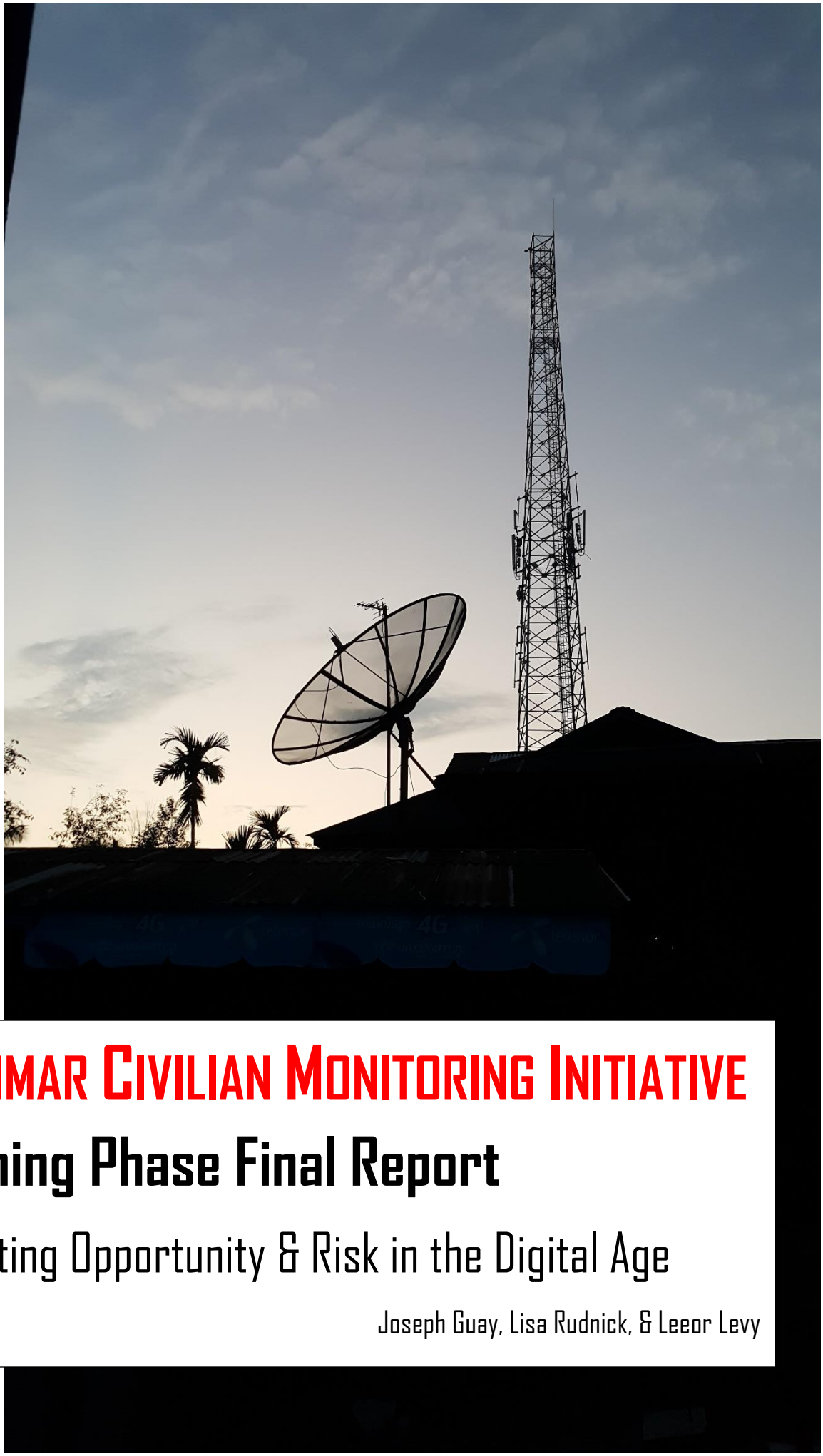


# Myanmar Civilian Monitoring Initiative

## Learning Phase Final Report

### Navigating Opportunity & Risk in the Digital Age

Joseph Guay, Lisa Rudnick, & Leeor Levy

# INTRODUCTION

## Background

### Problem & Opportunity

Over the last 6 years, high-intensity armed conflict in the north of Myanmar has claimed the lives of thousands, displaced more than 100,000, and damaged the country's otherwise impressive democratic reform and peacebuilding processes. Military restrictions on humanitarian and media access to affected areas obscures the conflict from national and international audiences while enabling a culture of impunity among those who perpetuate the violence. Hidden from public view, affected populations suffer human rights abuses and are now seeing humanitarian assistance decline as more visible conflicts draw the gaze of international donors.

Since 2012, Nonviolent Peaceforce (NP) has been "engaging key stakeholders and partners in Myanmar at the request of local civil society organizations as well as the Myanmar government" to support local actors endeavoring to address these conditions. An "international NGO that supports peace by facilitating dialogue and protecting vulnerable civilians in situations of violent conflict," NP has supported civilian protection and ceasefire monitoring efforts in a number of states, works with civil society groups, and has provided training in ceasefire monitoring and implementation to Liaison Offices of Ethnic Armed Organizations."[1]

With NP's support, civilian ceasefire monitors (CCMs) began working in Myanmar in 2015. Today, repositioned as **Community Peace Support (CPS) networks**, they are located throughout much of the country, reporting on conflict and humanitarian challenges through an approach aimed at improving relationships and conditions for peace. NP and others have observed their significant monitoring, reporting, and peacebuilding potential, but also recognize that CPSs face a range of significant and limiting challenges and obstacles. At the same time, the evolving scale and humanitarian impact of violent conflict in Myanmar's north, and the lack of both national and international awareness and response to these conditions, continues to cause grave concern.

**In light of the successes demonstrated by current CPSs and community protection monitors in their work, NP has proposed that by improving the functional and technical capabilities of CPSs, they might be able to contribute much-needed information about conflict-related incidents and displacement through their monitoring work**. The underlying assumption of this proposition is that providing such information will allow for both the scale and the humanitarian impact of violent conflict in Myanmar's north to be better communicated to, and understood by, national and international stakeholders, thereby enabling more timely and effective conflict prevention and humanitarian assistance efforts in turn.

NP and The Policy Lab (TPL) therefore formed a partnership **to explore *whether* recent advances in mobile communications technology (1) can be leveraged to address some of the key challenges CPSs currently face in their work, and (2) *whether in so doing*, they can**

[1] Nonviolent Peaceforce (2016) Civilians protecting civilians through ceasefire monitoring: Civilian ceasefire monitoring in Myanmar: 2012-2016. (p.4)

**enable monitors to generate timely, verifiable, and context-relevant information for peacebuilding and humanitarian actors.**

To respond to these questions, a program of work was needed to determine whether this initial proposition is a viable one and if so to translate it, in a subsequent phase, from a proposition to a prototype solution that is fit for both purpose and context.

Recognizing the importance of problem definition for innovation initiatives addressing humanitarian challenges,[2] NP and TPL applied to the Humanitarian Innovation Fund for support to conduct a formal Problem Recognition phase to support this work, and thereby launch the first phase of a formal innovation cycle.

This report reflects the learning and outcomes of this first phase, as adapted to resources.

# Innovation

## The Problem Recognition Phase

"Innovation" is sometimes used interchangeably with other terms such as "experimentation" or "creativity." However, a growing body of work is helping practitioners and stakeholders alike to recognize the key and common characteristics of successful innovation initiatives. Drawing from that work as well as our own practical experience, use the following definition:

> *A dedicated **process** of exploration, learning, designing, prototyping, and testing that is undertaken for the purpose to either improve upon existing solutions to challenges, to create new ones, or to use new approaches for the discovery of solutions.*

Framed this way, innovation is fundamentally about problem solving. What's more, the solutions born out of this process come in all shapes and sizes. In other words, innovation can lead to solutions that are products, but it can also lead to new ways of doing things (such as new processes, practices, or techniques). Finally, our definition is deliberately *not* anchored in technology, and is therefore equally open to any new means to solve problems, technological or otherwise.

Successful innovation processes – those that result in meaningful solutions and lead to improved positive outcomes without increasing vulnerability or introducing harm to affected people – follow such a cycle of learning, designing, testing, and refining. Importantly, they also dedicate time and resources to the activities of Problem Recognition in first phase of work in order to build the foundations needed for subsequent phases.

[2] See Ian McClelland, "Supporting Innovation: Where Humanitarians Struggle Most, and How Our New Field Guide Will Help" (February 28, 2018). Citing extensive research on the stages of innovation that need the most targeted support and the cross-cutting issues that need the most guidance in humanitarian contexts, "Many people highlighted the need to strengthen problem diagnosis and better identify existing opportunities, citing the importance of identifying root causes for designing the right approach, and the need to avoid duplication of innovation efforts…. The results of the survey were similar across all organizational types but, interestingly, it was those who identified as 'experienced' or 'very experienced' who showed a clear preference for guidance on problem diagnosis—perhaps reflecting involvement in projects that have wasted too much time trying to solve the wrong problem for the wrong people, an issue that could have been avoided by a better understanding of the problem from the start."

We take **Problem Recognition** to involve the important work of identifing and learning about the challenges and needs to be addressed, by whom, and testing initial assumptions about potential solutions.[3] Such assumptions have a way of shaping how we may think about what is needed, and why. Taking time to investigate *in situ* the nature of challenges being experienced, by whom, helps provide us with clarity around key issues at the start of an innovation process, including but by no means limited to:

- What is the nature, scope, and complexity of the problem(s) to be addressed?
- Where and how will you "set parameters" around the problem to help define it?
- Who are the key stakeholders involved or implicated, and what challenges are faced across or among different stakeholders?
- What is known about existing solutions or past efforts to address the problem and meet the needs of key stakeholder groups?
- What information regarding the context (or operational environment) is particularly relevant in exploring or explaining the problem?
- How might you explain the key drivers, barriers, and gaps that might be causing or contributing to the identified problem?
- How might uses (of innovation solutions) vary for different user groups, depending upon their particular needs and challenges?

Problem Recognition is important because it creates an anchor for the innovation process to respond to, and criteria against which to evaluate the evolving solution. It helps to focus the innovation process upon challenges, problems and needs that are either experienced by stakeholders, or that have consequential implications for their well-being and daily lives. It helps to guard against the potential of creating a solution in search of a problem.

The key outcome of the Problem Recognition phase, then, is the Design Brief – the foundation upon which the next phase in an innovation cycle – the design phase – can be built to create a tangible tool or solution that can ultimately address challenges in meaningful ways.

# Approaches

## Evidence-based Design (EBD)

One approach to innovation is Evidence Based Design, or EBD.[4] Like other innovation approaches, EBD progresses through three iterative and collaborative phases: Diagnose, Design, and Deliver. These correspond with the phases of the innovation cycle that are employed in the development of innovation solutions, whether they are products, processes, services, or systems innovations.

[3] See HIF Guide Problem Recognition modules in the Humanitarian Innovation Guide: "Recognition should be the first stage of any innovation journey. It broadly consists of identifying a problem or opportunity to respond to, collecting and assessing readily available knowledge on the issue and context, diagnosing root causes, and properly framing the challenge."

[4] See Miller and Rudnick (2012) "A Framework Document on Evidence-Based Design for Reintegration" (UNIDIR: Geneva); and Miller and Rudnick (2014) "A Prototype for Evidence-Based Programme Design for Reintegration" (UNIDIR: Geneva). Refer to "Using and Integrating Evidence" Enabling Factors in the Elrha Humanitarian Innovation Guide (May, 2018).

| DIAGNOSE | DESIGN | DELIVER |
|---|---|---|
| **i)** Learning about the nature of the problem, where it takes place, who it affects, and how people experience it.<br><br>**ii)** Applying learnings to identify opportunities, consider risks and define/refine our objectives. | **i)** Employing knowledge gained from the "diagnose" phase as raw material for generating design propositions in an iterative process to create, test and refine solutions that are problem-driven, user-centered and evidence-based. | **i)** Communicating solutions in ways that are meaningful to those who will implement them, and those likely to be affected by them.<br><br>**ii)** Piloting solutions in context, or otherwise supporting their launch. |

| | | | | |
|---|---|---|---|---|
| FORMATIVE LEARNING > | INSIGHTS > | IDEATION > | DESIGN > | PROTOTYPE PILOT + TESTING |

While EBD works through the same basic sequence that most approaches to innovation have in common, some key features of the EBD approach that distinguish it from others include:

- attention to the role of information and evidence in design;
- deliberation on the achievement of both strategic and social impact; and
- consideration of vulnerabilities, threats, and unintended consequences of any proposed solutions.

Because of this, EBD is particularly well suited to innovation in complex, high-risk environments, especially when this involves the development and application of new technologies, and when unintended consequences to safety and well-being are a concern.

Currently, the Myanmar civilian monitoring initiative is in the Diagnose, or **Problem Recognition** phase of its innovation cycle. As discussed above, this crucial phase enables us to verify our assumptions and add to our understanding about the nature of the problem to be addressed. This is achieved through a proces of contextual research that generates crucial, design-relevant information that must be taken into account in the development of a prototype.

We draw upon key elements and principles of EBD to guide the Problem Recognition phase through the questions we ask, the data we seek, and the analytical approaches we use to move knowledge into action. This ensures that the outcomes produced can serve as the primary resources required to move responsibly into the next phase of innovation, the Design phase.[5]

## Accountable Humanitarian Innovation

As innovators and humanitarians, we are concerned with fostering discussion about what it means to be accountable in our efforts to leverage the creativity and dynamism of innovation and technology to tackle problems in contexts that are both culturally unfamiliar, as well as insecure.[6] This means asking not only what we *can* do, but also, what

[5] Miller & Rudnick (2011); Miller, Rudnick and Levy (2014)

[6] There is "growing evidence to suggest that humanitarian innovation practices are exposing vulnerable populations to new risks, especially when aid agencies and private sector partners experiment with emerging technologies in operational environments," (Humanitarian Innovation Guide, 2018). Even seemingly successful digital interventions innovations raise questions around the harmful effects of

we *should* do, through innovation. We believe that when innovating in and for disasters and complex emergencies, there are special considerations to take into account.[7] Therefore, we have developed an initial set of principles to help guide us in such work.

