On Enforcing the Digital Immunity of a Large Humanitarian Organization

Stevens Le Blond, Alejandro Cuevas, Juan Ramón Troncoso-Pastoriza, Philipp Jovanovic
Bryan Ford, Jean-Pierre Hubaux
École Polytechnique Fédérale de Lausanne
{first_name.last_name}@epfl.ch

***Abstract*—Humanitarian action, the process of aiding individuals in situations of crises, poses unique information-security challenges due to natural or manmade disasters, the adverse environments in which it takes place, and the scale and multidisciplinary nature of the problems. Despite these challenges, humanitarian organizations are transitioning towards a strong reliance on the digitization of collected data and digital tools, which improves their effectiveness but also exposes them to computer-security threats. In this paper, we conduct a qualitative analysis of the computer-security challenges of the International Committee of the Red Cross (ICRC), a large humanitarian organization with over sixteen thousand employees, an international legal personality, which involves privileges and immunities, and over 150 years of experience with armed conflicts and other situations of violence worldwide. To investigate the computer security needs and practices of the ICRC from an operational, technical, legal, and managerial standpoint by considering individual, organizational, and governmental levels, we interviewed 27 field workers, IT staff, lawyers, and managers. Our results provide a first look at the unique security and privacy challenges that humanitarian organizations face when collecting, processing, transferring, and sharing data to enable humanitarian action for a multitude of sensitive activities. These results highlight, among other challenges, the trade-offs between operational security and requirements stemming from all stakeholders, the legal barriers for data sharing among jurisdictions; especially, the need to complement privileges and immunities with robust technological safeguards in order to avoid any leakages that might hinder access and potentially compromise the neutrality, impartiality, and independence of humanitarian action.**

I. Introduction

The humanitarian mandate of saving lives, reducing suffering and respecting human dignity in the context of natural or man-made disasters makes humanitarian organizations attractive targets for surveillance. In particular, armed conflicts and other violent situations often subject civilian populations, including humanitarian workers, to threats of electronic surveillance, censorship, and coercion by local authorities and armed forces. Due to the geopolitical importance of these conflicts, the data collected exclusively for humanitarian purposes could be valuable to other (potentially malicious) entities as well [42]. Unfortunately, although these adversarial environments call for strict data minimization, humanitarian work cannot be effective without the collection, processing and transfer of highly sensitive and identifying information including full names, medical records, possibly biometric details, and any other information necessary to assist or protect vulnerable populations. The recent and still-ongoing digitization of these data flows (which used to exist only on paper) increasingly makes humanitarian organizations the targets of state-sponsored and other resourceful attackers.

Numerous examples of attacks against humanitarian organizations have been documented [35]. These attacks threaten the safety of vulnerable people and humanitarian workers, as well as the neutrality of humanitarian action at large. For example, in the Pattern of Life presentation, the NSA suggested hiding tracking devices in medical supplies to pinpoint the whereabouts of persons of interest [44]. Also, security researchers found that employees of the International Committee of the Red Cross (ICRC) might have been targeted with iOS zero-day exploits, similarly to Ahmed Mansoor, a Middle East political dissident, who was targeted by at least three governmental malware families between 2011 and 2016 [43].

The ICRC, the organization we study in this paper, is one of the world's largest and oldest humanitarian organizations: an impartial, neutral, and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflicts and situations of violence, and to provide them with assistance. The ICRC is one of a handful of humanitarian organizations operating in armed conflicts and other situations of violence and the only one benefiting from the privilege of non-disclosure, which means that it cannot be legally compelled to disclose information [9]. The sensitivity of the contexts in which the ICRC operates, combined with the translation of its legal status (which arose from the Geneva Conventions and their Additional Protocols in 1949 and 1977, respectively [47]), pose fundamental challenges to the enforcement of its digital immunity, *i.e.*, computer security and privacy encompassing technical and organizational factors, and privileges and immunities. However, as we will see, despite the ICRC's unique mandate and legal status, many humanitarian organizations (*e.g.*, United Nations) face similar information security challenges.

