide for Humanitarian Organizations" (Brussels, BE: Directorate General for Humanitarian Aid - ECHO, European Commission, 2004); International Federation of the Red Cross and Red Crescent Societies, "Stay Safe: The International Federation's Guide to a Safer Mission" (Geneva: International Federation of the Red Cross and Red Crescent Societies, 2007), <https://media.ifrc.org/ifrc/wp-content/uploads/2018/03/Personal-SecurityENGLISH.pdf>; Humanitarian Practice Network, "Operational Security Management in Violent Environments (Revised Edition)" (London, UK: Overseas Development Institute, Humanitarian Practice Network, December 2010), <https://odihpn.org/resources/operational-security-management-in-violent-environments-revised-edition/>; Jan Egeland, Adele Harmer, and Abby Stoddard, "To Stay And Deliver: Good Practice for Humanitarians in Complex



Early in the research design we aimed for a collaborative and transparent approach, not knowing our expected rate of response. The team utilized a three-stage approach to locate relevant educational and training materials. Initially, the research team contacted 76 organizations.<sup>121</sup> This list was generated through a survey of relevant organizations in the field at large and *not* on the basis of where we were likely to find suitable materials. In order to locate security guides and other materials, the websites of these organizations were first reviewed. Second, additional materials were located through the use of open-source repositories such as Relief Web’s 885-item training archive.<sup>122</sup> When researchers were unable to locate relevant materials for a particular target organization, the organizations were contacted via email and/or phone.

### Methodology

Within the approach to qualitative coding employed, before excluding an organization as unresponsive, researchers utilized standardized search strings to locate materials hosted online. For example, using Google’s library of search operator functions,<sup>123</sup> researchers deployed queries such as:

SITE:icrc.org FILETYPE:PDF security AND safety OR risk\*

This string would return *only* PDF files (the most likely file type for organizational reports or guides), hosted on a given domain (in this case icrc.org), and featuring keyword combinations (in this case *security* and *safety*, or *security* and *risk/risks/risking...*). If these digital searches generated no useable results *and* the organization was unresponsive to email/phone outreach, it could be excluded from the final analysis.

Using this triple-method approach—website review, email/phone outreach, tailored searches—researchers *were* able to locate materials from dozens of organizations ranging from the late 1990s to the present. The universe of organizational materials was evaluated by the following three-pronged criteria for inclusion:

1. Are there available education-training materials (i.e., digital/PDF guides, slide decks, other print publications), produced by or for the benefit of organizations working

---

Security Environments,” Policy and Studies Series (New York, NY: Office for the Coordination of Humanitarian Affairs Policy Development and Studies Branch, 2011); Abby Stoddard, Adele Harmer, and Katherine Haver, “Safety and Security for National Humanitarian Workers,” Policy and Studies Series (New York, NY: Office for the Coordination of Humanitarian Affairs Policy Development and Studies Branch, 2011); Jones et al., “Managing the Security of Aid Workers with Diverse Profiles”; Geneva Centre for the Democratic Control of Armed Forces and The International Committee of the Red Cross, “Addressing Security and Human Rights Challenges in Complex Environments Toolkit (3rd Ed.)” (Geneva: DCAF/ICRC, 2016); Care International and Robert Macpherson, “Safety & Security Handbook” (Geneva: Care International, 2004); United Nations Office for the Coordination of Humanitarian Affairs, “United Nations Disaster Assessment and Coordination (7th Ed.),” UNDAC Field Handbook (Geneva: United Nations Office for the Coordination of Humanitarian Affairs, 2018).

<sup>121</sup> For a complete listing of the organizations contacted, see Appendix 3: Initial Respondent Pool

<sup>122</sup> For example, see: <https://reliefweb.int/training>.

<sup>123</sup> For more information, see: Moz, “Google Search Operators [2021 SEO],” Moz, 2021, <https://moz.com/learn/seo/search-operators>.

broadly in the fields of: conflict and violence prevention/intervention, human rights and security, peacekeeping, protective accompaniment, humanitarian and disaster relief, emergency medical services and other direct aid-related areas?

2. Are they from nonprofits, non-governmental organizations, and/or multinational organizations such as the various United Nations bodies, and including both secular and faith-based organizations?
3. Are the materials authored in English by US, international, or those organizations based in non-US countries?

In order for the materials to be evaluated, researchers required that the organization make materials available in English, and for the sake of relevancy, the organization must still be in operation at the time of investigation.

Using this approach and inclusion criteria, researchers located and reviewed 39 educational-training publications in a variety of forms.<sup>124</sup> Some of the materials reviewed were fully dedicated to safety and security, while others consisted of sections of reports, or larger training modules. Each guide was qualitatively coded by two researchers, and reviewed by a third, to capture publication information, contact information of the organization, and topics covered. Researchers additionally coded three qualitative measures of the guide:

1. Did the organization state that it was mandatory for its staff to read the material?
2. Did the material provide a framework for threat modeling and risk analysis?
3. Did the material discuss digital operational security (e.g., smartphone encryption, virtual private networks)?

In addition to basic information such as publication dates and page length, the organizations' *responsiveness* was also evaluated, marking those who were not reached as nonresponsive. When coding an organization's responsiveness, six values were used:

1. Unresponsive
2. Unresponsive, but materials exist/found
3. Unresponsive, but fairly certain materials exist<sup>125</sup>
4. Responsive, no materials exist
5. Responsive, materials exist but not provided<sup>126</sup>
6. Responsive, materials provided

Finally, beyond collecting, reviewing, and qualitatively coding the available training and educational materials, researchers selected five guides for secondary review, generating concise research briefs to summarize the publications' content and foci. These briefs were

---

<sup>124</sup> A complete listing of these publications, including hyperlinked backups of the materials reviewed, is included as Appendix 5: Guides, Reports, and Educational Training Materials Reviewed.

<sup>125</sup> This value was used when researchers found evidence of materials existing (e.g., mention of training or a safety guide in other educational materials), but the actual publication was not actually located.

<sup>126</sup> This value was used when organizations were responsive, but unable or unwilling to provide materials for privacy, safety, or other reasons.

written to provide succinct insights into the structure and recommendations of the guides that contained the most comprehensive risk assessment frameworks, the most extensive safety advice, and the widest variety of topics. Each brief abridges a guide and provides a summary of its recommendations, and are included at the conclusion of this paper as appendices.

## Findings

Through surveying 76 organizations, we found that 22% (17 organizations) provided their constituency with safety, security, and/or risk/threat assessment training, or were highly likely to do so. Our team was able to locate these materials from 14% of the widest sample. In our initial outreach, we contacted 72 organizations,<sup>127</sup> with a response rate of 12.5%. While some organizations were responsive to our inquiry and confirmed they provided such materials, others were unable or unwilling to provide the materials. In these cases, the reasons mentioned included a lack of physical documentation (e.g., training was conducted as in-person modules), and the intentional withholding and/or obfuscation of materials for safety and privacy reasons. In other cases, organizations were not responsive to our inquiry but referenced relevant materials on their website or other public materials. Detailed figures on response rates are included as part of Appendix 4: Field Survey Results.

When exploring the websites and publications of the various organizations being surveyed, it quickly became clear that determining which utilized a security posture meeting our definition was difficult, with most organizations remaining opaque regarding their training (likely a good security practice in and of itself), and others simply nonresponsive. Certainly, researchers were able to locate dozens of reports and guides which matched what we expected to find, and in seeking these out, researchers were able to learn that other organizations<sup>128</sup> have specially-developed “training curriculum for personal security and organizational security management,” some of which seeks to promote a “threat assessment” framework. Although not as widespread as initially imagines, many of the materials reviewed *did* include a framework for understanding and measuring risk, and these specially should be consulted for those looking to further understand risk, threat, and vulnerability analysis.<sup>129</sup>

Through this qualitative coding, we found that many guides were likely to be *mandatory* reading for staff. Although explicit reference to such a requirement was rarely stated, many written materials did mention that individuals should review safety materials before any field trips or travel into operational zones. From the materials which were surveyed, the vast majority (91%) provided *some* elements of a framework for risk assessment and threat

---

<sup>127</sup> Our team was also able to locate 4 additional organizational training-educational guides from entities we *did not* initially survey. These were included in the final analysis.

<sup>128</sup> According to Fast (2014, 180-181), these include portions of the UN such as UNOCHA, InterAction, the NGO Registry for Engineers in Disaster Relief, European Commission’s Humanitarian Aid and Civil Protection department, amongst others.

<sup>129</sup> For example, see: Care International and Macpherson, “Safety & Security Handbook”; Bickley, “SAFETY FIRST: A Safety and Security Handbook for Aid Workers”; Rogers and Sytsma, “World Vision Security Manual: Safety Awareness for Aid Workers”; International Federation of the Red Cross and Red Crescent Societies, “Stay Safe: The International Federation’s Guide to a Safer Mission (4th Ed.)”; Metcalfe, Martin, and Pantuliano, “Risk in Humanitarian Action: Towards a Common Approach?”; Frontline Defenders, “Workbook on Security: Practical Steps for Human Rights Defenders at Risk” (Dublin, Ireland: Frontline Defenders, 2011); Humanitarian Practice Network, “Operational Security Management in Violent Environments (Revised Edition).”

modeling, often dedicating sections to different strategies or security frameworks. These radically varied throughout the materials. While some publications briefly mentioned the notion of mapping threats and weighing risks, often restricted to a single paragraph or subsection, others delved more deeply into measuring risk, gaining situational awareness, and modeling threats for safety and security. Despite the frequent presence of such themes throughout the educational-training materials surveyed, few publications provided an agile or adaptable approach. Instead, many offer an approach which is temporally, locationally, and contextually-situated, and without frequent review and revision, are likely to be quickly outdated. While an overwhelming majority of the sampled materials provided a security framework, only 18% discussed *digital* operational security, seemingly one of the more pressing matters for contemporary practitioners. The guides that *did* consider this area did so by discussing computer and phone security and surveillance technology (e.g., encryption, password), although only briefly.

### Comparing Our Findings

In attempting to understand our paper within the realm of complementary explorations, we sought other field-wide assessments and evaluations. In the closet equivalent study located—a 2013 assessment of US, European, and Japanese NGOs—the researchers yielded “20 security manuals, 12 policy/guideline documents, and 5 sets of training materials”<sup>130</sup> from a wider pool of potential respondents. From a review of these materials, the author concluded that although “all of the NGOs [surveyed]...have some form of security *manual*,” not all of the organizations utilized a coherent security *policy*.<sup>131</sup> In their assessment, 90% (18 of 20) of the organizations surveyed utilized materials which incorporated “threat/risk assessment processes,” and 70% (14 of 20) included a “framework for determining acceptable and unacceptable risks to staff, assets, and image of organization.”<sup>132</sup>

On average 81% (16 of 20) contained conceptual or analytically-orientated approaches (e.g., risk assessment and management, threat intelligence) within their security materials.<sup>133</sup> This is a slightly lower figure than that established in the present study which could indicate a positive trend upward, though it could similarly be an outcome of a differentiated sampling approach. While Fast’s *Aid in Danger* concluded that NGO training materials “emphasize threat and risk assessment,”<sup>134</sup> in many of the samples surveyed, this did not appear to be the case. This may simply be a case of divergent standards by researchers. Our team sought materials where such an approach was a *focus*, yet the aforementioned study noted that instances which they coded in the affirmative (i.e., as having a security focus), would have been considered below our team’s threshold. To quote the study:

Eight of the 12 policy documents also reference security assessment. The guidelines, in general, contain a similar framework, with comparable concepts and definitions;

---

<sup>130</sup> Rowley, Burns, and Burnham, “Research Review of Nongovernmental Organizations’ Security Policies for Humanitarian Programs in War, Conflict, and Postconflict Environments,” 242–43.