These evolving principles include:

- **Being problem-driven**
  We undertake innovation activities from a problem-driven, rather of solution-lead, stance. Therefore, we employ innovation as the means by which to achieve positive impact, and not as an end in itself. We commit to using innovation only to the extent that helps us achieve the goal of positive impact for affected populations.

- **Being contextually grounded**
  Knowing what makes different places and situations different, rather than what makes them same, is critical for creating solutions to problems as they play out in real life. We commit to conducting in situ research, and cooperative and first-hand learning with affected people to the greatest extent possible within a given project and conflict context, for the purpose of ensuring awareness about the kinds of issues being faced and the kinds of contexts in which innovation solutions must "live." Being contextually grounded means solutions are both created from—and tested against—such information.

- **Being evidence-based**
  We commit to the explicit application of information and evidence throughout the design process, not only in an effort to demonstrate need or evaluate effectiveness, but in the development and testing of propositions as well. We apply the Confidence Criteria from the EBD approach to ensure that our propositions and designs are accountable to what we do know, and transparent about what we don't.

- **Doing no harm**
  We commit to the principle of doing no harm from the point of view of both local notions of harm and the potential unintended consequences of any solution or intervention introduced by an innovation process. Under no circumstances should humanitarian innovation lead to intentional harm, unintentional harm, or other negative externalities that could have otherwise been avoided through appropriate review, responsible processes, and proper consideration of local contexts. Applying 'Do No Harm' necessitates an anticipatory approach toward identifying, describing,

experimentation, violations of privacy, and the disclosure of sensitive data that might expose vulnerable populations to new threats to their security, safety, and well-being. By uncritically adopting innovation-centric, techno-utopianism, practitioners are failing to keep in view the experimental nature that characterizes contemporary humanitarian innovation, thereby ignoring or undervaluing the risks posed to vulnerable populations--the human subjects, end users, recipients of this experimentation.

[7] In the Humanitarian Innovation Guide (2018), we have identified the following factors: (1) **Humanitarian Contexts** (the physical, social, and operational "environment" that characterize humanitarian emergencies); (2) **Crisis Affected Populations** (the particular vulnerabilities, needs, and capacities of individuals, groups, and communities that are directly or indirectly affected by a humanitarian crisis): and (3) **Humanitarian Principles and Standards** (the normative principles—such as humanity, impartiality, independence and neutrality—that form the foundation for integrated and widely accepted codes of conduct, commitments, and core standards that humanitarian actors are accountable to). See Humanitarian Parameters (HIF Innovation Guide).

and analyzing intended and unintended impacts that might arise as a result of research and experimentation.

These principles (among others) play an important role in shaping the research agenda, guiding the research methods, determining criteria and protocols for the generation, storing and sharing of project data (see Research Ethics and Data Security below). They also play an important role in evaluating the propositions put forward in a humanitarian innovation process. Learning how to operationalize these principles in practice is part of an on-going (and admittedly evolving) effort and for our team, and an important reflection point for this project.

# Research Objectives

## Learning for Design

Within these larger considerations about accountable innovation, the research of the problem recognition phase has a specific job to do. In addition to identifying the core challenge to address, another primary objective of the first phase of any innovation cycle is to create learning for design. In other words, **to generate the findings and insights that form the foundations upon which any prototype solution must be built**. These foundations support the development of design criteria, enable the development of the design brief, and constitute the raw materials from which prototype propositions are developed.

The research we have undertaken therefore has four primary purposes:

- First, to generate ***formative research*** about contexts, users, challenges, needs, vulnerabilities, threats, and opportunities within CCM networks in Northern Myanmar.

- Second, to use our learning to ***develop initial insights*** to guide the next steps in the innovation process.

- Third, to use that information and those insights to ***refine the design brief*** by clarifying and verifying priority challenges or problems to be addressed with an eventual prototype.

# Research Agenda

## Focal Concerns

As indicated above, this phase of work is being carried out to help us explore whether recent advances in mobile communications technology (1) can be leveraged to address some of the key challenges CCMs currently face in their work, and (2) whether in so doing, they can enable monitors to generate timely, verifiable, and context-relevant information for peacebuilding and humanitarian actors.

Hence, the research objectives for this project direct our attention to two key concerns:

- The ***primary*** focus involves learning about the practices, experiences, challenges and threats faced by of monitors and coordinators (at the village, township, and

district level), as both producers and users of information.

- A ***secondary*** focus involves learning about the information practices and needs of other actors who are users of the information produced by the monitor networks for decision-making and action, such as (1) humanitarian protection actors and (2) peacebuilding and security actors.[8]

## Primary Research Questions

With our focus trained upon the practices and challenges faced by of monitors and coordinators, we have organized the research agenda around a set of primary research questions. These questions guide investigation and anchor analysis, reflect the principles for accountable innovation, and utilize elements of evidence-based design. These questions also ensure we create resources that are both useful to, and usable in, the upcoming phases of design and innovation.

They are:

**RQ1**. What is civilian monitoring (its purpose, functions, practices)?

**RQ2**. How is this work carried out by monitors working as part of the CPS mechanism in Kachin State?

**RQ3**. What are the most critical challenges and risks monitors experience in carrying out their monitoring work?

**RQ4**. Are any of these challenges and risks best addressed through technological solutions?

**RQ5**. Are any of these critical challenges and risks best addressed through other kinds of solutions?

## Areas of Inquiry

As we set about investigating these questions, we paid attention to five general areas of inquiry to help us gain a contextually-grounded and practice-based view of civilian monitoring in Myanmar as it is carried out by the NP-trained monitors working as part of the Nyein (Shalom) Foundation.

[8] While we were able to generate useful learning about the practices, experiences, challenges and threats faced by of monitors and coordinators, as both producers and users of information (i.e. primary focus), due to limitations and constraints around lead time, resources, and security concerns (as explained below), we were limited in our ability to generate granular, verifiable information around the practices and needs of other actors who are users of the information produced by the monitor networks for decision-making and action (i.e. secondary focus).

These included:

**(1) Context**: What is the operational context in which the tool must function? This question directs inquiry in to matters such as: What are the physical, social, technical, political, conflict & security conditions that characterize the contexts in which the tool will be used and needs to function?

**(2) System:** What is the administrative or institutional system in or through which conflict monitoring occurs? Who are the actors that make up this system? What are the key roles played? How do they relate to each other and how do they interact? What are the guiding parameters or structures of this system?

**(3) Practice**: How is conflict monitoring carried out? What tools, methods, and practices are used to carry out the tasks of conflict monitoring? By whom? How are they used (i.e. as intended, with work-arounds or adaptations? Why?) What works, what doesn't, and from whose perspective?

**(4) Data Flow**: What is the journey of the information produced by conflict monitoring across actors, time, channels? Understanding the present data flow - that is, the journey data follows from the observation of incident, to its recording reporting, verification, interpretation, distribution, and use, for example - is essential. What are the phases of this process in practice, and what fail-points are encountered?

**(5) Technology**: Are there existing digital tools that can be adapted to the set of needs and contextual features discovered? A range of digital tools exist which might offer platforms or capabilities that may be relevant for this project. With the understanding and insight gained through inquiry into the areas above, we will then be in the position to ask: Are any of these relevant to the needs and context in Myanmar? Can these be adapted to the local context—and if so, what needs to be adapted, and why? If not, what needs to be done next?

Observations about each of these areas informs our learning throughout.

## Research Methods

A combination of techniques for data generation and analysis were used in an integrated research model to conduct the Learning Phase.

First, as part of our Field Preparation, we produced an overview of the operational context (political, practical, digital) through a Landscape Assessment, which was developed through a desk review of relevant literature and online resources, and by holding a number of consultations with key experts in the field of humanitarian data technologies (such as mobile data management, conflict early warning systems, participatory mapping, etc.). The findings of this assessment were deepened through qualitative fieldwork conducted in Myanmar, and provided a foundation for our analysis here.

With the orientation that this landscape mapping offered, we used a range of qualitative field methods to carry out activities in Myanmar to explore the practices of the CPS monitors in Kachin state, and the institutional system (the mechanism) through which it plays out. Here we employed data generation techniques such as open-ended and depth interviews

and workshop observations and participation. We conducted storytelling and practice mapping activities together with civilian monitors to discern practices of data generation and use, and to map technology use, data flows, and, when possible, identify key areas of vulnerability for monitors. This created a heuristic, which was in turn used to guide data analysis through a series of team activities during the final three days of TPL's visit to Myanmar.

Finally, to make sense of the data thus generated, a range of analytic approaches were used, including thematic analysis and data flow analysis.

## Site Selection

Field work was conducted in Yangon (as the location of NP's head office in Myanmar), as well as Myitkyina, Kachin State, from May 17 – May 31.

The decision was taken to focus on monitoring being conducted in Kachin State for a range of reasons. First, Kachin is among the places of concern that lead to the inception of the project—the state has, for the past few years, been the location of highest intensity conflict with concomitant humanitarian implications. Given restrictions on travel for foreigners, the prevalence of most violence in non-government controlled areas, and the limited information available on conditions in the remote north while there is an active military campaign being waged there by the Myanmar Army, the chance to work directly with monitors living and working in remote areas of the state (like Putao) provided an important opportunity.

Second, as the Kachin CPS network has taken a more independent approach as compared to some other CPS networks, they have had more space to develop their own systems. Hence a focus on Kachin provided a complementary learning opportunity for NP and other stakeholders.

Third, while plans had been developed to carry out comparative work in Shan State, logistical and scheduling challenges involved in arranging interlocutors in that location during the particular week of our visit, compared to the access that was possible to both local and international stakeholders in Myitkyina, lead us to the conclusion that our time would be best spent in Myitkyina where interlocutors were guaranteed. Finally, but not least, having attracted the attention of the special police in Myitkyina, it became evident that it would be unwise for the TPL team to travel independently (i.e. without NP staff and/or CPS interlocutors to join us) to Shan State as planned.

## Activities and Participants

Field work was conducted in Kachin together with NP support staff, members of the Kachin-based CPS network (Bhamo, Putao, Myitkyina, and Mohnyin districts), as well as other actors working on protection and peacebuilding matters in Kachin State (such as various UN agencies and humanitarian NGOs, local activists, journalists, and community-based organizations affiliated with the peace process).

This phase of data generation and analysis (May 17 - 31) included reviewing 25 NP and CPS-related documents (such as external evaluations, strategies, workplans, communications, and reports) as well as conducting 12 semi-structured interviews (with local and international organizations), facilitating 4 storytelling and mapping activities with monitor groups (one per district), and participating in a two-day, end-of-year Evaluation Workshop led by NP staff in Kachin.

Research carried out in Yangon included interviews with leadership of Nyein Foundation, debriefings with NP staff, and interviews with UNDP, Phandeeyar (an innovation hub), and Internews. The TPL team then initiated preliminary data analysis and initial threat mapping activities together in Yangon, before departing to our respective home countries.

Following these activities, we continued remote-based analysis and insight generation, and reporting, employing both collaborative and independent analytic techniques to identify patterns and themes, and an application of threat mapping techniques. (See annex for schedule of key activities).

## Research Ethics and Data Protection Protocols

We have carried out this learning phase through a process that responds to key principles of ***Accountable Innovation***. These principles include:

- Being problem-driven, instead of solution-lead;
- Responding to Evidence-based Design criteria (discussed below);
- Doing no harm; and
- Being contextually grounded and locally-informed.

These principles (among others – see Ethical Guidelines for Humanitarian Innovation) played an important role in shaping the research agenda, guiding the research methods, determining criteria and protocols for the generation, storing and sharing of data, as well as indicating criteria for what propositions to put forward.

First, it was important for our work to be conducted in conformity with internationally recognized **human subjects research standards** and in conformity with **responsible data best practices**.

We therefore:

- **Ensured all interviews and group activities conformed to ethical guidelines set forth by the Belmont Report**: (a) respect for persons, (b) beneficence, and (c) justice. Participants were informed in great detail as to the nature of our partnership with NP, the reasons for our conducting diagnostic research in Myanmar with the CPS network (i.e. that this was not an evaluation), and were informed as to the processes we use for all data activities (how information would be collected, stored, analyzed, and destroyed), and how field data would be used in our analysis and final reporting (i.e. for the purposes of identifying general trends, themes, and patterns only).

- **Informed all participants of the confidential and voluntary nature of the interviews, observations, and group activities, and gained the consent of *every single participant* before proceeding with our activities**. (All participants self-selected / signed up for our sessions, and we assured them that we would not make our findings attributable to any one individual.)

- **Took proper precautions to ensure high standards for data protection and information assurance**. This included: (1) the anonymization of all personally-identifiable information (we did not permanently record the names of individual participants); (2) the decision not to audio record *any* of our sessions (should the recording devices or digital files fall into the wrong hands or be intercepted); (3) regularly backing up all field notes through secured means; and (4) destroying all analog field notes before leaving the country (we kept only securely managed

digital files for our subsequent analysis and reporting work back home) and ensuring operational data security at all times while in country (see below).

## Limitations

Upon award of the HIF grant and successful completion of the Due Diligence requirements, **we were informed that the field work aspect of our project had to be completed by May 30th**.

Initially, the timeline for the research design, logistical preparation and project planning, and preliminary desk research was to be completed in May/June, with field research to be carried out in June/July, and analysis and reporting writing for August/September.

However, due to a number of reasons relating to donor requirements, programmatic cycles, worsening security conditions in Kachin State, and political friction in the peace-process, Nonviolent Peaceforce had to temporarily close out their Kachin-based programs by May 30th. [9] This turn of events significantly impacted our ability to carry out the project as originally designed:

**First, lead time for field preparation was hindered**. Site selection for field research was decided very late into the planning process and only finalized about one week prior to arrival on site. The foreshortened lead-time limited our ability to prepare (orientation to the background of the context for the researchers) and make the appropriate logistical arrangements (meetings with key stakeholders, getting access to relevant internal documentation and contact lists, etc).

**Second, our project was now significantly under resourced** – we had been in conversations with potential donors to provide match funding for the additional 11,500.00 GBP required to cover the costs of the core research team, and with limited time to prepare and carry out the field work, we were unable to acquire that support.