In this paper, we perform a qualitative analysis of the information-security challenges faced by the ICRC by conducting semi-structured interviews of 27 ICRC field workers, IT staff, lawyers, and managers. Combined, the interviewed staff has accumulated over 250 years of experience in humanitarian field work, data protection, and management, which gives us a view of the information security challenges they face at the individual, organizational, and legal levels. We discuss the data collected as part of eight sensitive humanitarian activi-

ties (economic security, forensics, health, protection of civilian populations, restoring family links, visit of detainees, water and habitat, and weapon contamination) and the procedures for mitigating risks for beneficiaries and field workers. We then analyze the data flows resulting from these activities in the context of the unique operational, organizational, and legal factors governing the ICRC's field work. Finally, we use the lessons learned to make recommendations for the design and deployment of secure software systems that provide effective defenses to humanitarian organizations. We identify five key takeaways:

- Takeaway 1: Data management rights should be granted on a need basis and should take citizenship, Privileges and Immunities (P&I), and susceptibility to coercion into account.
- Takeaway 2: Operational security might need to be traded off to accommodate the needs and requirements of beneficiaries, field workers, and local authorities.
- Takeaway 3: The ability to establish secure communications among field workers and beneficiaries depends on their P&I, physical locations, and technological capability (or IT service).
- Takeaway 4: Data protection can hamper humanitarian action; in particular, jurisdictions with conflicting legislations can preclude data sharing.
- Takeaway 5: P&I enable humanitarian activities in adversarial environments; however, to be effective, they must be complemented with operational and technological safeguards.

Although this study shares similarities with recent work on computer security for political dissidents and journalists, humanitarian action differs in terms of organizational structure, data flows, and threat models. First, unlike political dissidents who often act individually or as part of small non-governmental organizations (NGOs) [23], [22], [27], [15], [26], to be effective, humanitarian action needs considerable logistical support, generally from a large organization, which significantly complicates the security of the corresponding data flows. In this respect, humanitarian action is more akin to journalism for large media outlets. But, unlike journalism, where one anonymous source generally communicates with one or a few journalists [29], [30], [24], the scale and multi-disciplinary nature of humanitarian action often results in engagement among numerous parties, each with its own area of expertise. Although large collaborations with more than one hundred journalists do exist (*e.g.*, Panama Papers), they tend to not involve anonymous sources and to take place after whistleblowing has occurred [31]. Furthermore, like political dissidents and media outlets, humanitarian organizations are prone to being targeted by powerful attackers; however, to our knowledge, the related work on journalists security has focused on case studies where such attackers were out of scope of their threat model [31].

The rest of this paper is organized as follows: We present an overview of the ICRC, with background pertaining to its organizational structure, privileges and immunities, and operational units, the Data Protection Office and IT department, in Section II. We then describe our methodology in Section III and our qualitative results in Section IV. We discuss potential solutions based on our findings and the lessons learned, for extending the ICRC's P&I to its digital operations, in Section V. Finally, we conclude in Section VI.

II. Overview of the International Committee of the Red Cross

The ICRC as an organization is a three-time Nobel Peace Price laureate with Headquarters in Geneva, Switzerland, and is one of the largest and oldest humanitarian organizations.

At the time of writing, the ICRC has over 16,000 employees, an annual budget of over $2.1 billion, and it conducts numerous humanitarian activities worldwide in situations of armed conflicts and other situations of violence. Unlike many other humanitarian organizations, the ICRC has international legal personality, in-house IT and IT security teams, and an annual investment budget for IT of CHF 20 millions; being a large and well-established humanitarian organization, its advances in technology adoption and security practices could be closely watched and followed by other organizations.

The combination of the ICRC's humanitarian capacity with its unique legal status enables the ICRC to carry out extremely sensitive activities that other organizations, and sometimes even governments, cannot. For example, the ICRC is the only humanitarian organization allowed to visit detainees in Guantanamo, to provide physical rehabilitation care in North Korea or to supply forensics capacity to the government of Mexico in the search of missing persons (where cyber attacks against officials, including the ICRC's interlocutors, have recently been reported by the media [41]).