<sup>131</sup> Rowley, Burns, and Burnham, 243 Emphasis added.

<sup>132</sup> Rowley, Burns, and Burnham, 244.

<sup>133</sup> Based on calculations using the figures in Table 3 Rowley, Burns, and Burnham, 244.

<sup>134</sup> Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*, 180.

however, they range in level of guidance from a few sentences or paragraphs covering definitions, concepts, and formulas, to several pages focusing on the purpose of each assessment, including guidelines, checklists, matrices, graphs, and worksheets. Of the 18 security manuals that cover security assessments, 3 provide relatively low detail, 7 provide well-developed detail, and the rest fall between these boundaries.<sup>135</sup>

This key distinction should not be overlooked. In *our* assessment “a few sentences or paragraphs” focused on a security-centered framework would not warrant distinction. Instead, our assessment and Rowley, et. al.’s agree that many materials offer more of a *proscription* for security rather than a framework to develop the cure on one’s own.

Despite being unable to locate some of the guides and training resources in their complete form (i.e., only locating brief descriptions, or excerpts), it appears as if many organizations *do* see assessing security a primary concern, even if they do not promote a particular framework for practitioners to adopt.<sup>136</sup> Reconciling these findings with those of Rowley, et. al.’s study, we can conclude that what the authors consider “conceptual/analytical-orientated security management subcomponents” still function more akin to security *directives* than agile, contextually-situated approaches to which seek to tailor security to one’s unique environment. Moreover, both Rowley et. al.’s survey and our own conclude that the seeming absence of readily available security training materials appears to be less a product of organizations failing to consider security, and more the result of a fractured, “ad hoc approaches to security.”<sup>137</sup>

## Future Directions

Future focus on safety, security, and risk should help to move the conversation from the identification of *insecurity* to the promotion of embodied security in practice. To this end, future research should prioritize the development of tools suited for field implementation, including the articulation of those specially-tailored for risk analysis, and intersectional threat modeling. These tools can include those noted within this paper such as mind maps, risk matrices, SWOT analyses, user archetype mapping, and security product reviews.

In developing these tool sets in conjunction with the findings of this paper, a multi-month educational-training curriculum could include the following four stages for preliminary foci:

1. Hosting focus groups comprised of community stakeholders to provide feedback on this report and its findings.
2. Developing and circulating a tool-based analytical framework for developing tailored risk analyses and threat models for practitioners.
3. Hosting preliminary workshops where practitioners can learn about tool sets and ‘field test’ them in safer, controlled (i.e., simulated) environments.

---

<sup>135</sup> Rowley, Burns, and Burnham, “Research Review of Nongovernmental Organizations’ Security Policies for Humanitarian Programs in War, Conflict, and Postconflict Environments,” 245.

<sup>136</sup> Fast, *Aid In Danger: The Perils and Promise of Humanitarianism*, 179–80.

<sup>137</sup> Rowley, Burns, and Burnham, “Research Review of Nongovernmental Organizations’ Security Policies for Humanitarian Programs in War, Conflict, and Postconflict Environments,” 248.

4. Hosting secondary workshops where practitioners attempt to apply the tool sets developed, providing feedback for further refinement.

The abovementioned approach can help to develop the stakeholder community of practitioners by utilizing a community approach to provide feedback, offer peer review, review subsequent iterations, and eventually, field test. This approach has already begun with the formation of a post-report working group, organized by the Better Evidence Project. The first stage of this working group will be to review and provide feedback on the present paper, and to engage our stakeholders to help curate and promote a growing community of engaged scholar-practitioners.

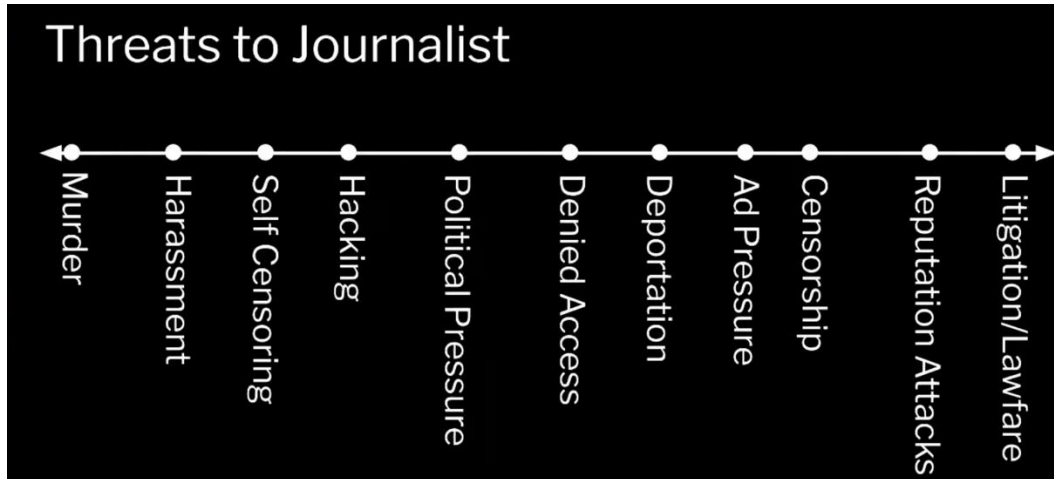
## Conclusion

Following a multi-method investigation of safety, security, risk, and danger facing conflict practitioners, several trends are quite apparent. Practitioners are under threat—likely increasing threat—and the wider community of engaged scholars, activists, workers and policy makers are *more* focused on documenting this trend than promoting ameliorations. This may be due to the fact that while the dangers share a great degree of commonality, their mitigations are uniquely situational, deeply contextual, and as fluid as their changing environments. This is precisely why this paper has advocated for a *framework* rather than a set of pointers. While our community should be thankful to the many thinkers who have developed security-themed mitigation checklists, what about when the threat environment changes, the local conflict morphs, or technology outpaces the materials? It is a forgone conclusion that anything written dealing with technology is outdated nearly before it is read, so keeping up on the treadmill of risk-attack-solution-risk is a near impossibility. Perhaps the goal of providing field-wide security guidance is faulty from its conception, and while the present examination has sought to promote a flexible, and nimble framework rather than a blueprint, this too may be difficult given the varied needs of those in the field.

The task for those deployed in the field, as well as those whom advise, direct, and provide support, should be to maximize engagement, reduce violence, and promote a moral peace, while reducing or ideally eliminating risks to the individuals' safety and security. In order for such an aim to become a reality, our goals should begin from *understanding* our security posture, its aims, and its limitations. This will inherently be a tailored and temporal assessment, but through repetition, can become more routine. Security architects often remark that the best means are those that are unobtrusive, and those which do not diminish useability for the practitioner. In this manner, our security aims should be the elimination of unnecessary danger while simultaneously not burdening the individual with awkward procedures and mitigations. Embracing the tenants of harm reduction—beginning with the acknowledgement that risk and danger are ever-present realities unable to be solutioned away—we can work to reduce risk and increase security, so that individuals and their organizational sponsors can continue to promote a more just world of decreasing violence, expanding freedoms, and the flourishing of justice.

## Appendices

### Appendix 1: 'Threat to journalist' continuum (NYT) <sup>138</sup>



<sup>138</sup> DEF CON 29 - A Look inside Security at the New York Times or A Media Security Primer for Hackers, Streaming video hosted by Youtube, Def Con 29, 2021, pt. 17:16-21:46, [https://www.youtube.com/watch?v=U2-8MNx8nsg&ab\\_channel=DEFCONConference](https://www.youtube.com/watch?v=U2-8MNx8nsg&ab_channel=DEFCONConference).

## Appendix 2: Risk, Danger, and Threat Mind Map for Conflict Practitioners (Loadenthal)



This risk, dangers, and threats mind map was developed by Michael Loadenthal, and subsequently reviewed by numerous field-based practitioners who provided feedback and additions. These practitioners included individuals involved in conflict zone protective accompaniment, legal services to marginalized communities, anti-pipeline direct action campaigns, electronic security education, and individuals working in diplomatic and post-conflict peacekeeping operations.



### Appendix 3: Initial Respondent Pool

1. Action Against Hunger
2. Action Aid
3. Action on Armed Violence
4. Active Learning Network for Accountability and Performance (ALNAP)
5. Adventist Development and Relief Agency International
6. African Centre for the Constructive Resolution of Disputes
7. Alliance for International Medical Action
8. Americares
9. Amnesty International
10. Berghof Foundation
11. CARE International
12. Caritas Internationalis
13. Catholic Relief Services
14. Children of War Foundation
15. Concern Worldwide USA
16. Conflict Dynamics International
17. Cordaid
18. Corus International
19. Danish Refugee Council
20. Direct Relief International
21. Doctors of the World
22. Doctors' Without Borders
23. Food and Agriculture Organization of the United Nations (FAO)
24. Frontline Defenders
25. Geneva Call
26. GlobalMedic
27. GOAL
28. Human Rights Watch
29. International Campaign to Abolish Nuclear Weapons (ICAN)
30. International Committee of the Red Cross/Red Crescent
31. International Crisis Group
32. International Medical Corps
33. International Organization for Migration (IOM)
34. International Rescue Committee
35. INTERSOS
36. Iraqi Christian Relief Council
37. Keeping Children Safe
38. Kvinna Till Kvinna
39. Lutheran World Relief
40. MapAction
41. Medair
42. Mercy Corps
43. Migrant Offshore Aid Station
44. Mines Advisory Group
45. Muslim Hands
46. Norwegian Refugee Council
47. Ockenden International
48. Operation USA
49. Oxfam International
50. Plan International
51. Real Medicine Foundation
52. Refugees International
53. Samaritan's Purse
54. Save the Children
55. Shelter Now
56. ShelterBox
57. SOS Children Villages International
58. Team Rubicon
59. Tearfund
60. TECHO/Un Techo para mi País
61. Terre des Hommes
62. The Borgen Project
63. The Islamic Relief
64. United Methodist Committee on Relief
65. United Nations Children's Fund (UNICEF)
66. United Nations Development Programme (UNDP)
67. United Nations High Commissioner for Refugees (UNHCR)
68. United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA)
69. United Nations Relief and Works Agency (UNRWA)
70. War Child
71. Women's Refugee Commission
72. World Central Kitchen
73. World Concern
74. World Food Programme
75. World Health Organization
76. World Vision International

## Appendix 4: Field Survey Results

KEY & STATS			
Unresponsive, no materials located	48		
Unresponsive, but materials exist/found	5		
Unresponsive, but fairly certain materials exist	10		
Unresponsive in total	63		
Responsive, no materials exist	7		
Responsive, materials exist but not provided	2		
Responsive, materials provided	0		
Responsive in total	9	Response rate	12.5%
Did not contact (N/A) — YES/NO was found through research online	5	Total # of orgs. surveyed	76
Materials exist/fairly certain they do although we may not have all of them	17	% of orgs. sampled with guides	22.1%
Number of guides located	11	% of orgs. sampled with located guides	14.3%