We responded by:

- Rapidly lining up the schedules of our team members to be available to conduct field work in Myanmar in mid-late May. (A number of personal obligations such as family events, holiday time, and pre-existing contractual obligations made this very difficult. Flexibility on the team, however, allowed for this schedule to be met.)

- Providing pro-bono support to the project on the back end of the project, post field work. (The Policy Lab team contributed 11,500.00 GBP worth of support to meet the objectives and deliverables originally outlined in the Project Proposal).

- Cutting costs, where possible. (We decided to leverage the expertise of Adapt Peacebuilding's Stephen Gray remotely, instead of in-situ, for example, which greatly reduced the costs of the field work.)

[9] This meant that NP's in-kind support for the HIF-project (provision of translators, in-country travel and accommodation, administrative support, office space, etc) would not be available to us to draw from, beginning on June 1. It also meant that NP had to conduct their end-of-year evaluation (a two-day workshop, bringing together 45 monitors from across Kachin-state) within a very small time frame (late May).

## Security

Second, carrying out field research in Kachin State (*especially* on matters pertaining to ceasefire monitoring, civilian protection, and human rights issues, and *especially* toward the possible development of digital technology solutions to aid volunteer informant networks in doing this kind of work) engendered significant risks to both CPS stakeholders (such as village monitors, district coordinators, NP staff, and members of local CBOs whom we interviewed for this project) and to the project staff (i.e. the international (read: *foreign*) researchers from TPL).

First, conflict conditions themselves represent a range of particular **challenges for conducting the kind of ethnographic and user-based approaches to learning** and innovation that, in stable contexts, can be less problematic (comparatively speaking).[10] For example, in the context of an active conflict, matters of access and trust, upon which such research and learning depends, can be fraught or impossible to overcome, particularly in a short space of time. Any research team, whether local or international, would need to take such issues into account in the design and implementation of activities.

Second, **worsening conditions in Kachin state** (renewed fighting between EAOs and Tatmadaw, increasing social tensions and communal unrest, protests, bombings, renewed forced displacement, and reports of destruction of civilian property and armed conflict in close-proximity to non-combatants) posed concerns for the project team. We determined that destabilization in the Myitkyina area (caused by increased fighting in the region and displacement) as well as targeted violence toward international aid workers, bombings, and kidnapping were possible, though unlikely.

Third, matters of **surveillance of civilians; intimidation; and unlawful and arbitrary arrest and detention of activists, dissidents, and community leaders** were of serious concern to our project team. The Myanmar Army routinely detains and searches civilians (for example, at designated check points), conducts arbitrary arrest and imprisonment without fair trial, and regularly surveils internationals (either through the use of covert details and informants, or via means of unlawful digital intrusion). We had identified that being harassed or detained by local/national authorities is an unlikely, but possible, situation.

*Members of our own team were actively surveilled by the Secret Police and Special Intelligence Unit of the Myanmar Army throughout the duration of our trip to Myitkyina*. In one instance, hotel informants sent reports to the Kachin State Secret Police that resulted in the Chief of that unit to personally detail the perimeter of our hotel.

We responded to these security threats by:

- Holding **operational security briefings** to provide the team with relevant information regarding possible security threats (e.g. including reviews of UNDSS, Save the Children, and NP situation reports) so that we could make informed decisions about our safety, security, and well-being.

- **Instituting regular check-ins via multiple communications channels** (missed check-ins would signal an elevated protocol, and failed elevated protocols would trigger emergency procedures), and made strict rules about adhering to curfew, protocols

[10] Research activities directed at understanding barriers to effective conflict monitoring could, if not designed and conducted carefully and with the input of local actors, raise the stakes involved for civilian monitors considerably, and present an additional threat to their safety and security.

for passing through checkpoints, learning and abiding by local customs and regulations, and staying in pairs when outside of our hotels, and being accompanied by a Burmese NP staff member throughout field work in Kachin.

- **Taking proper precautions to ensure basic digital data protection, digital security, and digital hygiene**. We put together a mandatory **Digital Security Checklist** for all project staff, to ensure the use of encrypted communications and data storage as well as other methods by which to be protected from attackers when connecting to the internet (via mobile phones, wi-fi access points) in Myanmar.

- **Finally, we made an important decision to table a trip to Lashio**, a second field site, which would have (1) split up our team and (2) introduced a second operational environment for which we were not prepared for. While this second location would have provided interesting and potentially-useful comparative insights, we made the choice to stay with our local guide throughout the remainder of our Kachin trip.

## Outcomes and Contributions

There are several **outcomes** of the research agenda outlined above. Broadly speaking, this research and analysis helps to identify: (1) a range of opportunity areas whereby an innovation process could deliver tangible and practical improvements to CPS monitor's work; and (2) new mission critical knowledge gaps to attend to (in subsequent research);

More specifically, we have used this work to develop an initial Design Brief to help guide concept development for the next phase in the innovation cycle - the design of tools, processes, and protocols that might collectively support solutions embedded within a complex system. The design brief draws upon the observations and findings generated through the research and analysis of the problem recognition phase to outline key issues that need to be addressed, objectives that need to be achieved in response to each issue, and, and criteria that should be met by any proposed design concepts and solutions in order to both address key challenges and needs, while meeting our criteria for accountable innovation.

This revised design brief provides NP and TPL with a shared foundation upon which to focus efforts in this Design phase, and thereby create the grounds for initial messaging for potential donors and supporters.

In addition to these project outcomes, the project makes a range of **contributions** to the humanitarian innovation community. It provides a timely opportunity to generate and test insights around much-needed innovation management methods, techniques, tools, and guidance for the humanitarian innovation ecosystem to benefit from. Our approach to evidence-based design contributes to this knowledge base by creating empirical knowledge on project-level humanitarian innovation, carried out in the field, which could be used to compliment the Humanitarian Innovation Guide.

We expect that this initial research will help shed light on the kinds of practices suitable for the development of *systems innovation* in complex and fragile contexts, therefore contributing toward Lessons Learned, in terms of process and emerging interdisciplinary practices and approaches, and specifically pertaining to navigating both opportunity and risk in the digital age.

# RESEARCH FINDINGS

## Overview

In this section we present the formative learning generated through this research agenda.

We begin with a brief overview of civilian monitoring as practice, and then turn our attention to monitoring and protection activities as it is practiced in Kachin State by monitors and coordinators working as part of the Nyein Foundation's network Having illustrated a basic practice sequence along which monitoring and protection activities unfold, we then turn to a description of the challenges faced along that sequence from the point of view of the monitors and coordinators we had the opportunity to work with, and identify "hot spots" along the monitoring sequence where challenges seem to be the most acute. Finally, we explore the implications of these challenges within the context of the CPS network in Kachin.

Learning about the experiences from the point of view of people carrying out monitoring activities provides us with invaluable information for exploring our innovation objective of addressing some of the key challenges CPSs currently face in their work. As monitoring practice is, at heart, an information practice, and today, information practices are inherently also digital ones our analysis also revealed digital threats, their associated vulnerabilities and consequences.

As a result, we gain a sense of how the practices of civilian monitors interact with both the administrative system of the CPS network, and larger context around them, to create a range of challenges, and vulnerabilities.

## Civilian Monitoring

### **RQ1**: What is Civilian Monitoring?

There are many different approaches to monitoring, and purposes for which monitoring activities can be conducted. According to NP, monitoring—"the practice of observing compliance to a standard,"—is mobilized in support of various actors "to make appropriate and timely judgments and decisions that will improve the quality of the work, ensure accountability, and encourage implementation according to plan," whether that is in service of ceasefire monitoring (i.e. in observance of implementation and/or violations of ceasefire agreements); for the direct protection of civilians (i.e. to provide physical presence in insecure areas and engage with armed actors to minimize harm to civilian populations); for the facilitation of humanitarian assistance (i.e. to inform response strategies, and communicate directly with vulnerable populations and humanitarian agencies); or for human rights purposes (i.e. to improve human rights protection through accountability and advocacy work).

In contrast to formal ceasefire monitoring, which is conducted by actors mandated by the ceasefire parties and tends to focus on military matters, informal, civilian approaches to ceasefire monitoring (1) focus more on the impact that ceasefire violations and armed clashes have on civilian populations (such as community protection needs); and (2) rely on direct, community-led field presence for a more localized, bottom-up, and grassroots

approach for enabling direct protection and local response to the needs of conflict-affected communities.[11]

Regardless of the particular purpose, focus, and approach, however, monitoring is concerned with the practices of collecting, verifying, and communicating information, according to some set of criteria, and both within a particular system of actors, and across different systems of actors. It is crucial to note that such information is generated with a view to being used - in taking decisions and actions - whether by monitors themselves, or others. Monitoring is therefore, fundamentally, a practice concerned with the generation and application of information.

# Civilian Monitoring in Kachin State

### **RQ2**: How is monitoring carried out in Kachin State?

With this project, we are interested NP's particular approach to CCM, and how participants in the Kachin CPS network carry this model out in actual practice. This approach is special in its integration of peacebuilding objectives and techniques, such as **Unarmed Civilian Protection** (UCP), into monitoring practices, creating new opportunities to build and improve relationships out of monitoring, documentation, and reporting activities.

The process of civilian monitoring in Myanmar is based on NP's approach to the theory and practice of Unarmed Civilian Protection (UCP), which is defined by NP as "the practice of deploying unarmed civilians before, during, and after violent conflict to prevent or reduce violence, to provide direct physical protection to other civilians and to strengthen or build resilient local peace infrastructures." Key aspects of UCP, for NP, "include (1) a focus on proactive engagement with all key actors before, during, and after incidents of violence; (2) a focus on encouraging potential perpetrators to minimize harm to civilians rather than blaming perpetrators for their actions; and (3) a focus on direct physical protection of civilians by civilians."

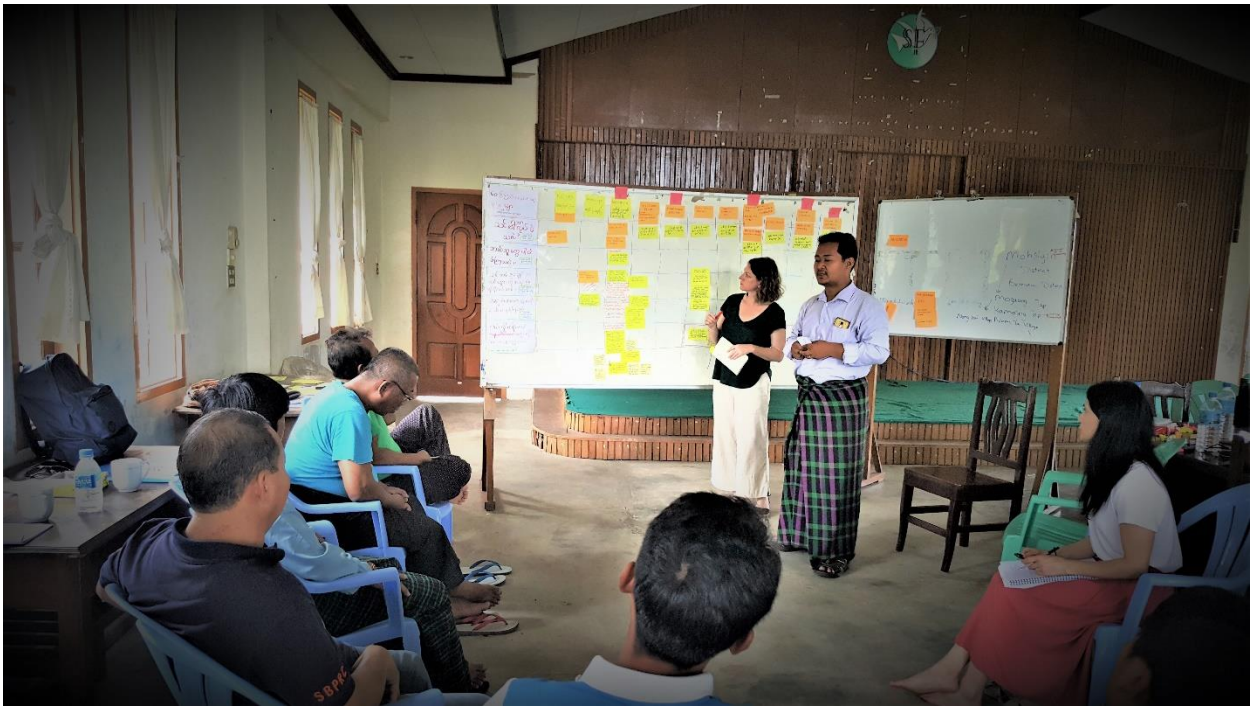
NP's efforts to support civilian monitoring networks —leveraging UCP – center around the dual goals of contributing to stable ceasefires and improved civilian protection. According to its 2016-2018 Project Plan, the overarching goal of NP's efforts in Myanmar is therefore to prevent or reduce violence, protect civilians from violence and promote nonviolent resolution of conflicts. NP doesn't view the compliance or the continuation of ceasefire agreements as its goal, but as a means – and at this point in time the most promising means – to increase security of conflict-affected communities across Myanmar and create a space for peacebuilding efforts.[12] NP also learned that in a context where formal ceasefire implementation mechanisms are weak or inexistent, like Kachin, local communities have found more meaning in directly (often quietly) resolving protection concerns with local commanders than reporting violations to a system that operates outside of their control, is often weighed down by political dynamics, and designed to prioritize military matters over civilian affairs.

[11] Documentation, verification and reporting are, in such views, considered to be insufficient for the protection of civilian populations.
[12] For NP, this means (a) maintaining ceasefires and minimizing human rights violations, (b) improving the protection of civilian populations, and (c) increasing awareness and capacities among civilian populations to enable active participation in the peace-process.

This has led to a type of monitoring that is less focused on gathering information for the benefit of decision makers, to seek accountability, or to influence public opinion than on formulating appropriate and immediate responses to protect civilians from imminent threats.

After a review of documentation describing and depicting NP's innovative model, and observing activities and discussions during the May evaluation workshops conducted by NP, we engaged 4 monitoring teams from different areas of Kachin in storytelling and participatory mapping activities. This allowed us to hear about how civilian monitoring can unfold in actual practice and how monitors describe those experiences from their own point of view, to help us learn about their practices and explore some of the key challenges that they face.