A. Background

1) Organizational Structure: The ICRC comprises *headquarters*, based in Geneva, Switzerland, and external offices, or *delegations*, in countries where the ICRC operates. Each delegation is under the responsibility of a *head of delegation* who is the official representative of the ICRC in the respective country. Delegations are further grouped into *regions* (currently Africa, Americas, Asia and the Pacific, Europe and Central Asia, Near, and Middle East). Each delegation hosts one or more *units* mandated with a humanitarian *activity*. Units belong to two broad *divisions*, *assistance* and *protection*, mainly depending on whether their provide goods or services, respectively. For example, the *health unit*, which provides medical drugs or war surgery, is part of the Assistance Division, whereas the unit responsible for *prison visits* is part of Protection. These units provide assistance and/or protection to people in need, referred to as *beneficiaries*.

In addition to the ICRC, the *International Red Cross and Red Crescent Movement* also comprises *national societies*. Within their own countries, national societies are autonomous humanitarian organizations that are subject to national law. Although the ICRC and national societies are not linked

hierarchically, national societies outside the host country can provide funding and/or personnel to the ICRC in conflict situations. According to the 1977 Seville agreement, the ICRC takes lead responsibility in conflict areas and for Restoring Family Links activities [46].

In the following, we refer to *mobile staff*, *resident staff*, and *local workers*, as expatriates hired by the headquarters to work in delegations, nationals hired by the delegations and non-ICRC staff (*e.g.*, employed by national societies), respectively.

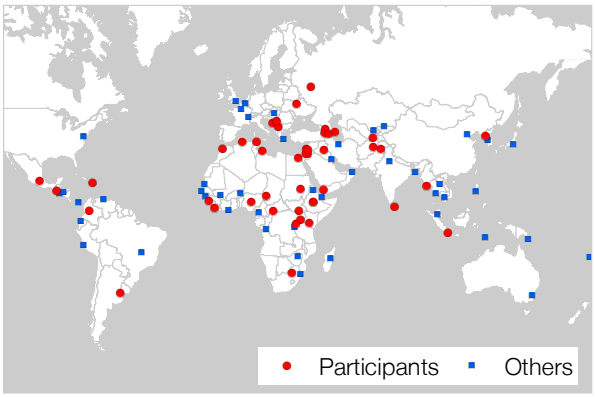

Fig. 1. Location of ICRC delegations where our participants operated (circle) and other delegations (square).

2) Characteristics: At the time of writing, the ICRC has delegations in more than 80 countries (Figure 1) and national societies are present in 190 countries. Out of the 16,000 ICRC employees, approximately 4,000 are hired by the headquarters (HQ) and 12,000 by the delegations. Of the 4,000 staff hired by the headquarters, approximately 900 work in Geneva and 3,100 work as mobile staff. About half of the 3,100 mobile staff serve as delegates managing the ICRC operations in the different countries, and the other half are specialists such as doctors, agronomists, engineers, or interpreters. Delegations also often work closely with the national societies of the countries where they are based, thus they can partner with the national societies for some activities (mainly assistance and Restoring Family Links).

TABLE I
COMPARISON OF THE P&I FOR THE ICRC, NGOS (*e.g.*, MÉDECINS SANS FRONTIÈRES) AND OTHER INTERNATIONAL ORGANIZATIONS SUCH AS THE UNITED NATIONS (UN).

Organization type	*P&I*	*Non-disclosure Privilege*
NGOs		
UN	✓	
ICRC	✓	✓

3) Privileges and Immunities (P&I): P&I [9] apply to both the ICRC institution, and the individuals working for it; they include P&I for the ICRC's property and assets, the inviolability of premises and archives (including electronic documents and data), the exemption to provide evidence in legal proceedings, and the freedom to use the means of communication that the ICRC deems most appropriate. Heads of delegation also usually benefit from the same status accorded to diplomatic officials. At the time of writing, the ICRC has concluded bilateral status agreements recognizing its legal status and P&I with, or obtained equivalent recognition through domestic legislation in, 95 countries.

Together with the United Nations (UN) and a handful of intergovernmental organizations (*e.g.*, ECHO [48]), the ICRC is the only humanitarian organization benefiting from P&I, which sets the ICRC's legal status apart from non-governmental organizations (NGOs). Furthermore, the ICRC is the only international organization benefiting from the privilege of non-disclosure of information, which makes the ICRC immune to legal coercion in this context. We summarize the differences in terms of P&I between the ICRC, NGOs, and the UN in Table I.