## Appendix 5: Guides, Reports, and Educational Training Materials Reviewed

1. [“NGOs and Risk”](#) by Abby Stoddard, Katherine Haver, and Monica Czwarno
2. [“Safety and Security Handbook”](#) by Care International
3. [“NGO Safety and Security Training Project”](#) by Christine Persaud
4. [“Safety and Security Incident Information Management”](#) by Cornerstone on Demand Foundation
5. [“Protecting the Protectors: Strengthening the Security of NGOs in Conflict Zones”](#) by Daniela Irrera
6. [“Staying Alive”](#) by David Lloyd Roberts
7. [“Addressing Security and Human Rights Challenges in Complex Environments”](#) by DCAF and the International Committee of the Red Cross
8. [“Operating in Insecure Environments”](#) by Department for International Development
9. [“Security Incident Information Management Handbook”](#) by EISF
10. [“Workbook on Security: practical steps for human rights defenders at risk”](#) by Front Line Defenders
11. [“Research Review of Nongovernmental Organizations’ Security Policies for Humanitarian Programs in War, Conflict, and Postconflict Environments”](#) by Elizabeth Rowley, Lauren Burns, and Gilbert Burnham
12. [“Aid Worker Security Report 2020”](#) by Humanitarian Outcomes
13. [“Mainstreaming the Organisational Management of Safety and Security”](#) by Humanitarian Policy Group
14. [“Operational Security Management in Violent Environments”](#) by Humanitarian Policy Group
15. [“Risk in Humanitarian Action: towards a common approach?”](#) by Humanitarian Policy Group
16. [“Operational Guidance to Establish and Enhance the Protection of Women Peacebuilders”](#) by ICAN
17. [“Stay Safe: The International Federation’s guide for security managers”](#) by the International Federation of Red Cross and Red Crescent Societies
18. [“Stay Safe: The International Federation’s guide to a safer mission”](#) by the International Federation of Red Cross and Red Crescent Societies
19. [“Volunteers, Stay Safe!”](#) by the International Federation of Red Cross and Red Crescent Societies

20. [“NGO INSECURITY IN HIGH RISK CONFLICT ZONES”](#) by John F. Mitchell
21. [“Understanding Attacks on Humanitarian Aid Workers”](#) by Kristian Hoelscher, Jason Miklian, and Havard Mokliev Nygard
22. *Aid in Danger* by Larissa Fast<sup>139</sup>
23. [“Mind the gap: Documenting and explaining violence against aid workers”](#) by Larissa Fast
24. [“A Reflexive Approach to Risk and Intervention for Third-Party Intervenors”](#) by Larissa Fast
25. [“Security and Risk Management for Peacebuilding Organisations”](#) by Larissa Fast
26. [“Final Report Security Perceptions Survey”](#) by Larissa Fast and Dawn Wiest
27. [“The promise of acceptance as an NGO security management approach”](#) by Larissa Fast, Faith Freeman, Michael O’Neill, and Elizabeth Rowley
28. [“Protecting Women Peacebuilders: the front lines of sustainable peace”](#) by Melinda Holmes
29. [“Project Cycle Management and Counterterrorism Risks”](#) by Norwegian Refugee Council
30. [“To Stay and Deliver”](#) by OCHA
31. [“Annex I to ‘To Stay and Deliver’”](#) by OCHA
32. [“United Nations Disaster Assessment and Coordination”](#) by OCHA
33. [“Berkeley Protocol on Digital Open Source Investigations”](#) by OHCHR
34. [“Safety First: a safety and security handbook for aid workers”](#) by Save the Children
35. [“Alternative Community Security: Initiatives and Stories”](#) by Shanti Sena Network and Nonviolence International
36. *Death Threats and Violence* by Stephen J. Morewitz<sup>140</sup>
37. [“Security in the Field: Information for staff members of the United Nations system”](#) by the United Nations
38. [“Rapid Risk Assessment of Acute Public Health Events”](#) by the World Health Organization
39. [“WorldVision Security Manual”](#) by WorldVision

---

<sup>139</sup> A copy of this publication is not provided as it is a full-length book.

<sup>140</sup> A copy of this publication is not provided as it is a full-length book.

## Appendix 6: Complete Coding Table for Responsive Organizations

ORGANIZATION	Response?	Guide Located	Date 1st published	Date last updated	page count	Reading Mandatory?	Framework provided for threat modeling?	Digital OPSEC discussed?	Abbreviated list of topics covered	Contact info	Website
Acme Corp	responsive	YES	2005	2010	30	YES/No/unknown/ N/A	YES (section: how to measure risk & situational awareness)	YES (page 3)	digital security, preventing kidnapping, situational awareness, how to measure risk	Admin@acme.com	<a href="http://acme.com">http://acme.com</a>
Bell Inc.	responsive, no guide	NO	N/A	N/A	N/A	N/A				no one contacted	<a href="http://bell.com">http://bell.com</a>
International Committee of the Red Cross/Red Crescent	Unresponsive, but materials exist	YES	2012	2012	55	Unknown	YES (section: mapping the security situation at branch level)	No	Road safety, personal health, managing stress, disaster safety	Emailed through website, 41 22 734 60 01	<a href="http://www.icrc.org">International Committee of the Red Cross (icrc.org)</a>
CARE International	Unresponsive, but materials exist	YES	2004	2004	158	Unknown	YES	No	Site management, travel safety, medical emergencies, assault, bombings, kidnappings	cisecretariat@careinternational.org	<a href="http://www.care-international.org">Home Page: I Care International (care-international.org)</a>
World Vision International	Unresponsive, but materials exist	YES	1998	1999	148	Unknown	YES	No	Security awareness, hostage situations, shootings, site management, communications	illian_omarib@wvi.org	<a href="http://www.wvi.org">Homepage: I World Vision International (wvi.org)</a>
Save the Children	Unresponsive, but materials exist	YES	2003	2010	210	Unknown	YES	No	Personal security awareness, medical emergencies, travel safety, natural disasters, armed robbery	supportercare@savechildren.org	<a href="http://www.savechildren.org">Humanitarian Aid Organization for Children (Save the Children)</a>
INTERSOS	Unresponsive, but fairly certain materials exist	YES	N/A	N/A	N/A	Unknown	Unknown	Unknown	Training course that includes a section on security, topics covered unknown	intersos@intersos.org	<a href="http://www.intersos.org">Homepage: I INTERSOS</a>
International Medical Corps	Unresponsive, but fairly certain materials exist	YES	Unknown	Unknown	N/A	Unknown	Unknown	Unknown	Unknown	inquiry@internationalmedicalcorps.org	<a href="http://www.internationalmedicalcorps.org">International Medical Corps: First there, no matter where</a>
Norwegian Refugee Council	Responsive, materials exist but were not provided	YES, and HEAT security training course	Unknown	Unknown	12	Unknown	No	No	Kidnappings, bombing, counterterrorism, armed violence	nrc@nrc.no	<a href="http://www.nrc.no">NRC</a>
SOS Children Villages International	Responsive, no materials exist	NO	N/A	N/A	N/A	N/A	N/A	N/A	N/A	info@sos-usa.org	<a href="http://www.sos-usa.org/">https://www.sos-usa.org/</a>
UNOCHA	N/A	YES	unknown - 5th ed in 2000	2018	272	unknown	pg 91? - UN goes over Security Risk Management model	no	Tenets of humanitarian response, safety and security, assessment and analysis	no one contacted	<a href="http://www.unocha.org/sites/unocha/files/1823826E_v eb_pages.pdf">https://www.unocha.org/sites/unocha/files/1823826E_v eb_pages.pdf</a>
UNHCR	Unresponsive, but fairly certain materials exist	reports found talking about improving safety of staff/aid workers, but no mention of an actual guide								USAWA@UNHCR.ORG	<a href="http://www.unhcr.org">https://www.unhcr.org</a>
World Health Organization	N/A	yes	2012	2012	44	unknown	yes	no	risk assessment, risk communication, control measures	no one contacted	<a href="http://www.who.int">www.who.int</a>
Americares	Responsive, materials exist but were not provided	YES								info@americares.org	<a href="http://www.americares.org">Americares: I Disaster Relief &amp; Global Health Organization</a>
MapAction	Unresponsive, but fairly certain materials exist	YES	Unknown	Unknown	N/A	YES	Unknown	Unknown	Unknown	training@mapaction.org	<a href="http://www.mapaction.org">MapAction - The humanitarian mapping charity</a>
Tearfund	Responsive, no materials exist	NO	N/A	N/A	N/A	N/A				info@tearfund.org	<a href="http://www.tearfund.org">Tearfund</a>
Medair	Responsive, no materials exist	Has one day of security training as well as on-demand additional training, but no guide								info@medair.org	<a href="http://www.medair.org">Home (medair.org)</a>
UNDP	Unresponsive, but fairly certain materials exist								Several documents cover risk assessment but are not specific to the organization's workers	undp.washington@undp.org	<a href="http://www.undp.org">UNDP: I United Nations Development Programme</a>
Ockenden International	Responsive, no materials exist	NO	N/A	N/A	N/A	N/A				enquiries@ockendenprizes.org	<a href="http://www.ockendenprizes.org">Home - Ockenden International (ockendenprizes.org)</a>
GOAL	Unresponsive, but fairly certain materials exist								Safety and risk assessment measures exist but are not specified	info@goal.ie	<a href="http://www.goal.ie">Homepage: - GOAL Global</a>

ORGANIZATION	Response?	Guide Located	Date 1st published	Date last updated	page count	Reading Mandatory?	Framework provided for threat modeling?	Digital OPSEC discussed?	Abbreviated list of topics covered	Contact info	Website
Kvinna Till Kvinna	Unresponsive, but fairly certain materials exist	YES	Unknown	Unknown	N/A	YES	YES	YES	Criminal acts, surveillance, digital threats, legal environment, attitudes and beliefs	info@kvinnatillkvinna.se	<a href="https://kvinnatillkvinna.org/">https://kvinnatillkvinna.org/</a>
Action on Armed Violence	Responsive, no materials exist	NO	N/A	N/A	N/A	N/A				loverton@aoav.org.uk	<a href="https://www.actiononarmedviolence.org/">Action on Armed Violence   AOAV</a>
Danish Refugee Council	Unresponsive, but materials exist	HEAT Security Training Course ( <a href="https://drc.ngo/our-work/resources/heat-and-re-heat/">https://drc.ngo/our-work/resources/heat-and-re-heat/</a> )	N/A	N/A	N/A	No	Unknown	Unknown	Mine risk education, negotiations, vehicle safety, first aid, conflict survival	drc@drc.ngo	<a href="https://www.drc.org.uk/">DRC   Danish Refugee Council</a>
Plan International	Responsive, no materials exist	NO, but provide online security training course that we have (it includes five modules, and a short video on situational awareness)	N/A	N/A	N/A	N/A	N/A	N/A		emailed thru website	<a href="https://plan-international.org/">https://plan-international.org/</a>
Samaritan's Purse	Unresponsive, but fairly certain materials exist	unsure, found <a href="#">this</a> in regards to safety but does not include the threats we seem to want to address								emailed thru website	<a href="https://www.samaritanspurse.org/">https://www.samaritanspurse.org</a>
Operation USA	Responsive, no materials exist	NO	N/A	N/A	N/A	N/A	N/A	N/A	N/A	info@opus.org	<a href="https://www.opusa.org/">https://www.opusa.org/</a>
IOM	Unresponsive, but fairly certain materials exist	talk of security training/guides in an HR report, so assuming yes								info@iom.int hq@iom.int	<a href="https://www.iom.int/">https://www.iom.int/</a>
FAO	Unresponsive, but fairly certain materials exist	mention of security training in reports but no guide								FAO-HQ@fao.org	<a href="http://www.fao.org/home/en/">http://www.fao.org/home/en/</a>
IFRC	N/A	YES		2013	216	unknown	YES (ch 1: security framework)	no	security framework, personal security, vehicle safety and security, field movement, health, communication, natural disasters, dangerous situations	N/A	N/A
Front Line Defenders	N/A	YES		2011	109	unknown	YES (ch 3: analyzing threats)	yes p 88-90	assessing risk, analyzing threats, wellbeing and stress, creating security plans. checklists in appendices includes things such as abduction, demonstrations, assault, ect.	N/A	<a href="https://www.frontlinedefenders.org/">https://www.frontlinedefenders.org/</a>

## Appendix 7: Findings Table Restricted to Responsive Organizations

KEY & STATS			
Unresponsive	0		
Unresponsive, but materials exist/found	5		
Unresponsive, but fairly certain materials exist	10		
Unresponsive in total	15		
Responsive, no materials exist	7		
Responsive, materials exists but not provided	2		
Responsive, materials provided	0		
Responsive in total	9	<b>Response rate</b>	37.50%
		Total # of orgs. contacted	24
Did not contact (N/A) — yes/no found online	4	Total # of orgs. sampled	28
		<b>% of orgs. sampled with located guides</b>	
Number of guides found	14		50.00%

## Appendix 8: Research Brief #1

Frontline Defenders. “Workbook on Security: Practical Steps for Human Rights Defenders at Risk.” Dublin, Ireland: Frontline Defenders, 2011.