The stories we heard from monitors revolved around different kinds of incidents, including (1) a case of forceful recruitment of minors; (2) the documentation of a fatal landmine incident; (3) resolving disputes related to unlawful taxation; (4) and a missing persons case that rapidly escalated into a high-profile war crimes investigation into unlawful detention, torture, and execution of non-combatants.



While there was some variation in the descriptions of the specific steps taken by different teams (due in part, for example, to the varying nature of the different cases), or represented in documentation from networks in other states, we nevertheless discerned a central, and common sequence of general phases and practices that characterize the approach of civilian monitoring, as carried out through the NP framework in Kachin State.

We believe this sequence reflects the common training monitors have received from NP, but it also reflects the structure of the CPS network through which it is carried out. This is a

highly complex, multifaceted and multilayered administrative system, linking village, town, and state-level actors through a multistep and multi-phased process.

Though we have only been able to develop a very superficial understanding of this system in our brief time in Myanmar, we believe the general monitoring sequence that is carried out in most cases can be summarized in the most basic terms as follows:

**TEXTBOX | Kachin CPS Sequence**

**(1) Notify** – The Village Monitor is made aware that there has been a conflict or civilian protection-related incident, or that there is a concern or grievance in the community.

**(2) Mobilize** – The Village Monitor informs relevant stakeholders within the community (such as religious leaders, village administrators, or members of the Village Committee) and wider mechanism (such as Township Coordinators), according to protocol, which triggers a set of actions, according to the nature of the incident.

**(3) Verify** – The Village Monitor and other network actors (such as the Township and District Coordinators) confirm the occurrence and details of an incident (i.e. accuracy and validity), and assess the situation in order to determine the nature of the incident and how civilians have been affected by it (e.g. by travelling to the site, speaking to witnesses, identifying physical evidence, collecting other pertinent data).

**(4) Report** – The Monitor and Coordinators create and file a formal report about the incident to the State Secretariat and Project Team (i.e. Nyein) staff.

**(5) Plan** – Network leadership—at the township and state levels, and also in consultation with other relevant formal authorities, local partners, and sometimes in coordination with international organizations—develop a plan of action in response to the reported incident.

**(6) Share Information** – Monitors and Coordinators disseminate information (about the incident that has happened, the actors involved, and the response that has been planned) with the range of external stakeholders (such as local authorities, community leaders, armed actor groups, humanitarian organizations, etc) who are implicated in the planned response.

**(6) Respond** – The designated actors (typically the Village Monitors and Township Coordinators) carry out the agreed the plan of action for responding to a ceasefire violation (e.g. facilitating negotiations between parties to the conflict) or civilian protection concern (e.g. supporting the direct provision of humanitarian assistance, or by supporting an on-going investigation).

**(7) Follow-up** – Relevant actors from within the network follow up to ensure agreed resolutions are implemented and communicated with both families and communities about the status of a resolution and/or outcomes.

# Challenges Experienced by Monitors

**RQ3**: What are the most critical challenges and risks monitors experience in carrying out their monitoring work?

The tasks involved in the civilian monitoring sequence described above make for inherently difficult and dangerous work. With this research, we are focused on learning things about that work that can help us respond to the project's initial query: whether digital solutions might be useful in addressing key challenges monitors face in carrying out their work. We therefore direct our attention learning from monitors and township coordinators (henceforth "monitors") about the types of things that can make it difficult for them to carry out their monitoring work, that can hinder them from doing it effectively (contributing to intended outcomes) efficiently, and safely, or that can even prevent them from doing it all.

By looking across the 4 different cases described to us by the four monitoring groups, and the examples discussed in the context of the NP workshop, we found that several of the most important challenges faced by monitors in carrying out the activities of the monitoring sequence described above clustered around three key areas: (1) the operational context in which monitoring is being conducted; (2) the practices being used in order undertake the various tasks involved; and the (3) administrative system through which these are carried out.

We offer a brief description of the challenges inherent to each area below in an effort to characterize just some of the challenges that emerged prominently in the data we generated through our activities with monitors, NP staff, and stakeholders from other organizations active in Kachin. Our objective in this section is to capture key features that characterize central challenges to carrying out monitoring work, as described by those who do it.

## Context Challenges

Several of the challenges that monitors face in carrying out their work stem of course from the very context in which the activities play out. We use the term "context" here to refer to the physical, social, technical, political, conflict & security conditions that characterize the operational environment(s) in which monitoring sequences unfold. Some examples of these context-specific challenges include:

*(1) PHYSICAL ENVIRONMENT*

In Kachin State, a mountainous region characterized by dense forest and connected by few roads, the physical environment itself can present a challenge. For example, incident verification, reporting and follow-up activities often require monitors to travel to the incident site, which can be remote and often difficult to reach due to challenging terrain (e.g. dense forest) and a lack of infrastructure (e.g. poor quality or non-existent roads, railways, waterways, and domestic airports make travel to many areas almost impossible).

One monitoring group for instance described hiking for several days through remote forest in order to reach an incident site where several minors were being held by an EAO.[13]

[13] Members of the Putao District Sumpi Yang CPS shared with us a harrowing story of courage, determination, and true grit that is a testament to the network's success and the hardship of its members. A small team of Village Monitors and Township Coordinators garnered safe passage from KIA leadership to make an arduous three day trip on foot to a remote KIA outpost, where they engaged in negotiations

The physical environment can present monitors with physically challenging journeys, can put their physical well-being at risk, and can and make it difficult for them to reach sites quickly enough to carry out their work effectively.

*(2) CONFLICT & SECURITY CONTEXT*

The political environment in northern Myanmar provides both the need and motivation for civilian monitoring, and by default, is a source of some of the most difficult challenges for carrying this out. Renewed fighting between the Kachin Independence Army (KIA) and the Myanmar Army has generated significant security threats for civilian populations and the community-based organizations (CBOs), religious groups, and humanitarian and human rights actors who serve them.

These active conflict conditions mean that in addition to the challenging physical conditions of travel, the monitors frequently find themselves in, or must enter into, a range of unstable environments and situations that are a result of the on the ongoing and evolving conflict.

For example, monitors described regularly encountering armed checkpoints; being required to enter into areas where a landmine has detonated, and where other unmarked mines or IEDs could be present; needing to access sites where hostilities were escalating; entering into IDP camps, which can be chaotic and insecure places; and visiting the camps of the military or EAOs (as in the example above), where their personal safety may be at risk.[14]

According to one group:

> *"There are too many checkpoints to cross to reach communities. …Once we could not deliver medical aid [to a village] because we were stopped at a checkpoint and did not have the right documentation."* - Monitor

Furthermore, it is widely known that the Myanmar Army maintains a policy of constant surveillance of its citizens via strategies that encompass conventional security threats, (such as the stop-and-search of civilians by armed actors, regular surveillance of civilian activities and/or their abodes, and the use of covert informants), as well as new and emerging digital threats, such as surveillance of mobile, internet and other digital communications.[15] These

(based on violations of the ceasefire agreement) to persuade a battalion commander of to release thirteen children that were kidnapped from Sumpi Yang village and forcibly recruited. Eventually, the team brought all 13 children back to their families.

[14] In Kachin, access to areas of concern – whether or not that exhibit direct security threats to civilian populations – are prohibited by the Myanmar government, not only for the purposes of verification, documenting, and reporting ceasefire violations and/or protection concerns (which have been the foci of the network) but also for the provision of life-saving humanitarian assistance. This is true for both international staff and, more recently, for national staff and local volunteers. In recent months, restrictions have been heavily enforced through the use of check-points, restrictive travel authorizations, and the prohibition of international staff from many districts and townships in the state.

[15] Members of our own team were actively surveilled by the Secret Police and Special Intelligence Unit of the Myanmar military throughout the duration of our trip to Myitkyina. In one instance, hotel informants sent reports to the Kachin State Secret Police that resulted in the Chief of that unit to personally detail the perimeter of our hotel. Such instances are, of course, not unique when tourists or international staff visit places like Myitkyina and bring unwanted attention from the state intelligence apparatus.

and a host of related issues (address in closer detail in Section 3) play an important role in shaping the operational landscape that monitors must navigate.[16]

*(3) NATURE OF RELATIONSHIPS*

While the political conflict gives rise to many physical contextual challenges (e.g. of access and safety, as described above) so too do the difficult relationships that result from the political tensions and conflicts between civilians, military, EAOs, and other ethnic groups. As monitors, NP practitioners, and the literature all convey, the success of civilian monitoring is dependent upon the ability of monitors to foster relationships of trust with a wide range of actors, including with those who are sometimes hostile to them.

Monitor's explained that poor access to or relationships with the military for example, can present obstacles to key protection tasks, such as negotiating the release of civilians, addressing violations to the cease-fire agreements, or providing safe passage to civilians, in addition to posing issues for the safety of individuals.

Likewise, monitors have had to work hard at building trust with communities as well, who have lived through a conflict in which neighbor has been pitted against neighbor, sometimes in surreptitious ways, by the government. When community members do not trust the monitor's intentions, or affiliations with other conflict actors, this too becomes a central barrier to carrying out monitoring in several ways. First, it can make it hard to generate reliable information, and second, it can make it difficult for monitors to assist in the protection of civilians.

*(4) CONNECTIVITY*

Connectivity is another feature of the operational context that presents challenges to monitoring work. While Kachin already has a limited digital infrastructure, which is frequently exacerbated by the systematic disruption of telecommunications infrastructure in remote, hard to reach areas as part of its notorious "four cuts" counter-insurgency strategy. This strategy, which has featured in the recent escalation of hostilities in Kachin, aims to cut off food, funds, intelligence and popular support of armed resistance groups fighting for self-determination, and directly targets civilians in conflict zones.[17]

By cutting off communications infrastructure, the government blocks both the ability to convey, and to access, potentially life-saving information for vulnerable communities caught in harm's way, or in need of assistance.

Such information is essential for monitoring work. For those living in remote areas, unreliable connectivity due to poor information communications infrastructure (although this is gradually improving), or the deliberate disruption of internet connectivity and/or mobile

[16] The surveillance activities conducted by the military and state authorities are therefore an ever-present concern for village monitors, township and district coordinators, and to the partner organizations of the CPS. These concerns influence almost every aspect of how monitors carry out their work, especially pertaining to how information is gathered and communicated, but also with respects to the activities monitors conduct as part of response.

[17] The strategy was recently revived in Kachin State when the renewed fighting broke out in mid-2011 with the Kachin Independence Army (KIA), the armed wing of Kachin Independence Organization (KIO), which is calling for a political dialogue with the government.

telecommunications by the military as part of their "four-cuts" strategy, can impede the often time-sensitive verification and reporting work of monitors.[18][19]

*(5) URGENCY OF INCIDENTS*

The network engages with a wide range of issues, ranging from unlawful taxation, land grabbing, forced recruitment and abduction, to the systematic targeting of civilian populations by armed groups. But when urgent incidents occur - those in which the wellbeing of people is at immediate and serious risk, and/or there has been a violation of key agreements - monitors must act quickly in order to try and limit or prevent violence and carry out protection.

> *"Sometimes we must skip steps when an incident is urgent. For example, when the KIA and the Tatmadaw started exchanging fire near a village, the monitors had to immediately attempt negotiation with the military groups [without waiting for a more specific plan of action from the district and Secretariat offices.]."* - **Monitor**

The need to act fast presents a range of challenges, including the rapid mobilization of both human and material resources, which may or may not be readily available, and the need for monitors to find a way to balance human rights reporting requirements with immediate protection needs – or to potentially choose between them.

## Practice-based Challenges

Another set of challenges faced by monitors in carrying out their work stem from the practices involved in monitoring itself. We recognize that monitoring is inherently challenging, and that we cannot begin to fully capture the scope and true nature of that challenge here. However, in looking across the data generated through our research, a few key features stood out concerning the things that monitors do, and how they do them, that systematically and consistently present challenges and concerns.

*(1) INTERACTING WITH CONFLICT ACTORS*

In carrying out civilian protection and incident response activities, monitors are frequently required to engage directly with potentially threatening actors, such as EAOs and the military, or agitated communities or community members, to verify or otherwise address incidents. Some monitors expressed understandable concern about such interactions, or described that sometimes they are very intimidating, and some reported feeling underequipped to skillfully negotiate with such actors in an effective and safe way.

In addition, interacting with the military and the EAOs can present a risk of association in a climate that is marked by suspicion and fear of violence.[20] In other words, to be seen

[18] As we will discuss in the section on Vulnerabilities, unreliable connectivity not only disrupts monitors' ability to communicate with the network and relay critical incident and verification data, but it can also put them at risk, as monitors resort to analog methods for storing and transporting sensitive data (such as storing photos on their phones, or carrying hand-written notes or hard copy documentation from the area of concern to the closest wi-fi access point).

[19] At the same time that a lack of connectivity presents very real challenges to conducting monitoring work, connectivity in and of itself introduces risk to monitors in their work. We take this up in detail in the later section on Threat Analysis.

[20] Given that EAOs are considered illegal entities. monitors can be detained for meeting with them as outlined in the unlawful associations act.

speaking to different actors, and collecting information about such events, can place monitors as well as victims and other informants at risk of violence themselves (e.g. by perpetrators or their allies who may wish to prevent verification from occurring). Monitors explained that this can make some actors reluctant to speak, and can therefore present monitors with challenges of access (both to sites and information) that they require in order to verify the nature and impact of incidents.

*(2) DEALING WITH SENSITIVE INFORMATION*

Sensitive information is broadly understood as information having the potential to cause or lead to serious harm if lost, stolen, disclosed to hostile actors, or misused, even by allies. By this definition, the information that monitors collect, share, and have access to is highly sensitive in nature. Because of this, the very act of collecting, managing and communicating sensitive information can put monitors at constant risk. Handling sensitive data in a safe way requires a degree of knowledge and skill that is presently not available to most active monitors, making a challenging situation also a dangerous one.[21]

*(3) VARIED PRACTICES*

We have previously articulated the representative sequences of practices and the common features that characterize the approach of civilian monitoring, and how those practices are mobilized through the NP/Nyein framework in Kachin State. However, we have also observed some variation as to how this sequence of work is carried out on the ground, when it comes to the techniques and tools used by the monitors, the information outputs produced by them, and the methods and systems used by the Secretariat and Nyein project team to manage this process.