### Summary

“Human rights defenders need new strategies that are inspired by a theory of security and human rights, of dignity, freedom and justice. This Workbook, created with a view to protecting human rights defenders, is aimed at them...It aims to draw attention to specific situations arising from the activities carried out by human rights defenders, to prepare them to deal with the inconveniences, unexpected risks, threats and security incidents they may meet. It also seeks to prevent these situations and to deal with stress and insecurity.”<sup>141</sup>

### Topics covered

- 1) security planning regarding environment and identity
- 2) collective security planning and communication
- 3) creating security plans
- 4) aid workers’ wellbeing and stress
- 5) understanding the situational context

The organization Frontline Defenders developed *Workbook on Security: Practical Steps for Human Rights Defenders at Risk* (2011) with the goals of allowing for a strong overview of the risks faced by Human Rights Defenders (HRDs), the definitions of security and safety, and the steps necessary for HRDs to stay safe in operational zones. Frontline Defenders define HDRs “are those who work non-violently on behalf of others for any or all of the rights enshrined in the Universal Declaration of Human Rights. This includes those who work for civil and political rights, social, economic, environmental and cultural rights, and the right to equality, such as those working for women’s rights and Lesbian, Gay, Bisexual, Transgender and Intersex (LGBTI) rights. For example, a group running a legal aid clinic, an organization that supports sexual assault survivors, or those working for labor rights in disadvantaged communities. This guide is not solely for the people employed by Frontline Defenders, but for HDRs across all organizations, although general advice is rarely applicable to all HDRs under threat around the globe.

### Recommendations

1. **Produce a Security Plan Practical for the Environment & Identity:** These steps include context analysis, assessing risk, analyzing threats, producing security plans, and implementing and reviewing plans. When addressing risk assessment, the workbook integrates how one’s identity, profile, activities, and location may affect levels of insecurity, namely for female and LGBTI HDRs and those working in areas with fewer resources.
2. **Create Security Plans Collaboratively:** There are three different security strategies: the acceptance strategy, the protection strategy, and the deterrence strategy. It is most secure

---

<sup>141</sup> Frontline Defenders, “Workbook on Security: Practical Steps for Human Rights Defenders at Risk,” ii.



for an organization to have a security plan discussed and agreed upon collectively. Although each HDR will have unique attributes that can determine risk levels (such as gender, sexual orientation, age, etc.), individuals will generally make better security plans when drawing on the different experiences and perspectives of different members of the group.

3. **Maintain Mental Security & Wellbeing:** The lifestyle of an HDRs is inherently stressful. Identifying symptoms and causes of stress within one's environment is important to maintain physical security. Keeping a balanced diet, regular exercise and adequate amounts of relaxation and sleep are vital.
4. **Understand Your Context:** During the planning period, discuss with colleagues' aspects of insecurity in the environment to analyze the security situation. Share how to access influential contacts, known threats in the area, or cultural norms.
5. **Have a Plan for Common Threats to HDRs and Aid Organizations:** Common insecurities to aid workers include office and home security, demonstrations, detention, arrest, and abduction, defamation, and digital security. By providing adjustable securities plans (changed for other risks/threats faced given the environment), organizations can provide strong outlines for frequent risks.

*Research brief authored by Peyton Nielsen*

## Appendix 9: Research Brief #2

International Federation of the Red Cross and Red Crescent Societies. “Stay Safe: The International Federation’s Guide to a Safer Mission (4th Ed.).” Geneva: International Federation of the Red Cross and Red Crescent Societies, 2013. <https://media.ifrc.org/ifrc/wp-content/uploads/2018/03/Personal-SecurityENGLISH.pdf>.

### Summary

“Although the degree of risk varies from country to country, it is important to understand that security incidents can occur in all operational areas. Worryingly, a rising number and range of threats are being faced every day by humanitarian workers throughout the world, increasing their personal vulnerability. To fulfill their humanitarian mission, Red Cross and Red Crescent personnel must always follow basic security rules and act appropriately in any given situation”<sup>142</sup>

“Security starts with the individual. To achieve maximum security and safety, delegates and staff have to maintain a certain level of security awareness.”<sup>143</sup>

The International Federation of Red Cross and Red Crescent Societies outlined four goals in their guide *Stay Safe*:

- 1) to reduce the number of deaths, injuries, and impacts from disasters,
- 2) reduce the number of deaths, illnesses, and impact from diseases and other public health emergencies,
- 3) increase local community, civil societies, and Red Cross Red Crescent ability to address the most urgent situations of vulnerability, and
- 4) promote respect for diversity and human dignity, and reduce tolerance, discrimination, and social exclusion.

Along with this, the guide maintains priorities in advocating for the vulnerable in both those affected by disasters and public health emergencies and advancements in humanitarian issues, while covering issues of personal security for the humanitarian aid workers of the organization. The safety guide covers a large area in regards of personal security, including natural disasters, cultural sensitivity, vehicle safety, fire safety, health risks (physical and mental), hostage situations, and sexual assault. As the International Federation works in areas riddled with natural disasters and convoluted sociopolitical environments, human operations often face rapid and unprecedented change, increasing security risks for humanitarian workers. As there is

---

<sup>142</sup> International Federation of the Red Cross and Red Crescent Societies, “Stay Safe: The International Federation’s Guide to a Safer Mission (4th Ed.),” 11.

<sup>143</sup> International Federation of the Red Cross and Red Crescent Societies, 12.

a rising number of threats and risks for these workers across operational areas, International Federation employees are *required* to follow basic security rules that are outlined in this guide

### Topics covered

- |  |                                      |
|--|--------------------------------------|
| 1) multi-dimensional security frameworks | 7) safety while traveling            |
| 2) minimum security requirements         | 8) field trip planning               |
| 3) mission pillars                       | 9) residential and office safety     |
| 4) compound security plans               | 10) communication systems            |
| 5) roles and responsibilities            | 11) physical and mental health risks |
| 6) contextual insecurity and awareness   | 12) natural disasters.               |

### Recommendations

1. **Address Security as Multi-dimensional:** Organizations must have a multi-layered security framework, working inwards from strategic security to operational security and then placing individual security at the core. This layered model of security is mutually supportive, strengthening operational safety.
2. **Establish Minimum Security Requirements:** Outline the minimum criteria and procedures required to ensure that the organization is fulfilling its responsibilities to create a maximally safe and secure operational environment, while at the same time enabling its humanitarian mandate to be achieved. This may include personal conduct, training and preparation, security management, regulations, and contingency planning, security phases, critical incident management, field movement control, and finance.
3. **Maintain Universal Pillars of the Organization's Mission:** Have applicable pillars deal with political an operational acceptance, establish an effective mission, and maintain security of the aid workers. The Federation's pillars are acceptance, identification, information, regulations, behavior, communication, and protection.
4. **Have Effective and Compound Security Plans:** A functional security plan is often not one single document. It typical consists of security strategies, security regulations, contingency plans, operational security phases, security guidelines and advice, welcome pack, security briefings and debriefings, and critical incident management plan.
5. **Define Roles and Responsibilities:** Defining the roles which each team member is expected to fulfill creates a more effective security management system.
6. **Be Aware of Contextual Insecurity:** There are several factors increasing insecurity around the globe for aid workers, such as the nature of arm conflict, lack of respect for the mission, no code of conduct, and natural disasters. Be aware of constantly changing surroundings and the increase of security risks.
7. **Be Prepared and Attentive While Traveling:** Be adequately packed, research the operational area traveling to check the health requirements of the area, and register with

the national embassy of the state. When traveling, be aware of surroundings and security risks and do not lose sight of personal belongings and luggage.

8. **Plan for Field Trips:** Planning for a field trip minimizes the risk in security. This includes knowing the exact route you will travel, possible locations for an overnight stay, the weather condition, security information (understand the local situation including potential threats), local road conditions, the presence of checkpoints and other organizations operating in the area and being aware of your surroundings during any field movements. If there is any uncertainty about maintain adequate security of the trip, it should be terminated or postponed.
9. **Consider Residential and Office Safety:** Have strong perimeters, exterior lighting, heavy-duty doors and locks, an internal safe haven, fire and safety equipment, and an alarm system to maintain safety and security from intruders.
10. **Have an Effective Communication System:** The efficient use of these systems facilitates access to information and allows for a proper overview of a situation and rapid reaction when needed.
11. **Understand Both Physical and Mental Health Risks of the Operational Zone:** This may include diseases, natural disasters, war, or cumulative stress. Take necessary precautions such as immunizations, adequate preparation, and an end-of-mission physical. Moreover, maintaining proper hygiene, a balanced diet, proper hydration, awareness of sun exposure, and cognizance of insect or animal bites, injuries, and burnout symptoms, and maintaining stress management is essential.
12. **Have a General Plan for Natural Disasters:** Having plans for before, during, and after the disaster ensures that everyone on the team is taking the proper precautions. Construct plans for occurrences such as earthquakes, floods, mudslides, hurricanes, cyclones, and volcanic eruptions.

*Research brief authored by Peyton Nielsen*

## Appendix 10: Research Brief #3

Bickley, Shaun. "SAFETY FIRST: A Safety and Security Handbook for Aid Workers." London, UK: Save the Children, 2010.

### Summary

"Around the world, humanitarian workers are being targeted as never before. According to the UN, international aid work has now become one of the world's most hazardous professions."<sup>144</sup>

"Much of what is written here is basic common sense. Safety First provides useful reminders and easy-reference chapters to be consulted as safety and security issues arise. Not only is this book essential reading for staff about to take up their first field positions, it should be kept to hand as an indispensable reference for even the most seasoned aid worker. Safety First is one tool in a wider toolkit of material that is available in the humanitarian sector for managing and reducing safety and security risks."<sup>145</sup>

### Topics covered

- |  |                                     |
|--|-------------------------------------|
| 1) basic principles of managing security | 7) field communications             |
| 2) personal security awareness           | 8) natural hazards and disasters    |
| 3) staying healthy                       | 9) dealing with security threats    |
| 4) working in conflict environments      | 10) relocating and evacuating staff |
| 5) site safety and security              | 11) incident monitoring             |
| 6) travel safety and security            | 12) information management          |

The organization Save the Children created *Safety First: A Safety and Security Handbook for Aid Workers* (2010) in response to the increasing levels of hostility and violence that aid workers have been facing. The guidebook is a collection of the information and experience gained by aid workers in dangerous and challenging locations. *Safety First* is designed to provide Save the Children's staff with practical advice in order to reduce their risk exposure. It was originally written in 1995, then rewritten in 2003 to reflect changes in the approaches of international non-governmental organizations. The 2010 version has been further updated to reflect modern safety and security challenges. While the organization designed the guidebook with their own staff in mind, *Safety First* could serve as a valuable resource for all humanitarian aid workers.

### Recommendations

1. **Utilize a Security Management Framework:** Divide the safety and security management process into assessment, planning, implementation, monitoring, and reviewing components so that it is well-structured and organized.

---

<sup>144</sup> Bickley, "SAFETY FIRST: A Safety and Security Handbook for Aid Workers," 1.

<sup>145</sup> Bickley, 4.

2. **Build Relationships:** Develop a positive rapport with the people you work with so that they will warn you of and protect you from potential risks.
3. **Have a Plan in Place for Medical Emergencies:** Create a procedure for medical crises that includes information on local healthcare institutions, the nearest hospital of international standard, and air access points in the event of medical evacuations.
4. **Understand the Conflict Environment:** Research key groups and actors so that you can identify who you are dealing with and respect their chain of command.
5. **Select Sites Strategically:** Maintain a proper balance between physical protection and appearance. Security measures should keep you safe, but aggressive measures risk alienating you from the local community.
6. **Prepare For All Travel:** Learn about the routes, plan for delays, keep vehicles in good condition, and avoid routines in dangerous areas in order to stay safe while traveling.
7. **Choose the Right Communication System:** Consider operational needs, local regulations, and surrounding terrain when selecting a means of communication.
8. **Prepare for Natural Disasters:** Understand what natural hazards are most common in the region and plan how to respond before, during, and after events.
9. **Gather Information About Potential Threats:** Enquire about potentially dangerous locations and proper procedures for dealing with security threats in the region.
10. **Know When to Withdraw:** If staff are being exposed to unreasonable risk, humanitarian agencies are being targeted, local or international authorities recommend departure, and/or there is an immediate threat in the area, staff should consider either relocating or evacuating.
11. **Have an Incident Reporting System:** Staff should be able to provide their managers or base with immediate incident reports, and once there is time, formal incident reports that convey all necessary details. Additionally, agencies should maintain an incident log where all reports are stored so they are able to monitor incident trends and prevent further incidents.
12. **Share Information:** Disseminate safety and security information to all staff so that they are aware of all threats and can properly respond to incidents. Frequent staff meetings are also important so that staff are able to raise security concerns and provide their fellow agency members with updates and new information.

*Research brief authored by Devin McCarthy*

## Appendix 11: Research Brief #4

Rogers, Charles, and Brian Sytsma. "World Vision Security Manual: Safety Awareness for Aid Workers." Geneva: World Vision, 1999. <https://fmwm.org/wp-content/uploads/2016/02/WV-Security-Manual-amended.pdf>.

### Summary

"As a result of growing security risks for international field staff, World Vision's Partnership Security Task Force met for three days in Monrovia, California in October 1997. This cross-section of WV field staff and security specialists formulated 15 security policies they determined are essential to promoting field staff safety. The WV partnership formally adopted and implemented these 15 policies in January 1998."<sup>146</sup>

"World Vision and other relief and development organisations no longer enjoy the presupposed protection of the universal, apolitical, neutral delivery of humanitarian relief. Global trends and recent events signal the growing vulnerability of aid organisations."<sup>147</sup>

### Topics covered

- |   |  |
|---|--|
| 1) WorldVision's approach to security         | 6) implementing standard safety procedures       |
| 2) practicing security awareness              | 7) responding to emergencies                     |
| 3) developing security awareness              | 8) working effectively with the media            |
| 4) surviving attacks, clashes, and abductions | 9) managing stress and maintaining mental health |
| 5) conducting security assessments            |  |

The evangelical Christian humanitarian organization WorldVision created *WorldVision Security Manual: Safety Awareness for Aid Workers* in 1999. The guidebook was prompted by increasing concerns over humanitarian aid worker safety, exemplified by events such as the December 1996 murder of six International Red Cross staff members in Chechnya. In 1997, WorldVision staff formulated the security policies contained within the manual. WorldVision's Office of Corporate Strategy and the organization's senior leadership require all WorldVision staff to adhere to these policies. While the guidebook was created with WorldVision staff in mind and informed by the organization's religious beliefs, the advice contained in the manual could be useful for other groups regardless of whether or not they are faith-based organizations.

### Recommendations

1. **Create a Positive Security Profile:** Ensure that your messaging to governments and communities is clear so that they are willing to be incorporated into your security network. If your profile is properly crafted, there should be little room for groups to question your neutrality or intent.

---

<sup>146</sup> Rogers and Sytsma, "World Vision Security Manual: Safety Awareness for Aid Workers," xi.

<sup>147</sup> Rogers and Sytsma, 1.

2. **Maintain the Proper Demeanor:** Project confidence, but be discreet and dress conservatively and do not display wealth. Maintain a calm approach, be unprovocative, and sustain a sense of separation from armed personnel when accompanied by them.
3. **Be Aware While Traveling:** Monitor all situations in order to recognize potential conflict. Avoid traveling at night or alone when possible, and notify others of your itinerary and steps to take if you do not arrive on time. Observe local laws and regulations and never carry unauthorized personnel.
4. **Understand the Region:** Research the history of the region, particularly the identity of opposing groups, power structures of authority groups, and attitude toward foreigners. Also, an understanding of the region's cultural traditions and taboos is crucial for avoiding escalation during a crisis.
5. **Know How to Act During an Attack or Confrontation:** If you are robbed or threatened by an armed individual, never interfere with them or act aggressively. If you hear gunfire, stay calm and take cover immediately while steering clear of windows and doors.
6. **Conduct Regular Security Assessments:** These assessments are crucial in determining whether to continue, scale back, or end operations and what security measures to implement. These assessments should continuously collect, analyze, and disseminate information in order to determine threat levels and assess vulnerabilities.
7. **Implement Standard Security Procedures:** Security procedures should cover contingencies that occur in the field and prepare staff for incidents. These procedures should include an incident reporting system, security briefings and safety training, and site management policies.
8. **Prepare for Emergencies:** Have clear policies for staff so that they can properly respond to emergencies. This includes medical procedures, guidelines for hostage negotiations, and operational plans to follow in case evacuation is necessary.
9. **Avoid Certain Topics During Media Interviews:** Try to stay away from discussing the host government, local authorities, and the local political and military situation during interviews in order to avoid provoking violence against your organization.
10. **Use Stress Prevention Techniques:** Take care of your mental health by recognizing and acknowledging stress and taking action to prevent it. Stress prevention can take the form of spiritual practice, staying informed of anything that concerns you in your environment, and expressing your emotions and fears to your friends and colleagues.

*Research brief authored by Devin McCarthy*



## Appendix 12: Research Brief #5

Egeland, Jan, Adele Harmer, and Abby Stoddard. "To Stay And Deliver: Good Practice for Humanitarians in Complex Security Environments." Policy and Studies Series. New York, NY: Office for the Coordination of Humanitarian Affairs Policy Development and Studies Branch, 2011.

Stoddard, Abby, Adele Harmer, and Katherine Haver. "Safety and Security for National Humanitarian Workers." Policy and Studies Series. New York, NY: Office for the Coordination of Humanitarian Affairs Policy Development and Studies Branch, 2011.

### Summary

"In response to growing concerns regarding the insecurity of aid operations and the resulting decline in humanitarian access, the present study, commissioned by the UN Office for the Coordination of Humanitarian Affairs (OCHA), set out to identify and document those strategies and practices that have enabled humanitarian organisations to maintain effective operations in contexts characterised by high security risks."<sup>148</sup>

"Much of the report is practical: What's working, and why, and what lessons can be drawn across contexts and between agencies? The resulting compilation of practices offers an opportunity for peer learning and knowledge sharing among humanitarian practitioners across complex security settings. In addition, the study examines the wider, political constraints to humanitarian action in complex security environments, factors over which humanitarian actors have less control, but which they could more effectively approach through increased coordination and advocacy."<sup>149</sup>

### Topics covered

- 1) The threat environment: challenges to secure and effective humanitarian access
- 2) good practice for gaining and maintaining access in high-risk environments
- 3) political constraints
- 4) national and local humanitarian actors: key issues

The United Nations Office for the Coordination of Humanitarian Affairs (OCHA) wrote *To Stay and Deliver: Good Practice for Humanitarians in Complex Security Environments*, as well as *Safety and Security for National Humanitarian Workers: Annex I to To Stay and Deliver*, in 2011. The guidebook and its companion document were created in response to the increasing danger that humanitarian aid workers find themselves in. Aid operations have grown insecure due to the increased sophistication of threats, which has resulted in a shrinking of the humanitarian aid footprint. The two OCHA documents provide information and recommendations to

---

<sup>148</sup> Egeland, Harmer, and Stoddard, "To Stay And Deliver: Good Practice for Humanitarians in Complex Security Environments," 1.

<sup>149</sup> Stoddard, Harmer, and Haver, "Safety and Security for National Humanitarian Workers (Annex I to: To Stay and Deliver: Good Practices for Humanitarians in Complex Security Environments)," 1.

international aid workers so that they can better protect themselves, their colleagues, and their operations and expand their access to the communities they serve.

### **Recommendations**

1. **Prioritize Security Risk Management:** Ensure security considerations are part of the planning process from the onset so that resources can be properly allocated.
2. **Build and Maintain Acceptance:** Invest in the capacities and skills needed for dialogue, outreach, and negotiation with the community.
3. **Define a Threshold of Acceptable Risk:** Balance the criticality of the program with the threshold of acceptable risk and ensure that all staff members are aware of this threshold so that they can operate with informed consent.
4. **Collaborate With Local Partners:** Help partner organizations in the area determine their security support needs and provide them with the necessary financial, technical, and material resources so that they can assist your staff to the best of their ability.
5. **Adhere to Humanitarian Principles:** Ensure that all staff members have a sound grasp of humanitarian principles, invest in communicating the significance of these principles, and regularly review operations to make sure that all programs are complying with the principles.
6. **Work With Local Leaders:** Identify and collaborate with influential political, military, and religious figures actors to ensure that they are accepting of humanitarian action and will remain in open dialogue with staff.
7. **Communicate With Local Government Agencies:** Identify potential security concerns so that local government authorities can prevent interference and provide security guarantees to staff in the field.
8. **Create a Platform for Staff Communication:** Ensure that staff have a means of updating each other on proper operational procedure and safety concerns in complex security environments.
9. **Audit Security Resources:** Conduct comprehensive audits of the security resources provided to your staff to identify and resolve any inequities in human resources, skill development, and training policies.
10. **Increase Donor Support:** Utilize funding mechanisms to gain increased donor support for security resources, skill-set training, and other methods of care for staff.

*Research brief authored by Devin McCarthy*

# THREAT MODELING

READ MORE ABOUT ASSESSING YOUR RISKS AT  
[HTTPS://SSD.EFF.ORG/](https://SSD.EFF.ORG/)

**THREAT MODELING** helps you identify threats to the things you value and who you need to protect them from. When building a threat model, you can ask yourself the following questions.

- What do I want to protect?
- Who do I want to protect it from?
- What are the consequences if I fail?
- How likely are these consequences?
- How can I address the most likely risks?

## THREAT MODELING GLOSSARY:

**Asset:** What I want to protect

**Adversaries:** Who I want to protect my assets from

**Threats:** What are the potential consequences if I fail?

**Risk:** The likelihood that a particular threat against a particular asset will actually occur

**Adversary capability:** What an adversary is able to do to achieve its aim. For example, a country's security services might have the capability to listen to telephone calls while a neighbor may have the capability to watch you from their window. To say that an adversary "has" a capability does not mean that they will necessarily use that capability. It does mean that you should consider and prepare for the possibility.

*Try it! Make a threat model for a jewelry store owner:*

## THREAT MODEL FOR A JEWELRY STORE OWNER

**YOU inherit a JEWELRY STORE in the city.**  
 The JEWELRY STORE has:



- \$1 million worth of diamonds.
- A staff of five people.
- An alarm system.
- A safe.
- A cash register.
- A camera monitoring the door.
- A pin-protected alarm for the door.

1

What assets are you protecting?

- \$1 million worth of diamonds
- Money in the safe
- Alarm code
- **Anything else?**

2

Who are your adversaries?

- Jewelry thieves
- **Anyone else?** (Consider: Who might have access to the jewelry store safe? What about cleaning crews, or maintenance staff?)

3

What are the consequences if you fail?

- Theft of jewelry
- Any other **threats?** (What if the safe code or alarm code is stolen?)

4

How likely are these consequences?