On the one hand a variation in practices can be described (as it is by some NP staff) as useful adaptation to circumstances – such as the nature of the physical and conflict contexts, skills and resources available to a particular team, and the requirements of the case at hand. But on the other hand, this variation can cause challenges where procedure becomes confused, or access to needed support (whether in the form of expertise, political influence, or material resources) is not available or provided.[22]

*(4) LIMITED AWARENESS, GUIDANCE OR SKILLS TO SHAPE INFORMATION PRACTICES*

Monitors and coordinators use many different practices to share information. These include sharing information verbally in person (including interviews, informal conversations and meetings, and formal meetings), verbally over the phone, sharing handwritten reports, and sending texts/SMS and photos via mobile phones, e-mail, or over FB messenger.

But while selecting the method/tool of information sharing seems to be influenced by balancing between several factors,[23] this selection can only be made from within the range of practices and techniques about which monitors are knowledgeable and aware. This is

[21] For more detailed analysis see Section 3.

[22] In reviewing internal NP materials, for example, it appears that the organization is responsible for ensuring the appropriate functional monitoring systems and structures are in place. And yet, our review suggests that these commitments have not yet been developed as resources for the network, or are not of sufficient quality to be of use to network stakeholders.

[23] Factors include, for example: the urgency and sensitivity of the situation at hand; security concerns about the safety of the monitor and/or victims and their families; systemic requirements of the CPS; legal requirements (e.g. in cases when they are aware there are legal frameworks to take into account, such as when they know they are working on a HR violation).

something they themselves have cited as a challenge, noting a lack of specific training around data management generally, and the (safe and systematized) use of technology in such practices more specifically.

Monitors expressed a keen interest in developing skills for making better use of their phones for collecting storing and sharing information safely and effectively, and in increasing their awareness, for example, of what tools (such as apps) might be of use to them for doing so. When asked where they received information or guidance on such matters, they cited each other, and at least one team said they received some guidance from the clerk at the kiosk where they purchase their phones. Hence, we have observed that a key challenge monitors face concerns having fairly limited skills and knowledge around the range of technical options relevant to safe and effective information sharing.

## CPS System Challenges

A third set of challenges that monitors must contend with in carrying out their work, we found, stemmed from the CPS system itself. While we make no claim of having done a rigorous mapping of the network sufficient to a comprehensive understanding of the complexities involved in the structure and administrative functioning, certain kinds of CCM-related challenges consistently featured in the descriptions of different cases and experiences by different groups. When we consider monitor's challenges against descriptions of the network's administrative structure, procedures, and resources, a trickle-down effect comes into view concerning the ability not only of the monitors, but also of actors at different levels in the system and locations in the state, to implement response.

*(1) ADMINSTRATIVE BURDENS*

Monitoring activities operate within a complex organizational structure that has divergent and what appear as often cumbersome administrative and reporting requirements. For example, we have learned that monitors and coordinators (about 95 of them in Kachin) are required to submit weekly and monthly Activity Log reports to their supervisors (who also submit weekly and monthly aggregations of these reports), in addition to incident and verification reports. These Activity Logs detail and track a wide range of activities carried out by the network – i.e. not just matters of ceasefire violations or protection-related incidents, but the daily activities of monitors and events in their communities as well. Although we were not able to learn a clear description of what this detailed information is needed for, or specifically how it is used, we have understood that these and perhaps other reports are collected, consolidated, and shared up the organizational hierarchy.

The volume of reporting required from monitors (who are largely a volunteer staff and whose availability is already thinly stretched between operational, administrative, and income-generating activities) appears to present them with a significant administrative burden to address (and it may not be the only one).

*(2) LIMITED RESROUCES*

The CPS system is described by its participants as being resource-poor.

For example, human resources remain a concern for monitors and coordinators. Some monitors feel that there are not enough monitors on the ground to efficiently cover their regional area. For those regions with remote villages, a lack of in-situ capacity puts a burden on monitors (who may not have access to transport vehicles) to travel across

difficult terrain or long distances to carry out routine and/or incident response activities. Another example concerns the allocation of funding to monitors for activities. As township coordinators explained to us, Nyein Foundation allocated funds monthly in response to needs indicated by monitors' and network's monthly activity reports. This monthly funding cycle creates a resource gap whereby administrative processes fall behind time-sensitive requirements for incident response.

As a result, monitors are often left to pay out-of-pocket for the resources they need to carry out (often) urgent civilian protection activities, making responses dependent upon the personal resources monitors may have available at the time.

*(3) ADMINISTRATIVE BOTTLENECKS*

Whether they are a function of limited resources, or bureaucratic complexity, monitors contend with a number of administrative bottlenecks that make it difficult to carry out their work. For example, it was noted that budget for the networks of both Kachin and Shan states is controlled by a single individual at the Nyein Foundation, creating an administrative bottleneck that leads to delays in the processing of monitors' expense claims such as mobile phone costs.

Furthermore, the CPS network is a highly bureaucratic and hierarchical system, which itself endeavors to work in the context of broader legal frameworks at multiple levels (township, state, union). Therefore, there is sometimes a delay in securing the regulatory permissions that may be needed in order, for example, for some response strategies to be developed, and responses actions to be taken.

Monitors expressed some frustration at the delay in response time from further up the chain within the CPS system, and the hindrance this caused to responses at the local (village) level.

*(4) ABSENCE OF SYSTEM-WIDE TOOLS*

We observed that most community-level monitors use their own (personal) smart phones to perform their monitoring tasks, and that use is limited to basic applications and platforms such as photos, SMS, Facebook and voice calls. Coordinators and Monitors at the township and community level reported that while some offices may have one or two computers for the most part people do not have regular access to laptops, voice recorders, or cameras that could aid them in the verification and reporting of incidents. The lack of system-wide technical tools for carrying out monitoring tasks goes hand in hand with the variation of practices described above, and can lead to inefficiencies at different points across the system.

*(5) CHANGING STATUS*

At the time of our fieldwork, there was much discussion about the progress being made in the network's efforts to gain official status through government registration. From one perspective (an institutional one), this was described as a development that could help monitors achieve legitimacy and leverage with military actors, and therefore greater security. From another perspective, some monitors worried that this official status could undermine their standing with the community, who may lose trust in any group affiliated with the government. This highlights an unfortunate tension between security and effectiveness that monitors must grapple with in their interactions with community members,

who ask directly about the name change this shift in status has precipitated, and wondered aloud about what this means in terms of monitors' affiliations, loyalties, and trustworthiness.

### International Response System-related Challenges

Finally, key features of the broader international response system of peacebuilding action and humanitarian response presently active in Myanmar stood out as matters of concern in this basic review of challenges that monitors must contend with in conducting their work.

*(1) EMERGING PARALLEL SYSTEMS*

We learned from members of the Protection Working Group (PWG), (ICRC, various UN agencies, and international NGOs) that there is an urgent need in Kachin for verified protection-related information regarding displaced and besieged populations and host communities—especially those in remote or otherwise inaccessible environments.

While there are efforts to improve information sharing on such matters among various local and international actors, in the face of this urgent need many INGOs lacking direct access to conflict-affected areas in Kachin, are starting to leverage their own local informant networks for carrying out periodic needs assessments or verifying incident reports.

These parallel networks, and the use of their information by international actors, engender enormous risks for local intermediaries, and present monitors with challenges on many fronts - operationally, financially, and in terms of security.

**In considering the challenges described here**, we can see that some of them emerge either because there is a *barrier* that hinders or blocks the successful delivery of an activity, program, action, or task, or because there is a *gap*—something that is required to deliver on an action, activity, or program effectively and efficiently, is missing.

In the context of community protection and civilian ceasefire monitoring work, we can therefore define challenges as: *the combination of barriers and gaps that have a negative impact on the performance, functionality, and effectiveness of the monitoring network toward the achievement of its core strategic objectives and/or towards positive impact for civilian populations*.

Articulating these pressing challenges, in this regard, helps us begin to identify key areas **where significant improvement is possible, and if made** would be consequential for the network's ability to fulfill its explicitly defined objectives.

## Vulnerabilities Within the Network

In our initial assessment of the critical needs, challenges, and barriers monitors experience in carrying out their work, we have uncovered a number of concerning **vulnerabilities** within

the monitoring network that could significantly expose the monitors, the data they collect, and the populations they serve to a range of conventional and emerging **threats**.[24]

These vulnerabilities fall into four broad categories concerning data security and digital safety: (1) Lack of a systemic approach; (2) limited awareness and skills; (3) unsafe practices, and; (4) sensitive data.

## Lack of Systemic Approach to Data Security

Monitoring and reporting operations require digital security and data protection policies and protocols to set minimum acceptable standards that can be used to both guide and evaluate practice and behavior; foster staff capacity and development; and guide decision making and oversight. The absence of these resources can result in an inability to detect, respond to, and recover from critical incidents (i.e. compromised systems, data breeches, etc.) in a systematic or reliable way.

Anecdotal evidence collected by our team suggests that these measures either have yet to be developed, are not yet robust, or not being implemented consistently. This suggests a lack of prioritization of digital security and data safety in the operational mandate of these organizations. We see this reflected in the absence of dedicated mechanisms, requirements, incentives, or capacities for digital security and data protection compliance—to a set of defined technical standards—among network members, or any related compliance mechanisms.

As a result, NP and Nyein Project Team staff have a very limited vantage on technical compliance, adoption, and uptake regarding data security and protection practices of the monitors and coordinators. They reported limited knowledge on if and how monitors might be making use of digital security precautions. Furthermore, it appears that such matters are not integrated into monitor selection, team and system design, or capacity building.[25]

## Limited Awareness and Skills for Safe and Secure Practices

We have observed that network staff at all levels are operating with limited data literacy and digital hygiene, despite the centrality of digital information practices to their work, and the heightened levels of threats present in their operational context.

[24] Threats are a function of Risk: a calculation of likelihood that an adverse event (a threat) might play out in a particular context, and the impact (or consequences) of the event for the referent object (or objects) in question. Calculating risk helps us make assessments about potential courses of action and their implications for those involved. We can articulate risk profiles (the likelihood and impact of an adverse event) based on this very simple formula.

[25] Despite the high risk involved in collecting, storing and sharing sensitive information for incident verification and reporting, digital security training for monitors by NP is limited to few and basic strategies such as forwarding and deleting photos from smartphones. While some monitors may attempt to employ ad hoc strategies in an effort to reduce the risk posed to them in the collection, storing and sharing of verification and reporting data, such examples remain both limited and isolated. Currently there is no strategy in place for the development, systemization and diffusion of safe and secure data management practices and protocols across the mechanisms.

Digital hygiene describes the attitudes, behaviors, and practices associated with "healthy" use of digital devices, particularly around matters of security and privacy. This typically includes account management (2FA, password manager), communications (encryption), storage (encryption, back-up, usage of third party platforms, etc), and safely navigating online space (VPN, https secure, digital traces, social media, default settings).

We have noted very low data literacy among members of the CPS, and (generally) poor digital hygiene. While monitors are aware that data collection and handling creates personal risk, whether or not through digital means, they admit they do not possess skills and knowledge to address these risks through more secure digital protocols and better use of hardware, software and non-digital tools and methods. As a result, few, if any digital security measures are employed by monitors and mechanisms when using their mobile phones, laptops, or other connected devices.

According to two Monitors:

> *"We need technical support with: downloading data files; use of the internet; better connectivity, and; sending photos for reporting…We are always reminded by the secretariat to keep [incident] photos and information safe, but we are not taught many techniques for doing so – only to delete photos once we have sent them."*

In fact, there are some practices around how the monitors store and transmit digital data that are misinformed, which actually increase the risk of the monitors. As the first line of verification and response to civilian protection incidents, monitors represent "ground zero" with respect to the handling of sensitive information and personal and civilian data, yet their data security awareness and training remains rudimentary at best.

## Unsafe Practices

This state of affairs leads to a number of unsafe practices at both the institutional and individual level:

*1. RELIANCE ON PERSONAL AND SHARED DEVICES AND ACCOUNTS*

We are concerned of the extent to which monitors, coordinators, and other support staff rely on personal equipment to attend to monitoring work, and the degree to which they maintain separation between their personal and professional identities and digital accounts when it comes to their monitoring work.

Reliance on personal devices, social media, and communications accounts significantly compounds known vulnerabilities by increasing the attack surface of the system in question (i.e. outdated software or variance in tools, apps, plug ins), and complicates diagnostics and recovery work in the event of a successful intrusion or attack (i.e. loss of standardization and control). Personal-professional integration of devices and accounts also exposes monitors' personally-identifiable information through tracking and metadata and left over data exhaust from digital traces or signatures that users leave behind when they conduct their work online.

Civil society organizations are often especially vulnerable to these kinds of attacks if they are known to share computers, accounts, internet access points, which means large amounts of data can be compromised if attackers can breach only a relatively small number of devices and accounts. This results in sensitive information being managed with

unsecured (or potentially compromised) devices and puts monitors' personal safety at risk and leaves their data vulnerable to digital surveillance and attack.

*2. VARIATION IN WORKFLOW*

As noted previously, we have observed notable variance as to how monitoring work is carried out on the ground, when it comes to the techniques used by the monitors, the information outputs produced by them, and the methods and systems used by the Secretariat and Nyein project team to manage this process.

However, there appear to be no policies and protocols for their use (verification and reporting protocols do not include technique or application-level specificity), and our diagnostic activities revealed significant diversity in terms of tools, platforms, applications, and systems in use by the monitors that cannot be explained by localization and adaptation needs and environmental or contextual constraints.[26]

Coupled with unclear or non-existent data protection and digital security systems, policies, and procedures, this variation presents significant risks to the network, when it comes to matters of surveillance, search and seizure, and open-source monitoring. Overall, the more variation there is at each stage of workflow (i.e. data acquisition and storage, organization and tasking, analysis and interpretation, and the generation and dissemination of information products) the greater the attack surface is for the network as a whole.