Map the likelihood of these threats occurring on the back!

5

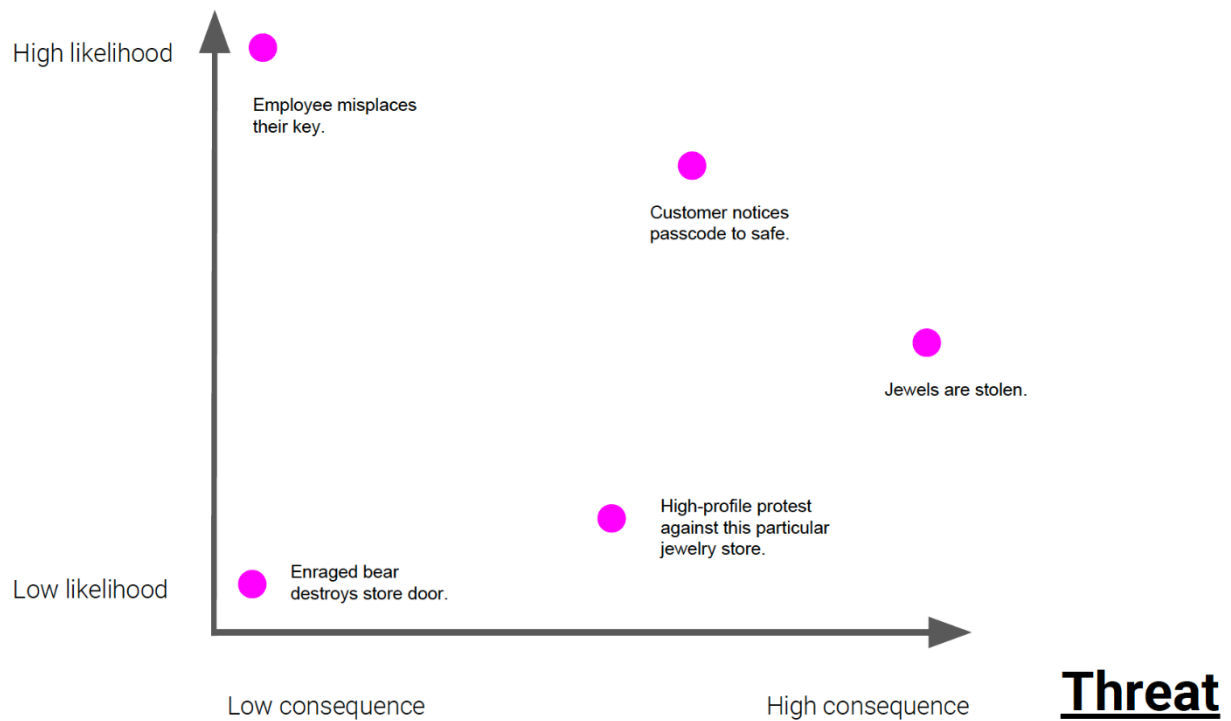
How can you address the most likely risks?

- Changing the passcode every month, and after an employee leaves.
- **What else?**

<sup>150</sup> Electronic Frontier Foundation, "Threat Modeling."

# Risk

How likely are these consequences? This depends on your adversaries' **capabilities**.



# ASSESSING YOUR RISKS

**1** ASSETS: What do you want to protect?

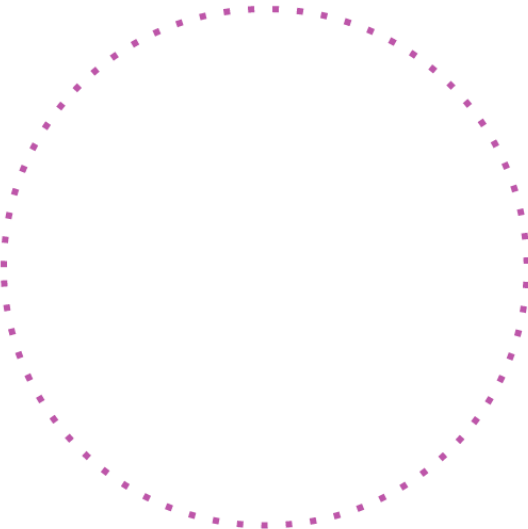
**2** ADVERSARIES:  
Who do you want to protect it from?

What would motivate your adversaries?

What are your adversaries' capabilities?

**5** What kinds of protections make sense in response?

Fill this section out after completing #4 on the back.  
Determining appropriate measures depends on your appetite for risk.



**6** Technologies and threats change.  
Plan to reassess your risks.

I will reevaluate my threat model on: \_\_\_\_\_

**3** THREATS:  
How would they threaten your assets?

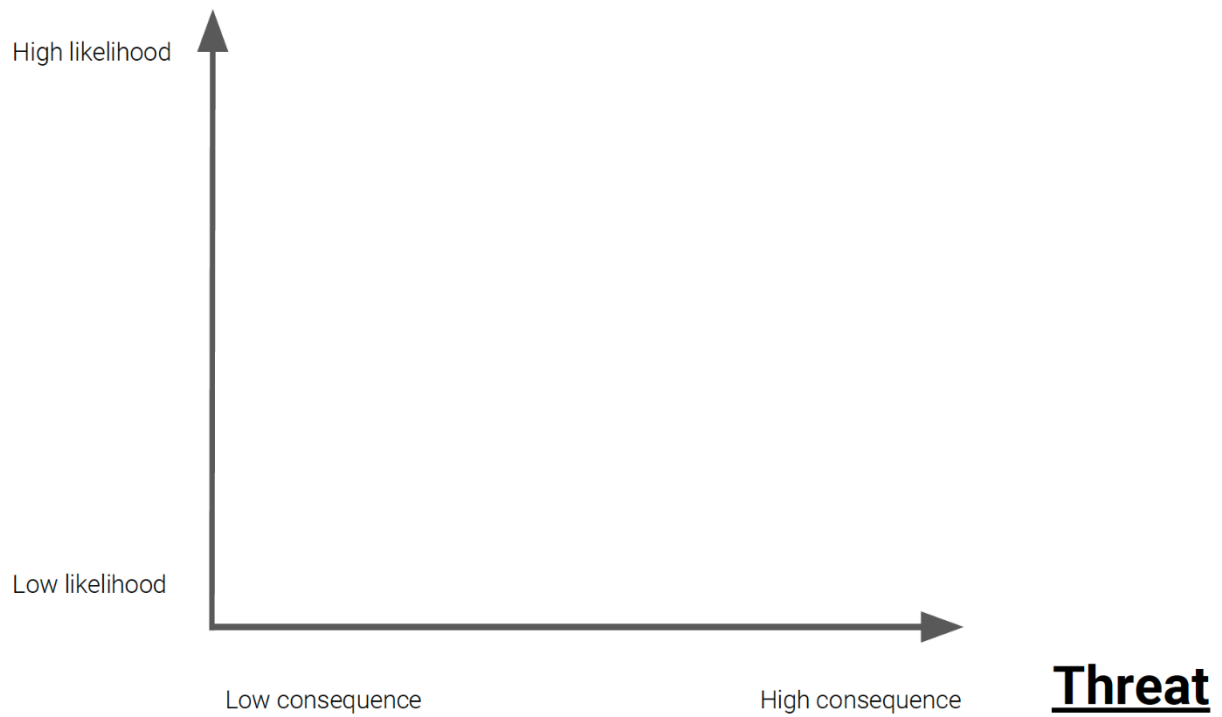
Map the likelihood of the threats on the next page!

**4**

# Risk



How likely are these threats? This depends on your adversaries' **capabilities**.



## Acknowledgements

This project was made possible with the support of George Mason University's Better Evidence Project (BEP), led by Dr. Susan Allen, with administrative support from Dr. Kristina Hook, Dr. Margarita Tadevosyan, and Shayla Gibson, and the research contributions offered by Peyton Nielsen and Devin McCarthy, students at the University of Notre Dame, employed by BEP as interns during the Summer 2021 term. Thank you to Ziad Al Achkar for agreeing to chair the working group formed to continue the work initiated by this paper, and the numerous scholar-practitioners who offered to engage beyond the page and into the future.

## Notes on contributors

*Dr. Michael Loadenthal* is a Senior Research Associate with the Better Evidence Project at George Mason University, during the Spring-Summer 2021 term. He concurrently serves as a Postdoctoral Research Fellow with the Center for Cyber Strategy and Policy (University of Cincinnati), an Associate Fellow with the Global Network on Extremism and Technology, the founding Executive Director of the Prosecution Project, and the Executive Director of the Peace and Justice Studies Association (Georgetown University). He holds a Ph.D. in Conflict Analysis (George Mason University), and a Master's degree in Terrorism Studies from the Centre for the Study of Terrorism and Political Violence (University of St. Andrews). He has worked in conflict and disaster zones on four continents as an organizer, researcher, and security consultant, and regularly trains social movement organizations and conflict practitioners in threat modeling, risk analysis, Open-Source Intelligence techniques, and digital-operational security.

*Devin McCarthy* is an undergraduate student studying Political Science and Global Affairs, with a concentration in International Peace Studies, at the University of Notre Dame. His academic work focuses on atrocity prevention, civil wars, and disarmament. Devin has extensive research experience tracking the triggers of state-sponsored mass killings, and has previously interned with EducationUSA in Brazil, and the Partnership for the Public Good in Buffalo, New York. He is currently working as a research intern with the Better Evidence Project at George Mason University.

*Peyton Nielsen* is an undergraduate student at the University of Notre Dame, where she is studying Economics and American Studies, with a minor in Digital Marketing. Her interests reside in policy, economic empowerment, and education. Her coursework consists of foreign relations, economics, and cultural analysis, and focuses her volunteer work and research on a more local level, working with multiple youth organizations on violence prevention through education and empowerment. Peyton serves as a research and social media intern with the Better Evidence Project at George Mason University.

## References

- Azores-Gococo Nicole M. and Fridberg Daniel J. "Harm-Reduction Strategies for Injection Drug Use." *Psychiatric Annals* 47, no. 1 (January 1, 2017): 45–48.
- Barratt, Monica J, and Alexia Maddox. "Active Engagement with Stigmatised Communities through Digital Ethnography." *Qualitative Research* 16, no. 6 (December 1, 2016): 701–19.
- Bickley, Shaun. "SAFETY FIRST: A Safety and Security Handbook for Aid Workers." London, UK: Save the Children, 2010.
- Booth, Ken, ed. *Critical Security Studies And World Politics*. Boulder, CO: Lynne Rienner Pub, 2005.
- . *Theory of World Security*. Cambridge, UK: Cambridge University Press, 2008.
- Braiterman, Zoe, Adam Shostack, Jonathan Marcil, Stephen de Vries, Irene Michlin, Kim Wuyts, Robert Hurlbut, et al. "Threat Modeling Manifesto." Threat Modeling Manifesto Working Group, November 17, 2020. <https://www.threatmodelingmanifesto.org/>.
- Burton, John W. *Conflict: Human Needs Theory*. New York, NY: St. Martin's Press, 1990.
- Buzan, Barry, Ole Waever, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Pub, 1998.
- Caballero-Anthon, Mely, ed. *An Introduction to Non-Traditional Security Studies: A Transnational Approach*. Los Angeles, CA: SAGE Publications Ltd, 2016.
- Calhoun, Frederick S., and Stephen W. Weston. *Threat Assessment and Management Strategies: Identifying the Howlers and Hunters, Second Edition*. 2nd edition. Boca Raton, FL: CRC Press/Taylor & Francis, 2016.
- Care International, and Robert Macpherson. "Safety & Security Handbook." Geneva: Care International, 2004.
- Chaplin, Daniel, John Twigg, and Emma Lovell. "Intersectional Approaches to Vulnerability Reduction and Resilience-Building." UK: BRACED, April 12, 2019. <https://cdn.odi.org/media/documents/12651.pdf>.
- Chisty, Musabber Ali, Syeda Erena Alam Dola, Nesar Ahmed Khan, and Md Mostafizur Rahman. "Intersectionality, Vulnerability and Resilience: Why It Is Important to Review the Diversifications Within Groups at Risk to Achieve a Resilient Community." *Continuity & Resilience Review*, January 1, 2021.
- Clark, Robert M., ed. *Intelligence Analysis; A Target-Centric Approach Fifth Edition*. 5th edition. Los Angeles, CA: CQ Press, 2016.
- Collins, Patricia Hill. *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment*. New York, NY: Routledge, 1991.
- Conway, Maura. "Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines." *Terrorism and Political Violence* 33, no. 2 (February 17, 2021): 367–80.
- Crawford, Neta C. "Once and Future Security Studies." *Security Studies* 1, no. 2 (1991): 283–316.
- Crenshaw, Kimberlé. *On Intersectionality: The Essential Writings of Kimberle Crenshaw*. New Press, The, 2012.
- Cutts, Mark, and Alan Dingle. *Safety First: Protecting NGO Employees Who Work in Areas of Conflict (2nd Ed.)*. London, UK: Save the Children, 1998.



- Dalby, Simon. "Climate Change and Environmental Security." In *Security Studies: An Introduction*, edited by Paul D. Williams, 2nd edition., 311–23. London ; New York: Routledge, 2012.
- DEF CON 29 - A Look inside Security at the New York Times or A Media Security Primer for Hackers. Streaming video hosted by Youtube. Def Con 29, 2021.  
[https://www.youtube.com/watch?v=U2-8MNx8nsg&ab\\_channel=DEFCONConference](https://www.youtube.com/watch?v=U2-8MNx8nsg&ab_channel=DEFCONConference).
- Doucet, Marc G., and Miguel de Larrinaga. "Human Security and the Securing of Human Life: Tracing Global Sovereign and Biopolitical Rule." In *Critical Perspectives on Human Security: Rethinking Emancipation and Power in International Relations*, edited by David Chandler and Nik Hynek, 129–43. New York, NY: Routledge, 2012.
- Dugan, Marie. "A Nested Theory of Conflict." *Leadership Journal: Women in Leadership* 1 (1996): 9–19.
- Egeland, Jan, Adele Harmer, and Abby Stoddard. "To Stay And Deliver: Good Practice for Humanitarians in Complex Security Environments." Policy and Studies Series. New York, NY: Office for the Coordination of Humanitarian Affairs Policy Development and Studies Branch, 2011.
- Electronic Frontier Foundation. "The Harm Reduction Approach." Security Education Companion, 2021. <https://sec.eff.org/articles/harm-reduction>.
- . "Threat Modeling," 2020. <https://ssd.eff.org/>.
- . "Your Security Plan." Surveillance Self-Defense, February 2, 2021.  
<https://ssd.eff.org/en/module/your-security-plan>.
- Ewing, J. Jackson. "Environmental Security." In *An Introduction to Non-Traditional Security Studies: A Transnational Approach*, edited by Mely Caballero-Anthon, 95–113. Los Angeles, CA: SAGE Publications Ltd, 2016.
- Fast, Larissa. "A Reflexive Approach to Risk and Intervention for Third-Party Intervenors." *Conflict Resolution Quarterly* 30, no. 4 (2013): 467–89.
- . *Aid In Danger: The Perils and Promise of Humanitarianism*. Pennsylvania Studies in Human Rights. Philadelphia, PA: University of Pennsylvania Press, 2014.
- . "Security and Risk Management for Peacebuilding Organisations." Berlin, Germany: Berghof Foundation, 2014.
- Fast, Larissa A. "Mind the Gap: Documenting and Explaining Violence Against Aid Workers." *European Journal of International Relations* 16, no. 3 (September 1, 2010): 365–89.
- Fast, Larissa, Faith Freeman, Michael O'Neill, and Elizabeth Rowley. "The Promise of Acceptance as an NGO Security Management Approach." *Disasters* 39, no. 2 (2015): 208–31.
- Fast, Larissa, and Dawn Wiest. "Final Report Security Perceptions Survey." Washington, DC: The United State Institute of Peace, August 2007. <https://gisf.ngo/wp-content/uploads/2014/09/0009-Fast-Wiest-2007-Security-Perceptions-Survey10.pdf>.
- Frontline Defenders. "Workbook on Security: Practical Steps for Human Rights Defenders at Risk." Dublin, Ireland: Frontline Defenders, 2011.
- Galtung, Johan. "An Editorial." *Journal of Peace Research* 1, no. 1 (March 1, 1964): 1–4.
- Garfinkel, Simson, and Gene Spafford. *Practical Unix & Internet Security, 3rd Edition*. 2nd edition. Sebastopol, CA: O'Reilly Media, 1996.

- Geneva Centre for the Democratic Control of Armed Forces and The International Committee of the Red Cross. "Addressing Security and Human Rights Challenges in Complex Environments Toolkit (3rd Ed.)." Geneva: DCAF/ICRC, 2016.
- Gordon, Eleanor. *Conflict, Security and Justice: Practice and Challenges in Peacebuilding*. London, UK: Macmillan International/Red Globe Press, 2019.
- Haftendorn, Helga. "The Security Puzzle: Theory-Building and Discipline Building in International Security." *International Studies Quarterly* 35, no. 1 (1991): 3–17.
- Harmer, Adele, Abby Stoddard, and Kate Toth. "Aid Worker Security Report 2013 - The New Normal: Coping with the Kidnapping Threat." Washington, DC: Humanitarian Outcomes, October 2013. [https://aidworkersecurity.org/sites/default/files/2020-08/AidWorkerSecurityReport\\_2013\\_web.pdf](https://aidworkersecurity.org/sites/default/files/2020-08/AidWorkerSecurityReport_2013_web.pdf).
- Hendrickson, Noel. *Reasoning for Intelligence Analysts: A Multidimensional Approach of Traits, Techniques, and Targets*. Lanham, MD: Rowman & Littlefield Publishers, 2018.
- Hoelscher, Kristian, Jason Miklian, and Havard Mokliev Nygard. "Understanding Attacks on Humanitarian Aid Workers." Oslo, Norway: Peace Research Institute Oslo, June 2015. <https://www.prio.org/utility/DownloadFile.ashx?id=101&type=publicationfile>.
- Hough, Peter. "Environmental Security." In *International Security Studies: Theory and Practice*, by Peter Hough, Shahin Malik, Andrew Moran, and Bruce Pilbeam, 211–24. New York, NY: Routledge, 2015.
- "Human Development Report 1994." New York, NY: United Nations Development Programme, 1994. [http://hdr.undp.org/sites/default/files/reports/255/hdr\\_1994\\_en\\_complete\\_nostats.pdf](http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf).
- Humanitarian Practice Network. "Operational Security Management in Violent Environments (Revised Edition)." London, UK: Overseas Development Institute, Humanitarian Practice Network, December 2010. <https://odihpn.org/resources/operational-security-management-in-violent-environments-revised-edition/>.
- InterAction, Working Group on NGO Security. "Report of the Working Group on NGO Security Training Curriculum." Washington, DC: InterAction, 1997.
- International Federation of the Red Cross and Red Crescent Societies. "Stay Safe: The International Federation's Guide to a Safer Mission (4th Ed.)." Geneva: International Federation of the Red Cross and Red Crescent Societies, 2013. <https://media.ifrc.org/ifrc/wp-content/uploads/2018/03/Personal-SecurityENGLISH.pdf>.
- IriusRisk. "IriusRisk Threat Modeling Platform: Community Edition," 2021. <https://community.iriusrisk.com/ui#!login>.
- Irrera, Daniela. "Protecting the Protectors: Strengthening the Security of NGOs in Conflict Zones." E-International Relations, August 25, 2020. <https://www.e-ir.info/2020/08/25/protecting-the-protectors-strengthening-the-security-of-ngos-in-conflict-zones/>.
- IT Governance USA. "ISO 27005," 2020. <https://itgovernanceusa.com/cyber-security-solutions/iso27001/iso-27005>.
- Jarvis, Lee, and Jack Holland. *Security: A Critical Introduction*. London, UK: Palgrave Macmillan, 2015.

- Jones, Emma, Kate Denman, Elizabeth Molloy, and Adelia Fairbanks. "Managing the Security of Aid Workers with Diverse Profiles." European Interagency Security Forum Research Paper. London, UK: European Interagency Security Forum, 2018.
- Kaldor, Mary. *Human Security*. Oxford, UK: Polity, 2007.
- King, Dennis. "Chronology of Humanitarian Aid Workers Killed in 1997– 2001." Geneva: UN Office for the Coordination of Humanitarian Affairs, January 15, 2002.  
<http://reliefweb.int/symposium/NewChron1997-2001.html>.
- King, Marcus Dubois. "Water Security." In *An Introduction to Non-Traditional Security Studies: A Transnational Approach*, edited by Mely Caballero-Anthon, 154–73. Los Angeles, CA: SAGE Publications Ltd, 2016.
- Kuran, Christian Henrik Alexander, Claudia Morsut, Bjørn Ivar Kruke, Marco Krüger, Lisa Segnestam, Kati Orru, Tor Olav Nævestad, et al. "Vulnerability and Vulnerable Groups from an Intersectionality Perspective." *International Journal of Disaster Risk Reduction* 50 (November 1, 2020): 101826.
- Legal Information Institute, Cornell Law. "18 U.S. Code § 2339A - Providing Material Support to Terrorists." LII / Legal Information Institute, 2009.  
<https://www.law.cornell.edu/uscode/text/18/2339A>.
- . "18 U.S. Code § 2339B - Providing Material Support or Resources to Designated Foreign Terrorist Organizations." LII / Legal Information Institute, 2015.  
<https://www.law.cornell.edu/uscode/text/18/2339B>.
- Loadenthal, Michael. "Advanced Threat Modeling and Key Points of InfoSec & OPSEC for Activists." Cincinnati, OH: IAT, 2020.
- . "Intersectional, Risk-Centric, Threat Modeling for Web 3.0." White paper series. Cincinnati, OH: Off the Page Consulting, February 2021.
- . "Legal-Centric Risk and Threat Modeling for Itme, a Solid Provider." White paper series. Cincinnati, OH: Off the Page Consulting, February 2021.
- . "Political-Centric Risk and Threat Modeling for Itme, a Solid Provider." White paper series. Cincinnati, OH: Off the Page Consulting, February 2021.
- . "Social-Centric Risk and Threat Modeling for Itme, a Solid Provider." White paper series. Cincinnati, OH: Off the Page Consulting, February 2021.
- . "Technical Risk and Threat Modeling for Itme, a Solid Provider." White paper series. Cincinnati, OH: Off the Page Consulting, February 2021.
- . "Understanding Contemporary Repression: Psychologically, Legally, Politically and Discursively." Southeast Ohio: Earth First!, 2018.
- . "Understanding Repression and Building Resilience." Worcester, MA: IAT, 2018.
- . "Web Security and Intersectional Threat Modeling for Activists and Organizers." San Francisco, CA: CoLab Cooperative, 2020.
- Matthews, Jessica Tuchman. "Redefining Security." *Foreign Affairs* 68, no. 2 (1989): 162–77.
- . "Redefining Security." *Foreign Affairs* 68, no. 2 (Spring 1989): 162–77.
- Mayhew, Barney. "Generic Security Guide for Humanitarian Organizations." Brussels, BE: Directorate General for Humanitarian Aid - ECHO, European Commission, 2004.
- Mead, Nancy R., Forrest Shull, Vemuru Krishnamurthy, and Ole Viladsen. "A Hybrid Threat Modeling Method." Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute, March 2018.