*3. RELIANCE ON THIRD-PARTY PLATFORMS*

Currently, the CPS network uses and relies on the use of open and unsecured digital tools, networks and systems for their communications, and for the gathering, storing and sharing of sensitive data related to incident reporting and response activities.

At the local level, monitors are not provided with secure tools by the network and instead use basic applications and platforms such as photos, SMS, Facebook and voice calls on personal devices and smartphones, all of which are highly vulnerable to tampering, surveillance and seizure by military agents. As sensitive information flows from monitors throughout the complex organizational architecture of the network (and its partners), the system-wide use of personal mobiles, open platforms and computers running on unsecured networks further compounds personal and data security risk.

Reliance on popular third-party communications platforms (Facebook, Youtube, Google, etc) for work is problematic for the network, because these platforms don't offer default settings that would naturally protect the data of higher-risk users (such as 2FA, or limits to sharing and tagging). Users of these platforms will always find approaches to protect their privacy (and that of their partners and sources) insufficient because the systems do not belong to them.

Examples of network-wide data security vulnerabilities encountered during the research phase include (but are not limited to): i) the widespread use of Facebook messenger; ii) ad hoc data management and "security" practices employed by monitors; iii) unregulated multi-user access to office laptops and desktops; iv) a lack of established staff protocols

[26] Village monitors, for example, differ in their use of web-based messaging applications, even within the same District, Township, or Village Track. The same appears to be true for usage of other collection, storage, and communications applications and platforms.

and training for digital security; and; v) inconsistencies in the adherence to safety protocols for the safe storage and archiving of incident reports and other sensitive information.

*4. FAILURE TO CALIBRATE DATA SENSITIVITY*

We are concerned with the extent to which Nyein and NP can calibrate the sensitivity of the highly-granular, real-time information being generated, stored, aggregated, and shared within and without the network on a daily, weekly, and monthly basis. The network appears not to distinguish (and therefore take the appropriate pre-cautions) between highly-sensitive (such as PII, DII, actionable intelligence, and evidentiary data) and less sensitive information generated through the sequence of monitoring work, as there is no readily available network-wide guidance for compartmentalizing sensitive data or treating this kind of information with special care (i.e. protocols and requirements).

*5. LACK OF DATA MINIMIZATION*

We are also concerned about matters of data minimization. Defined as the effort to collect or generate only the minimum required information necessary to achieve programmatic outcomes, data minimization requires that project teams identify--at the outset--the information needed to fulfill advocacy, operational, and evidentiary requirements, and collect nothing more than what is needed.

And yet, the network requires the regular reporting of Activity Logs without a strong case to what this detailed information is used for. Monitors and coordinators (about 95 of them in Kachin) are required to submit weekly and monthly reports to their supervisors (who also submit weekly and monthly aggregations of these reports)—outside incident and verification reports – that detail and track a wide-range of activities carried out by the network. The scope of this highly sensitive and valuable intelligence should not be underestimated: over a 12 month period, we are looking at around 5,000 weekly reports, and 120 monthly reports, fed into a system that we already know exhibits poor data protection and digital security practices. This information—simply by virtue of the fact that it exists—puts the CPS network, its partners, and the community members who are involved at great risk.

*6. DATA SHARING*

Network members routinely interact with local community members and partner organizations outside of the network to help carry out CCM activities, or to share information pertinent to the work of other civil society groups. These interactions with outside actors and systems elevate data security risk by: i) decentralizing the control of sensitive information, and; ii) increasing the digital attack surface as information flows through unsecured networks and devices outside of the mechanism and is handled in unknown ways. In the contexts of the unsafe practices discussed above, sharing data outside the network can makes monitors, victims, and the network dependent upon the good judgement and safe practices of others, which may or may not exist.

## Sensitive Data

CPS monitors are actively collecting, verifying, documenting, and reporting highly-granular and politically-sensitive protection and human rights data in an active conflict zone.

For example, members of the Bhamo District CPS were recently mobilized to respond to a missing persons case that rapidly escalated into a high-profile prosecution (military tribunal and Truth Commission) of a Tatmadaw military commander for war crimes, including the

unlawful detainment, torture, and execution of non-combatants and subsequent concealment of these crimes using unmarked mass graves.

Village Monitors, Township Coordinators, and Bhamo District Officers collected, stored, and shared information that included:

- **Report metadata** (such as incident code, author of report, timestamp, who the report was submitted to and verified by, and the methods of verification);
- **Personally-identifiable Information (PII)** of victims (name, age, address, family members, nature of harm/injury), family members, sources, eyewitnesses, informants, and other interested parties (such as community leaders, camp leaders, and contact information of KBC, KMSS, Metta, JST, UNHCR, local authorities, State officials (Chief Minister, State Border Affairs Minister, State Member of Parliament),
- **Location data** regarding key crime scenes (including site of apprehension, alleged torture, and burial site);
- **Incident data** (summary provided by CPS members), and possible archival information of official autopsy report;
- **Evidence**, including data in raw form, such as audio recordings, narrative transcriptions, photographic evidence of crime scene (gravesite, deceased bodies, etc.) and self-authored report of eyewitness accounts;
- **Regular weekly and monthly Activity Logs** for Village Monitors, District and Township Coordinators that detail information pertaining to the date and time, location, and content of all activities (such as meetings, trainings, conversations, etc.) carried out by each member, whether relevant or not to this particular incident.

**This kind of information is *highly valuable* to repressive governments** such as the Myanmar government and its military wing, the Tatmadaw, as well as the Chinese government and other interested geo-political actors. Such threat actors will go to great lengths to acquire intelligence from the CPS and its partners. Simply by virtue of the information they gather, therefore, the CPS network (its members, partner organizations, and the information they generate) has become a valuable intelligence asset for adversaries leveraging sophisticated cyber tools.

## Implications of Findings for Monitoring Work

The descriptions above provide us (as external actors) with important information otherwise unavailable to us (for example, through direct observation) about the nature of monitors work, the contexts they navigate, and their experiences in doing so - including some of their concerns, frustrations, and indeed accomplishments. But what do they mean for NP and Nyein's efforts to establish an effective CPS?

When we look across this array of challenges, risks, and vulnerabilities as described above, we see they have implications for monitoring work in three consequential areas:

**(1) OPERATIONAL EFFECTIVENESS**
Some of the challenges and vulnerabilities described above have a significant impact on the monitors' or network's ability to carry out work efficiently and effectively, and can prevent or hinder positive outcomes for affected civilians and communities. In so doing, they have implications for the operational effectiveness for monitors at an individual level, and the network at an institutional level.

Examples include:

- The physical environment, such as difficult natural terrain, and lack of quality infrastructure (physical and digital) makes it difficult to collect and transmit timely, granular information about incidents and their impacts across wide geographic areas;
- The nature of relationships between formal and informal systems, local and national (or international) actors, and between armed actor groups (such as EAOs and the Tatmadaw) and local community leaders and organizations makes it challenging to gain access to military actors for the purpose of negotiation, or to certain (potentially restricted) locations.
- Administrative burdens and bottlenecks; limited financial, human, and material resources available to the monitors; and lack of system wide resources and tools generate significant barriers to timely local response.

Threats to operational effectiveness impede monitors' ability to respond to incidents in a timely or efficient way and compromises their ability to respond to community protection needs.

**(2) DATA SECURITY**

A number of the challenges, concerns, and behaviors we have learned about can lead to critical data and system vulnerabilities, whether analog or digital, given the rapidly evolving nature of digital surveillance in conflict-affected environments such as Kachin State.

Examples include:

- A **lack of data security protocols**—across the network —which increase the exposure of sensitive information to targeted spear phishing campaigns that may intercept communications and exploit sensitive data collected, stored, and shared by CPS members and their partners.[27]
- **Limited skills, knowledge, and capacities** for securing digital data on the move, while on the ground at the community level—this can lead to data security issues such as the confiscation and exfiltration of data from unsecured personal devices (mobile phones and laptops) while operating in areas of concern in Myanmar.[28]

[27] Social engineering, lawfully-purchased surveillance, and remote-access intrusion software has been used widely by repressive governments. Once compromised, threat actors can control computer webcams and microphones (to record audio video), keystroke loggers (to uncover passwords), file processing protocols (to view and extract documents and files containing sensitive data), and can track users' location, internet browsing history, and communications logs.

[28] Today's off-the-shelf smartphones, particularly those available to many segments of the Burmese mobile consumer market, are equipped with dozens of sensors meant to capture, store, and transmit data of all sorts. Embedded microphones and cameras enable the collection, storage, and transmission of audio-visual data, such as audio-recordings, digital photographs, and videos. GPS configurations allow for highly-granular temporal and location-based data, which can be used to track the precise location of a user. And, due to advancements in CPU and memory storage, most phones contain personally-identifiable contact information, communications history logs, call detail metadata (CDRs), and even digital documents (such as saved MS word or PDF files). According to the Kachin Women's Network, "One youth leader had their phone confiscated by the Tatmadaw who checked their posts, activity and photos. These cases are happening now." (interview).

- **Exposing metadata and other sensitive information on open channels** through social media that is used to monitor and surveil targets via digital traces, or signatures (data exhaust) that internet users leave behind when they conduct their work online.[29]

Given the nature of the digital landscape in Myanmar, and the known surveillance culture of the Myanmar Government, the vulnerabilities we have observed (in systems, practices, and behaviors) regarding data security leave both individual monitors, and the network itself, open to serious potential harm.

**(3) PERSONAL SAFETY**

Other challenges and vulnerabilities have a direct impact on the personal safety, security, and well-being of monitors, other network members, and the victims, families, and communities exposed to or engaged in the work done by the network.

Examples include:

- The requirement for monitors to include their **personal information on written reports** puts them at continued risk of intimidation, arbitrary arrest, and detention in the event that a report falls into the wrong hands at any point in the chain of reporting across the mechanism and its partner organizations.[30]
- The collection and **aggregation of data** on incidents (which includes personally-identifiable information about the members, and the activities of the CPS) puts the wider network at risk when Secret Police visit the Secretariat office where monitor reports are collected, stored, and processed *without the requisite data protection and security policies and protocols necessary* to keep them confidential.
- **Direct engagement with Ethnic Armed Organizations (EAOs)** for verification, information sharing, or response purposes exposes monitors to intimidation, arrest, and detention if monitors lack the necessary paperwork for official status/permission, or if Myanmar authorities suspect CPS monitors of association with EAOs.

Threats posed by unsecured information processes and systems, and by the collection, storing and sharing of sensitive data, puts the lives of, activists, witnesses, and informants in peril. In addition, the acquisition of sensitive information (such as the identities of witnesses or informants) by malicious actors would enable them to target activists and sources involved in the CPS's operations, or covertly gain intelligence over time, allowing them to anticipate and counter the actions of humanitarian or peace-building actors.

**Illustrating Threats to Operational Effectiveness, Data Security and Personal Safety in Current Monitoring Practices**

[29] Our interviews suggest that the Myanmar government and various elements within the military are covertly infiltrating these Facebook groups, posing as activists and community members, in order to gain valuable information such as the identities and PII of participants and members, and relational information about who is in their network, as well as being able to intercept communications (posts) to the wider group.

[30] According to procedure, monitors are required to keep a copy of their reports, but often lack a secure place to store them. In a context of constant government surveillance, the requirement to keep documentation containing sensitive information in a personal and unsecured environment puts both the monitor and the community at risk. According to one monitor: "I don't write my [CPS] reports at home in advance because I am afraid of being stopped and searched on the way to the district coordinator [to deliver the report] by the Special Police. So instead I first travel to the district coordinator's house and then write the report from memory there…"…If I could not travel to the district coordinators home, I would probably send my reports via Facebook Messenger."

The following map presents a high-level overview of the current flow of information and data (digital and otherwise) across the CPS network. Mapping the data flow in this way allows us to clearly indicate and illustrate, at a high level, where and how risks to *operational effectiveness*, *personal safety* and *data security* are playing out in current CPS processes, thereby indicating "hot spots" for intervention through innovation and design initiatives.

Note that the map presented here provides a snapshot of data flow through the network from the "bottom-up" – i.e from monitors in affected communities through intermediate network levels and up to secretariat and partner levels of operation. While in reality the flow of information between network levels is bi-directional (for example, as in the case of township or secretariat members communicating a plan of action for incident response back to monitors), the upward flow of information and communication has been privileged here as a use-case for the sake of simplicity.

This birds' eye view, supported by our findings regarding the challenges and vulnerabilities inherent to the work of CPSs in Kachin, brings us to the central insight from this research:

> ***That the present orientation to information management (in terms of data protection and digital security), at both the organizational and individual levels, is creating or exacerbating serious vulnerabilities for the network, monitors, and affected people.***

While CPSs and monitors certainly face a wide range of challenges in carrying out their work safely and effectively, paramount among them are these issues around information management and digital practice, given the centrality of both to monitoring itself, and the seriousness of the vulnerabilities these create.

DATA FLOW + ECOSYSTEM

## SYSTEM

**Tools**

**Practices**

- In their first several years, mechanism secretariat offices submit consolidated incident and activity reports to the (Shalom) State Committee for quality control, and to check alignment of activities with program goals.
- Mechanism reports are received and stored on unsecured office computers.

**Vulnerabilities**

- ⚠ Mechanism members do not trust that sensitive reports with their PI are being securely stored.
- ⚠ Activity report templates do not address various organisational info needs (e.g. evaluation of mechanisms vs. [conflict] situational analysis).
- ⚠ A lack of digital training and protocols for data security impacts on personal risk.
- ⚠ Unsecured, open platforms are used to receive, store and share sensitive data.
- ⚠ A lack of standard digital tools, training and protocols creates data insecurity.

⚠ Personal Safety Risk
⚠ Data Security Risk
⚠ Effectiveness Risk

## MECHANISM

**Tools**

**Practices**

- Mechanism members send and receive voice calls, texts, photos and Facebook messages for incident notification, planning and reporting across the mechanism and with partners and government actors. They may also share info informally with other civil society organisations.
- Monitors submit written incident and monthly activity-log reports that are consolidated, digitised and re-submitted at each level of the mechanism.
- Government Special Police routinely visit the secretariat office where reports are stored.
- Monitor incident and activity reports are consolidated and digitized at the township and district levels and distributed upward.