Metcalfe, Victoria, Ellen Martin, and Sara Pantuliano. "Risk in Humanitarian Action: Towards a Common Approach?" Denmark: Ministry of Foreign Affairs, November 2010.  
[https://www.who.int/hac/techguidance/tools/risk\\_in\\_humanitarian\\_action.pdf](https://www.who.int/hac/techguidance/tools/risk_in_humanitarian_action.pdf).

MobLab. "Stay Safe out There: Threat Modeling for Campaigners." MobLab, August 12, 2015.  
<https://mobilisationlab.org/stories/threat-modeling-for-campaigners-and-activists/>.

Moßbrucker, Daniel. "Threat Modeling Guide: How to Identify Digital Risks in International Development Projects." Berlin, Germany: Akademie/German Federal Ministry for Economic Cooperation and Development, September 2020.  
[https://akademie.dw.com/docs/Handbook\\_Threat\\_Modeling\\_Guide.pdf](https://akademie.dw.com/docs/Handbook_Threat_Modeling_Guide.pdf).

Moz. "Google Search Operators [2021 SEO]." Moz, 2021. <https://moz.com/learn/seo/search-operators>.

National Harm Reduction Coalition. "Safe(r) Drug Use 101." *National Harm Reduction Coalition* (blog), 2021. <https://harmreduction.org/issues/safer-drug-use/facts/>.

Nye, Joseph S., Jr., and Sean M. Lynn-Jones. "International Security Studies." *International Security* 12, no. 4 (1988): 5–27.

O'Connell, Kit. "Threat Modeling For Activists: Tips For Secure Organizing & Activism." *Kit O'Connell: Approximately 8,000 Words* (blog), October 22, 2018.  
<https://kitoconnell.com/2018/10/22/threat-modeling/>.

O'Neill, Bard E. *Insurgency & Terrorism*. Dulles, VA: Potomac Books, 2001.

OWASP. "OWASP Threat Dragon," 2021. <https://threatdragon.org/login>.

Paris, Ronald. "Human Security: Paradigm Shift or Hot Air?" *International Security* 26, no. 2 (2001): 87–102.

Peoples, Columba, and Nick Vaughan-Williams. *Critical Security Studies: An Introduction*. Taylor & Francis, 2010.

Persaud, Christine. "NGO Safety and Security Training Project: How to Create Effective Security Training for NGOs." The European Interagency Security Forum/InterAction, 2014.  
[https://reliefweb.int/sites/reliefweb.int/files/resources/EISF%2520and%2520InterAction\\_Security%2520Training%2520Project\\_April%25202014\\_1.pdf](https://reliefweb.int/sites/reliefweb.int/files/resources/EISF%2520and%2520InterAction_Security%2520Training%2520Project_April%25202014_1.pdf).

Pincus, Jon. "Social Threat Modeling." Medium, May 11, 2018. <https://medium.com/a-change-is-coming/social-threat-modeling-the-winds-of-change-are-in-the-air-8dc330479a50>.

Pritchard, Carl L. *Risk Management Concepts and Guidance*. 5th ed. Boca Raton, FL: CRC Press, 2015.

Pym, D.V. "Risk Management." *PM Network* 1, no. 3 (August 1987): 33–36.

Reporters Without Borders. "Training: Your Threat Model." Helpdesk - Digital Security for Journalists, 2021. <https://helpdesk.rsf.org/training/your-threat-model/>.

Rice, Liz. *Container Security: Fundamental Technology Concepts That Protect Containerized Applications*. 1st edition. Sebastopol, CA: O'Reilly Media, 2020.

Roberts, David Lloyd. "Staying Alive: Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas." Geneva: International Committee of the Red Cross, 2005  
 1999.

Rogers, Charles, and Brian Sytsma. *A Shield About Me: Safety Awareness for World Vision Staff*. Monrovia, CA: World Vision, 1998.

- . “World Vision Security Manual: Safety Awareness for Aid Workers.” Geneva: World Vision, 1999. <https://fmwm.org/wp-content/uploads/2016/02/WV-Security-Manual-amended.pdf>.
- Rowley, Elizabeth A., Byron L. Crape, and Gilbert M. Burnham. “Violence-Related Mortality and Morbidity of Humanitarian Workers.” *American Journal of Disaster Medicine* 3, no. 1 (February 2008): 39–45.
- Rowley, Elizabeth, Lauren Burns, and Gilbert Burnham. “Research Review of Nongovernmental Organizations’ Security Policies for Humanitarian Programs in War, Conflict, and Postconflict Environments.” *Disaster Medicine and Public Health Preparedness* 7, no. 3 (June 2013): 241–50.
- Salter, Mark B., and Can E. Mutlu, eds. *Research Methods in Critical Security Studies: An Introduction*. New York, NY: Routledge, 2012.
- Schoenfield, Brook S.E. *Securing Systems: Applied Security Architecture and Threat Models*. Boca Raton, FL: CRC Press/Taylor & Francis, 2015.
- Shepherd, Laura J., ed. *Critical Approaches to Security: An Introduction to Theories and Methods*. New York, NY: Routledge, 2013.
- Shostack, Adam. *Threat Modeling: Designing for Security*. 1st edition. Indianapolis, IN: Wiley, 2014.
- . Threat Modeling for Social Issues. Interview by Anna Delaney. Video, January 28, 2021. <https://www.databreachtoday.com/threat-modeling-for-social-issues-a-15854>.
- . *Why Threat Model?* Streaming video. Adam Shostack & friends, 2021. <https://adam.shostack.org/blog/2021/06/why-threat-model/>.
- Sluka, Jeffrey Alan. “Too Dangerous for Fieldwork? The Challenge of Institutional Risk-Management in Primary Research on Conflict, Violence and ‘Terrorism.’” *Contemporary Social Science* 0, no. 0 (July 16, 2018): 1–17.
- Stoddard, Abby, and Adele Harmer. “Little Room to Maneuver: The Challenges to Humanitarian Action in the New Global Security Environment.” *Journal of Human Development* 7, no. 1 (March 1, 2006): 23–41.
- Stoddard, Abby, Adele Harmer, and Victoria DiDomenico. “Providing Aid in Insecure Environments: 2009 Update.” London, UK: Humanitarian Outcomes, April 2009. <https://www.humanitarianoutcomes.org/publications/providing-aid-insecure-environments-2009-update>.
- Stoddard, Abby, Adele Harmer, and Katherine Haver. “Safety and Security for National Humanitarian Workers (Annex I to: To Stay and Deliver: Good Practices for Humanitarians in Complex Security Environments).” Policy and Studies Series. New York, NY: Office for the Coordination of Humanitarian Affairs Policy Development and Studies Branch, 2011.
- Stoddard, Abby, Paul Harvey, Monica Czwarno, and Meriah-Jo Breckenridge. “Aid Worker Security Report 2020.” London, UK: Humanitarian Outcomes, August 2020. [https://www.humanitarianoutcomes.org/sites/default/files/publications/awsr2020\\_0\\_0.pdf](https://www.humanitarianoutcomes.org/sites/default/files/publications/awsr2020_0_0.pdf).
- Stoddard, Abby, Katherine Haver, and Monica Czwarno. “NGOs and Risk: How International Humanitarian Actors Manage Uncertainty.” Humanitarian Outcomes/InterAction, February 2016.

- [https://www.humanitarianoutcomes.org/sites/default/files/publications/ngo-risk\\_report\\_web.pdf](https://www.humanitarianoutcomes.org/sites/default/files/publications/ngo-risk_report_web.pdf).
- Stokes, Wendy. "Feminist Security Studies." In *International Security Studies: Theory and Practice*, edited by Peter Hough, Shahin Malik, Andrew Moran, and Bruce Pilbeam, 44–56. London, UK: Routledge, 2015.
- Tadjbakhsh, Shahrbanou, and Anuradha Chenoy. *Human Security: Concepts and Implications*. New York, NY: Routledge, 2007.
- Tarandach, Izar, and Matthew J. Coles. *Threat Modeling: A Practical Guide for Development Teams*. 1st edition. Sebastopol, CA: O'Reilly Media, 2020.
- Thompson, Eleanor E. *The Insider Threat: Assessment and Mitigation of Risks*. Boca Raton, FL: CRC Press/Taylor & Francis, 2019.
- Tickner, J. Ann. *Gender in International Relations: Feminist Perspectives on Achieving Global Security*. New York, NY: Columbia University Press, 1992.
- Tilly, Charles. *The Politics of Collective Violence*. Cambridge University Press, 2003.
- UcedaVelez, Tony, and Marco M. Morana. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. Hoboken, New Jersey: Wiley, 2015.
- Ullman, Richard. "Redefining Security." *International Security* 8, no. 1 (1983): 129–53.
- UNAIDS. "Harm Reduction Saves Lives." Geneva: Joint United Nations Programme on HIV/AIDS, 2017. [https://www.unaids.org/sites/default/files/media\\_asset/harm-reduction-saves-lives\\_en.pdf](https://www.unaids.org/sites/default/files/media_asset/harm-reduction-saves-lives_en.pdf).
- United Nations Office for the Coordination of Humanitarian Affairs. "United Nations Disaster Assessment and Coordination (7th Ed.)." *UNDAC Field Handbook*. Geneva: United Nations Office for the Coordination of Humanitarian Affairs, 2018.
- United States Department of Homeland Security. "Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide (3rd Ed.)." Washington, DC: United States Department of Homeland Security, May 2018. <https://www.fema.gov/sites/default/files/2020-04/CPG201Final20180525.pdf>.
- United States Institute of Peace. "Guiding Principles for Stabilization and Reconstruction: Safe and Secure Environment." United States Institute of Peace, n.d. <https://www.usip.org/guiding-principles-stabilization-and-reconstruction-the-web-version/safe-and-secure-environment>.
- U.S. Department of State, Bureau of Counterterrorism. "Foreign Terrorist Organizations." *United States Department of State* (blog), January 10, 2020. <https://www.state.gov/foreign-terrorist-organizations/>.
- Van Brabant, Koenraad. "Mainstreaming the Organisational Management of Safety and Security." HPG report. London, UK: Overseas Development Institute, Humanitarian Policy Group, March 2001. <https://gisf.ngo/wp-content/uploads/2014/09/0598-Van-Brabant-2001-Mainstreaming-the-Organisational-Management-of-Safety-and-Security.pdf>.
- Van Der Meer, Bram B., and Margaret L. Diekhuis. "Collecting and Assessing Information for Threat Assessment." In *International Handbook of Threat Assessment*, edited by J. Reid Meloy and Jens Hoffmann, 55–66. New York, NY: Oxford University Press, 2014.
- Vinyeta, Kristen, Kyle Powys Whyte, and Kathy Lynn. "Climate Change Through an Intersectional Lens: Gendered Vulnerability and Resilience in Indigenous Communities in the United

- States.” Washington, DC: United States Department of Agriculture, Forest Service, December 2015. [https://www.fs.fed.us/pnw/pubs/pnw\\_gtr923.pdf](https://www.fs.fed.us/pnw/pubs/pnw_gtr923.pdf).
- Warren, Lisa J., Paul E. Mullien, and Troy E. Mcewan. “Explicit Threats of Violence.” In *International Handbook of Threat Assessment*, edited by J. Reid Meloy and Jens Hoffmann, 18–38. New York, NY: Oxford University Press, 2014.
- Weber, Max. “Politik als Beruf (Politics as a Vocation).” Lecture presented at the Free Students Union, Munich University, January 1919.  
[http://www.ne.jp/asahi/moriyuki/abukuma/weber/lecture/politics\\_vocation.html](http://www.ne.jp/asahi/moriyuki/abukuma/weber/lecture/politics_vocation.html).
- Wibben, Annick T. R. *Feminist Security Studies: A Narrative Approach*. New York, NY: Routledge, 2011.
- , ed. *Researching War: Feminist Methods, Ethics and Politics*. New York, NY: Routledge, 2016.