**Vulnerabilities**

- ⚠ A lack of digital training and protocols for ensuring data security creates personal risk.
- ⚠ Unsecured, open platforms are used to receive, store and share sensitive data.
- ⚠ A lack of standard digital tools, training and protocols creates data insecurity.
- ⚠ Monitors do not trust that sensitive reports with their PI are being securely stored.
- ⚠ Incident reports may go missing or remain out in the open before being securely filed.
- ⚠ Monthly activity report formats are not readily usable for different organisational needs.
- ⚠ A lack of digital training and protocols for ensuring data security creates personal risk.
- ⚠ Unsecured, open platforms are used to receive, store and share sensitive data.
- ⚠ A lack of standard digital tools, training and protocols creates data insecurity
- ⚠ Mechanism computers and logins are used by multiple personnel, compounding risk.

## MONITOR

**Tools**

**Practices**

- Monitors place voice calls, text, send photos and use Facebook Messenger to notify the mechanism of an incident, plan next steps, and report incident and verification info.
- Monitors use print materials such as bilateral agreements as negotiation tools.
- Monitors routinely document incident investigation info in written notes and and regularly submit written reports that include their personal information.
- Concerned about carrying sensitive incident info in discoverable hard copy or digital files, monitors often commit incident info to memory until they can reach a safe place to report or record the information by phone or in person.
- Some monitors may be restricted to using a landline to communicate with the mechanism either due to service disruption or a lack of infrastructure in remote areas – but these landlines are routinely surveiled by the military.

**Vulnerabilities**

- ⚠ Taking + storing sensitive incident verification photos on mobiles creates personal risk.
- ⚠ Unsecured, open platforms are used to collect, store and share sensitive data.
- ⚠ "Spotlight effect" + data risk if community or media members publicly post sensitive incident info on unsecured networks like FB.
- ⚠ Monitors do not have a secure place to store written reports at home.
- ⚠ Delivering written reports in person or via third party puts monitors at risk if intercepted by the military en route.
- ⚠ Fragmenting incident information using different tools and methods impedes effective info management.
- ⚠ Using memory to store incident data undermines robust documentation.
- ⚠ Routine surveillance of landlines (or of abodes with landlines) puts monitors at risk when sharing or reporting sensitive incident info to the mechanism, but monitor may lack other means to communicate more securely.

## Summary of Findings

The research findings help us develop an understanding of some of the key **challenges** and **vulnerabilities** faced by monitors in carrying out their work. CPS monitoring efforts based on the traditional approach to monitoring. Through storytelling, practice mapping, depth interviews and focus groups conducted with monitoring groups from across Kachin State, as well as NP and Nyein staff in Yangon, we learned that monitors face a wide range of challenges in carrying out their work effectively, but also safely.

- Some of these challenges stem from **features of the context** in which they carry out their work, both in terms of the physical terrain and infrastructure where some of them live and work, to the nature of the political, conflict, and security conditions they face.
- Other challenges were found to stem from the **practices involved in monitoring work** itself, which range from responding to cease-fire violations, protection threats, human rights violations, inter-group tensions, and conflict incidents; negotiating with hostile actors; and which include an array of practices involving sensitive data in insecure and sometimes hostile environments.
- Still others, we learned, could be understood to stem from both the **administrative and bureaucratic system of the network** itself, and through which monitoring work is made possible.
- Last, but not least, a final set of challenges were found to derive from the **wider international response system** active in Kachin, especially in terms of the parallel monitoring systems presently being established by actors with little capacity for such work.

In our initial assessment of the critical needs, challenges, and barriers monitors experience in carrying out their work, we also uncovered a number of concerning **vulnerabilities** within the network that could significantly expose the monitors, the data they collect, and the populations they serve to significant risk.

- Some of the vulnerabilities stem from the **lack of a systemic approach** to data security and digital safety, as reflected in the absence of requisite mechanisms, incentives, capacities, and resources that are characteristic of the kinds of secure information management systems found in other remote-based distributed network models used for monitoring purposes elsewhere.
- Other vulnerabilities stem from **limited awareness and skills** among monitors, coordinators, and support staff around data literacy and digital hygiene.
- Others stem from a number of **unsafe practices** at both the institutional and individual level, including variations in workflow; reliance on personal devices and accounts; the use of unencrypted third-party platforms; and failure to calibrate data sensitivity and adhere to principles of data minimization when generating and sharing crisis data.
- Finally, vulnerabilities also stemmed from practices involving **sensitive data** such as report metadata, PII, location data, incident data, as found in Activity Logs.

We believe that each of these are key areas where significant improvement is possible, and that if made, will be consequential not only for the networks' ability to fulfill its explicitly defined objectives, but also for the safety and well-being of monitors, the CPS itself, and the communities they serve.

# DESIGN BRIEF

## Introduction

As we explained at the outset of this document, a primary objective of the first phase of any innovation cycle is to create learning for design. In other words, **to generate the findings and insights that form the foundations upon which any solution, concept, or prototype must be built**.

The previous section was dedicated to sharing those foundations - the findings and insights generated through our field work in Myanmar around key challenges to safe and effective monitoring work and vulnerabilities experienced by the CPS in Kachin. In this section, we now turn our attention to using these insights to refine the design direction and articulate the Design Brief.

The Design Brief represents a critical output of the learning phase. The function of the Design Brief is to guide concept development during the next phase in the innovation cycle – the ideation and design phase (which may involve "search and adapt" or "invent" according to the HIF Framework) – and keeping us firmly rooted in key learnings throughout that process.

As a reminder, the Design phase of the innovation cycle is defined as the second stage of the "Diagnose, Design, Deliver" process that: *employs the knowledge gained from the Diagnose phase as the raw material from which to generate design propositions in an iterative process to create, test and refine solutions that are problem-driven, user-centered and evidence based*.

As a key output of the Diagnose phase, the Design Brief therefore applies the observations and findings generated through the research and analysis of the problem recognition phase to outline:

- Key **issues** that need to be prioritized and addressed through the innovation initiative;
- Design **objectives** that need to be achieved in response to each issue; and
- **Criteria** that should be met by any proposed concepts and solutions to address key challenges and needs, while also meeting our criteria for accountable innovation.

In this way, the Design Brief can be viewed as an essential pivot point between the conclusion of the Diagnose phase and the start of the Design process, by linking the generation of knowledge to the execution of an informed and directed design approach.

The Design Brief therefore represents the natural conclusion to this phase of work by providing knowledge, conclusions and directives that constitute the starting point and catalyst for the next (Design) phase of the innovation process.

# The Design Brief:

**RQ4**: Are any of the critical challenges best addressed through technological solutions?

**RQ5**: Are any of the critical challenges best addressed through other kinds of solutions?

## Key **Issues**, Design **Objectives**, and Core **Criteria**

The initial proposition for this initiative was motivated by an objective to leverage CPS strengths to improve protection and peacebuilding outcomes for a wide range of stakeholders in Myanmar. It suggested that one way to do this could be leveraging digital technologies for improving the technical capabilities of monitors and enabling them to supply more timely, granular conflict-related information to humanitarian and peacebuilding actors.

**Our research has prompted us to reconsider this proposition** while keeping the impact objective of the original in view and positions us to now build a Design Brief.

Using the principles of evidence-based design and accountable innovation, the Design Brief presented below applies the research findings to articulate the key design issues and objectives that any proposed solutions must address, towards improving **the operational effectiveness** of the CPS, the **personal safety** of those working in it, and the issues of **data security** central to both.

The Design Brief is organized across four key issues of concern highlighted by the research. Each of these issues is then unpacked further into a discreet design objective and set of criteria to guide targeted concept ideation and development moving forward.

Specifically, the four key issues of concern have been identified as:

- Lack of systemic approach to information management
- Limited awareness, knowledge and skills around digital threats and vulnerabilities
- Unsafe practices
- Organizational structure and administrative inefficiencies that compound risk

### ISSUE I: LACK OF SYSTEMIC APPROACH TO INFORMATION MANAGEMENT

The lack of a systemic approach to information management at the institutional level contributes broadly to the following issues:

- Variation in (often unsafe) information practices and data flow across (and outside) the mechanism that raise questions around the analytical utility of information being generated;
- Low visibility on technical compliance, adoption, and uptake regarding data security and protection practices of the monitors and coordinators;
- Over-reliance on personal devices and accounts, third-party platforms, and ad-hoc work-arounds to collect, store, transmit, and share sensitive data; and
- The inability to detect, respond to, and recover from critical incidents (i.e. compromised systems, data breeches, etc.) in a systematic or reliable way.

**The design objective for addressing this issue is therefore:** to institutionalize data security as an operational pillar by standardizing information management practices, systems, and tools across the mechanism.

Proposed design solutions must therefore:

- Achieve and maintain data security for all stakeholders, systems, and practices at all levels of the network, while improving efficiencies;
- Enable appropriate responses and safeguards for critical incident detection, response, and recovery;
- Promote adoption and compliance around responsible data use, digital hygiene, data literacy, and data minimizations;
- Enable account management, user authentication, data compartmentalization, and real-time monitoring and oversight data access and use;
- Standardize the use of encrypted communications channels, and best practices for connecting to the internet and securing mobile devices;
- Anticipate, re-evaluate, and respond to changes in the (digital) threat landscape as new factors develop and become known, applications are added, removed, or upgraded, and user requirements evolve;

**Solution types may include**: (a) policies, strategies, and protocols; (b) visual maps, diagrams, and flow charts; (c) software packages, secure operating systems, or communications hardware; (d) human resources (with relevant domain expertise); and (e) incentive structures and compliance and oversight mechanisms.

**ISSUE II: LIMITED AWARENESS AND SKILLS AROUND DIGITAL THREATS AND VULNERABILITIES**

Monitors and network staff at all levels are currently operating with limited awareness of the data security threats inherent to their operational environment and communications systems and how to address them, despite the centrality of digital information practices to their work and the heightened levels of threat associated with this.

Limited awareness is further combined with a general lack of knowledge and skills around digital literacy and hygiene for preventing or addressing these risks. This lack of awareness, knowledge and skills leads to the adoption of unsafe practices at both the institutional and individual levels of the mechanism.

**The design objective for addressing this issue is therefore**: To address the technological knowledge and skills gaps of monitors, coordinators, and support staff across all network levels.

Proposed design solutions must therefore:

- Develop ongoing awareness of emerging digital threats, their associated vulnerabilities, and the human, material, and reputational consequences potential adverse scenarios;
- Promote an organizational culture around responsible data use, digital hygiene, data literacy, data sensitivity, and data minimization through appropriate incentive structures, access to educational resources, the creation of a set of CPS principles, and by providing safe spaces for learning (in controlled environments);

- Provide on-going digital security skills development by updating training materials and by providing targeted trouble-shooting and technical support via on-call assistance.[31]

**Solution types may include**: (a) Training and educational resources (such as guidance manuals, templates, workshops and simulations, instructional videos, etc); (b) community-derived frameworks (such as principles); (c) incentive structures and compliance and oversight mechanisms; (d) partnerships with digital security-oriented civil society groups that can provide on-call support.

**ISSUE III: UNSAFE PRACTICES**

Several information practices concerning the collection, sharing, and storage of data (whether digital or analog) can increase the vulnerability of monitors, victims, and the mechanism more broadly. There are three specific issues of concern around unsafe practices observed in Kachin, and likely relevant for other state mechanisms in Myanmar as well:

A. The systematic and continuous generation and sharing of large volumes of highly valuable and sensitive information (e.g. through regular multiple internal reports (Activity Logs) shared across a complex organizational structure) in the absence of a data security strategy;
B. Over-reliance on personal devices and shared accounts as well as unencrypted third-party platforms, applications, and communications channels to collect, store, transmit, and share sensitive data;
C. Approaches to sharing sensitive information with external networks of actors.

**The design objectives for addressing this issue are therefore:** To minimize system vulnerabilities and establish a more secure, closed and streamlined network of devices and platforms for carrying out CCM activities safely.

Proposed design solutions must therefore:

- Limit the collection and storage of personally-identifiable information (PII) and other sensitive information[32] so as to protect the identities of informants, eye-witnesses, and other stakeholders where privacy is warranted;
- Ensure obfuscation of demographically identifiable information (DII) when reports are shared or published;
- Enable account management, user authentication, data compartmentalization;
- Enable real-time systems monitoring and oversight data access and use;

[31] Monitors and other stakeholders have reported concerns around lack of technical support from the Shalom Project Team staff, and evaluations and other reports confirm the need for proper support via customized coaching workshops, trouble-shooting, and periodic technical training, especially around areas related to documentation, reporting, and general data protection and security. During the Evaluation workshop, and in some of our focus group sessions, monitors and coordinators expressed the need for more targeted technical support, and even requested that NP staff be based permanently in Kachin state to ensure access to and availability from NP coaches, trainers, and staff. However, in contrast to the pilots in Chin and Mon states, the model that is currently piloted in Kachin has the NP team "at arm's length" from the CPS network – Shalom, or Nyein, has taken up the primary focal point / interface / back-end support function that has, in other states in Myanmar, been carried out by NP.

[32] Such as report metadata, data exhaust and digital traces, personally-identifiable information, location data, audio-recordings, photographic evidence, attributable information.

- Standardize the use of encrypted communications channels, and best practices for connecting to the internet and securing mobile devices;
- Restrict use of devices or software provided by outside or unknown parties;
- Enable monitors to fulfill divergent and situational evidentiary requirements associated with their work, and to collect the right information at the right level of rigor to meet those requirements.

**Solution types may include**: (a) software packages, cloud-storage accounts, secure operating systems, or communications hardware; (b) human resources (with relevant domain expertise); (c) incentive structures and compliance and oversight mechanisms;[33] (d) Training and educational resources (such as guidance manuals,[34] templates, workshops and simulations, instructional videos, etc).

**ISSUE IV: ORGANIZATIONAL STRUCTURE AND ADMINISTRATIVE INEFFICIENCIES THAT COMPOUND RISK**

CCM activities operate within a complex organizational and administrative structure that contributes to operational bottlenecks and data security risks in several ways. Examples include: (a) a multi-layered, mechanism-wide consultation process for incident response that can impede timely response for urgent cases; (b) resource limitations for community incident response efforts and/or administrative delays in providing funding to monitors for essential incident response activities; and (c) burdensome reporting requirements and report templates that expose monitors' personal ID data and increase sensitive data exposure.

Such administrative inefficiencies were observed to compound challenges to operational effectiveness, personal safety and data security.

**The design objective for addressing this issue is therefore**: To align organizational structure, administrative processes and reporting practices with the practical needs of CPS staff for carrying out monitoring in a safe and effective way.

Proposed design solutions must therefore:

- Reduce administrative burden where this does not contribute to operational effectiveness, personal safety, or data security.
- Re-design reporting templates and pathways to reduce administrative burden, limit data diffusion, and address current data security vulnerabilities.
- Implement best practices around anonymization so as to protect the identities of informants, eye-witnesses, and other stakeholders where privacy is warranted, and to ensure that demographically identifiable information (DII) is appropriately obfuscated when reports are shared or published.
- Establish more centralized and secure data archiving processes and re-consider the distribution and storage of sensitive reporting documents
- Explore administrative shortcuts for identifying, resourcing, and responding to urgent CPM incidents.

[33] For example: to operationalize data protection, digital security, and risk mitigation measures, strategies, and requirements defined by Threat Modeling efforts and set forth in the data security policies of the CPS.
[34] For example - Develop guidelines for vertical (up the chain of command) and lateral (across district teams and with partners) data sharing in direct response to well-defined referral mechanisms.

**Solution types may include**: (a) Policies, strategies, and programmatic tools; (b) training and educational materials (such as guidelines[35]); and (c) community-derived frameworks (such as principles).

## Design Brief Summary

**Revised proposition:**

We propose that in order to improve the capacity of CPSs to help address knowledge gaps experienced by peacebuilding and humanitarian actors working in Myanmar, it is crucial to first improve the safety and effectiveness of civilian monitoring practices for monitors, the CPS network, and affected populations in Kachin.

Our revised proposition therefore suggests exploring the following:

***How might we*** *address key challenges and barriers to operational effectiveness, personal safety, and data security for monitors through addressing these design objectives:*

*1. Institutionalize data security as an operational pillar.*
*2. Address the technological knowledge and skills gaps of staff across all network levels.*
*3. Minimize system vulnerabilities and establish a more secure, closed and streamlined network of devices and platforms for carrying out CCM activities.*
*4. Reduce vulnerabilities caused by intra- and inter-organizational data sharing while ensuring that mission-critical information is generated and shared appropriately, safely and effectively.*
*5. Review and re-consider administrative processes to streamline and improve operational efficiencies while addressing data security and personal safety vulnerabilities.*

[35] For example, develop guidelines for vertical (up the chain of command) and lateral (across district teams and with partners) data sharing in direct response to well-defined referral mechanisms.

## Preparing for Ideation

As a key output of the problem-definition activities of this project, the Design Brief is a direct product of the research and analysis process. It provides the guidelines for concept ideation in the next (Design) phase of the innovation process and will act as the touchstone against which all selected concepts and prototypes will be evaluated as they move through their development cycle. Supported by the key learning and insights generated from the research, the Design Brief will provide NP and TPL with a shared foundation upon which to focus our efforts moving forward, and create the grounds for initial messaging for potential donors and supporters.

The four key issues and five accompanying design objectives developed in the Design Brief outlined above represent complex challenges involving diverse elements, from human awareness to administrative systems, digital networks and more. However, while some of the critical challenges we have identified and translated into the Design Brief can be best addressed through technological solutions, technology alone cannot fulfill all of the stated design objectives.

Applying one of the key principles of accountable innovation and therefore being problem driven rather than solution lead, prompts us to take a broad approach to the development of design solutions.

Rather than asking: "*how can we use digital technologies here?*" we instead look across the problems of concern and ask, "*how might we improve this situation?*"

This represents a shift in approach to innovation from looking for ways to apply technological solutions, to looking for ways to solve practical problems, however that might best be accomplished. Doing this allows us to align problems with their most relevant responses, and in this case, can help us increase the likelihood of achieving a robust, practical and sustainable set of operational and institutional improvements that positively impact the network at all levels.

Therefore, while we anticipate solutions for addressing several of the design objectives above to include the development of digital systems and tools, the range of solutions will not be limited to strictly technological approaches. Other approaches such as processes, protocols, strategies, practices and "low" or non-tech solutions will likely be required, either as additional stand-alone elements when they best are suited to address a particular problem, or as supporting features needed for technical solutions to achieve their impact.

## Further Reflections

We include here a range of further observations that can help us reflect upon the goals of our project:

**TENSIONS AND TRADEOFFS**

There is a tension between helping monitors carry out their work in more safe and effective ways, and the generation and sharing of more timely, granular, and highly-sensitive crisis data with other actors. If we want to hold both objectives in view, we will need to do so carefully. The humanitarian and human rights technology community is coming to terms with a deeply flawed logic embedded into our assumptions around the relationship

between information communication technologies and protection outcomes for affected populations: *that more information about mass atrocity situations leads intrinsically to better outcomes for affected people*. In reality, it is likely that the opposite is the case: *digital technologies are often a causal vector for harm*.[36] Monitor's personal safety and their special peacebuilding roles therefore need to be carefully considered, as we move into the innovation cycle.

**PURPOSE MATTERS!**

We observe that civilian monitoring, in Kachin as elsewhere, can be conducted for different purposes, each of which holds significance for the ways in which information is collected, reported, and used.[37] The diverging evidentiary requirements that accompany these different purposes matter from an operational and functional perspective.[38] This means that for information produced by CCM activities to be a usable and useful resource for different actors, they must be aligned with both the particular uses to which it will be put, and the practical needs of those who will use it. Without a process for aligning information practices with the different evidentiary standards required for different purposes (which includes standards for how that information is collected, stored, and aggregated), *much of what is generated ends up not being fit for purpose*.

If there is the ambition for monitors to eventually contribute information towards human rights monitoring, then existing training will need to be adapted to sufficiently equip them to (a) recognize if they are engaged in a civilian protection case vs a human rights case; (b) identify the verification standards required in each case, and; (c) act with the skills, knowledge or means to collect the right information at the right level of rigor to meet those requirements.

**BREADTH VS. DEPTH?**

In contrast to the pilots in Chin and Mon states, the model that is currently piloted in Kachin has the NP team "at arm's length" from the CPS network – Shalom, or Nyein, has taken up the primary focal point and back-end support function that has, in other states in Myanmar, been carried out by NP.[39] Such an arrangement makes it difficult to effectively monitor and ensure the quality of monitoring activities; understand and mitigate the transfer of risk to local actors; and provide the kinds of ongoing, targeted, coaching and technical support to the monitors if NP is unable to gain real-time, ground level insights on the challenges and needs faced by individual monitors.

---

[36] In the context of Kachin, for example, reporting or sharing highly-sensitive information may actually undermine community protection and efforts to sustain the peace process.

[37] When monitoring work is carried out in support of documenting human rights violations, for example, information generated by the monitors is used as evidence in order to build legal cases to prosecute and try individuals accused of crimes. But when monitoring work is carried out in support of humanitarian operations, CCM information is used as actionable intelligence to inform the decision-making capabilities of humanitarian actors to develop response strategies, design relevant and effective programming, and communicate directly with vulnerable populations.

[38] This has significance for (a) the workflows and processes employed, (b) the techniques and methodologies used, (c) the granularity and scope of data required, (d) the security measures taken, and (e) the ways in which analytical products are designed, disseminated, and applied toward the protection of vulnerable populations.

[39] The model used by NP in Kachin state, in other words, is similar to a remote-based management situation, whereby the operational responsibilities, usually carried out by NP staff or in close collaboration with partners, have been transferred almost exclusively to Nyein Foundation, *who may or may not have the capacities, competencies, approaches, and resources for effectively delivering on these responsibilities*.

The Nonviolent Peaceforce may need to (re)consider the requisite capabilities, capacities, and approaches that might be put into place in order to fulfill a more targeted, back-end operational support role in Kachin state. NP will have to decide if it wants to further broaden its scope in partner organizations and geographical coverage (a facilitation, or brokerage role), or if it makes sense to focus on providing more targeted, in-depth, operational support to its existing partners.

**NAVIGATING OPPORTUNITY AND RISK**

Novel and little understood digital threats pose significant challenges and risks for CPS monitors in throughout the monitoring cycle, most notably in their verification, reporting, information sharing activities. What's more, this state-of-affairs may actually be exacerbated by the administrative infrastructure of the network. We recognize that in our short exposure to this system, we can only begin to grasp the most basic fundamentals. However, from risk analysis perspective, we recognize a number of vulnerabilities are being introduced through the very nature of the system.[40] [41]

The humanitarian sector is still learning about the range of digitally derived threats and vulnerabilities that crisis affected populations—and the humanitarians who serve them—are facing in fragile contexts. We are still grappling with the emerging concerns around the ways in which our own attempts to "innovate" in operational environments may engender harm. Moving forward, a holistic understanding of both the opportunities afforded by innovation and risks that are engendered by our own actions in an attempt to harness the transformative potential of the digital age is rapidly becoming a pre-requisite for responsible, accountable, and effective humanitarian innovation.

# Conclusion

CPSs and monitors face a wide range of challenges in carrying out their work safely and effectively. Paramount among these are issues around digital practice, given the centrality of information practices to monitoring itself, the seriousness of the vulnerabilities these create.

These findings give us a new perspective from which to reflect upon the original proposition for this innovation initiative. To review, this proposition invited us to consider whether, in light of the successes demonstrated by current CPSs and community protection monitors, improving the functional and technical capabilities of CPSs might enable them to contribute much-needed information about conflict-related incidents and displacement through their monitoring work, for peacebuilding and humanitarian actors.

[40] For example, variation in workflow, in combination with practices in use that are not known to NP or Shalom, are compounding the risk profile of the mechanism. Coupled with unclear or non-existent data protection and digital security systems, policies, and procedures, this variation presents significant risks to the mechanism, when it comes to matters of surveillance, search and seizure, and open-source monitoring.

[41] We are also concerned matters of data minimization. Data minimization requires that project teams identify--at the outset--the information needed to fulfill advocacy, operational, and evidentiary requirements, *and collect nothing more than what is needed*. And yet, the mechanism requires the regular reporting of Activity Logs *without a strong case to what this detailed information is used for.* The scope of this highly sensitive and valuable intelligence should not be underestimated: simply by virtue of the fact that it exists, it puts the CCM mechanism, its partners, and the community members who are involved at great risk.

**Our research suggests that before contemplating how CPSs could adopt new tools in order to help address information gaps experienced by peacebuilding and humanitarian actors, it is crucial to address the serious implications (tor the safety, security, and well-being of those involved in the monitoring network) created by the present situation.**

It is our view that the issues we have observed around information practices and data flow should be ***prioritized*** to improve the safety, security, and effectiveness of the CPS overall. Once these steps are taken, consideration could be given to expanding those practices and elaborate (or complicate) existing data flows and information management practices, in order to avoid compounding existing vulnerabilities that are already grave.

## Opportunities

Despite this challenging (and potentially alarming) state-of-affairs, there is great opportunity ahead. The Nonviolent Peaceforce has contributed much toward a more inclusive and sustainable peace for the people of Myanmar. It has built an incredible network of civilian volunteers and community leaders, leveraging its pioneering approaches to unarmed civilian protection. NP therefore has the opportunity to take a leadership position on tackling very real challenges and grave threats to its operations and the people it serves.

This project represents an initial but significant first step towards empowering NP to not only address a range of evolving threats to CPS monitors and coordinators, NP and its partner organizations, and the populations they serve, but to also leverage the transformative potential of accountable innovation toward the development of a more effective and formidable CCM 2.0 model.

Having concluded the learning phase and developed a Design Brief to guide ideation, we have now laid the foundation for an innovation process to address the challenges and vulnerabilities we have identified.

The Nonviolent Peaceforce is a key player in the advancement of civilian monitoring efforts in Myanmar and elsewhere. The peacebuilding and protection communities will likely continue to look to NP to play a leadership position on these emerging issues. As such, it has the capability--and responsibility--to tackle the issues and challenges presented in this report, to promote the safety and effectiveness of monitoring networks.

Investment that supports NP to advance in this innovation process will support the systematizing, contextualizing, and scaling of an improved CCM model, and build their capacity to navigate an increasingly hostile digital terrain.

# ANNEX

## Schedule of Key Activities

| | |
|---|---|
| April 1 - May 1 | **Initial Strategy Meetings** (scope, stage gates, resources, team roles) |
| May 1 - 17 | **Research Design**: key areas of inquiry and research questions developed; methodology finalized; activities designed; key tasks assigned; data generation and capture materials finalized and shared; documents reviewed for data protection |
| May 1 - 17 | **Field Prep**: make logistical arrangements (permissions, permits, visas, participant recruitment, scheduling, book travel and accommodation arrangements) |
| May 4 - 14 | **Team Briefings**: (*methods*, *context*, *security*) |
| May 10 - 17 | **Preliminary Research:** desk review (context, technology landscape, evaluations of monitoring practices, relevant background materials), remote interviews (experts) |
| May 17 | **TPL team: Travel**: Depart for Myanmar (international flights) |
| May 19 | **TPL team: Travel**: Arrive in Yangon |
| May 20 | **TPL team: Travel**: Depart and arrive at site #1 (Myitkyina, Kachin); planning meeting with NP team (evening) |
| May 21-22 | **TPL team: Site #1: NP Assessment Workshops**<br>Participant observations; interactive activity afternoon of 22nd (see workshop agenda) |
| May 23 - 24 | **TPL team: Site #1: Mapping Activities** (monitors) |
| May 25 | **Team A: Site #1: Depth interviews** (protection and peace-building actors)<br>**Team B: Site #2: Mapping Activities** (monitors) |
| May 26 | **Team A: Site #1: Depth interviews** (protection and peace-building actors)<br>**Team B: Site #2: Depth interviews** (local organizations) |
| May 27 | **TPL team: Travel**: Depart for site #2 (Yangon) |
| May 28-29 | **TPL team: Site #2: Interview (**Protection and Peacebuilding; Local Technology Actors) |
| May 30-31 | **TPL team: Depart for home** |
| June – October 31 | **TPL team: Analysis and Writing** |