P&I are essential for the ICRC to be able to effectively carry out its humanitarian mandate in volatile, dangerous and geopolitically sensitive environments in a neutral, impartial and independent manner. For example, compelling a local worker to testify in favor, or against, one of the parties in an armed conflict could be perceived as a violation of the ICRC's neutrality and independence and, ultimately, compromise its possibility to have access to areas of conflict and other situations of violence, and proximity to victims. P&I also shield the ICRC employees from negative consequences resulting from the exercise of their functions or from their efforts to respect their contractual duties to the ICRC. An example of the former is engaging with armed groups to secure access to affected populations or address humanitarian concerns and alleged violations of international law. An example of the latter is the duty of discretion of the ICRC employees, which includes a prohibition against providing evidence in legal proceedings without prior consent from the ICRC.

B. ICRC Units, and Legal and Technological Departments

Below, we briefly describe the mission of the Assistance and Protection divisions, and of the Data Protection Office (DPO) and technological departments that we interviewed in this study. We refer to Appendix C for more details on the ICRC's organizational structure.

1) Assistance Units:

- *Economic Security.* The Economic Security unit helps individuals, households or communities with food, basic shelter, clothing, and hygiene, as well as the essential assets needed to earn a living.
- *Health.* The Health unit ensures that people affected by a conflict can get basic health care that meets universally recognized standards. This might involve assisting existing health services or temporarily replacing them.
- *Water and Habitat.* The Water and Habitat unit provides water in conflict zones and creates or maintains a sustainable living environment.
- *Weapon Contamination.* The Weapon Contamination unit ensures the safety of the ICRC employees and beneficiaries with respect to conflicts relying on conventional (*e.g.*,

landmines) or unconventional weapons (*e.g.*, chemical munition).

2) Protection Units:

- *Forensics.* The Forensics unit handles the finding, recovery, and identification of the bodies of people who have died during wars, disasters or migrations.
- *Restoring Family Links (RFL).* Together with national societies, the RFL unit locates people, exchanges messages, reunites families, and clarifies the fate of persons missing due to conflicts or disasters.
- *Protection of Civilian Populations (PCP).* The PCP unit enforces the Geneva Conventions's mandate that prohibits all attacks on civilians and others not taking part in combat and requires that they be protected [47].
- *Visit of detainees.* The unit responsible for visits of detainees aims to secure humane treatment and conditions of detention for all detainees, regardless of the reasons for their arrest and detention.

3) Data Protection Office (DPO): The DPO[1] is the ICRC's supervisory body with regards to all personal-data protection matters. It is empowered to perform its duties and exercise its functions with complete independence and acts as the essential component for the protection of individuals with regard to the processing of their personal data. In order to protect natural persons in relation to the processing of their personal data, the DPO monitors the application of the provisions of the ICRC rules on the protection of personal data and contributes to its consistent application throughout the operations of the ICRC. In the case where a person considers that their rights have been infringed under the ICRC rules on data protection, the DPO refers the matter to the ICRC data-protection independent commission that will examine the case and make a decision.

4) Information and Communication Technology (ICT): The ICRC's ICT department designs, develops, and implements new technologies and systems in line with the ICRC strategy. In particular, it ensures the staff's permanent access to IT systems by maintaining reliability, system integrity, and security of electronic data. It provides an efficient operating service easily accessible and able to deliver support, and a homogeneous and centralized service management. Finally, it contributes to training and raising the ICRC employees' awareness of ICT processes, rules and tools.

III. Methodology

Due to the lack of prior studies on security challenges faced by humanitarian organizations, we opted for an inductive approach (*i.e.*, development of theory based on data). We chose in-depth interviews as our main qualitative method for better understanding the different factors that pose challenges to humanitarian personnel. Secondly, we surveyed our participants in order to retroactively obtain information of interest that was not originally collected in the interviews. Finally, we incorporated an observational approach by reviewing internal policies, documents, procedures, and observing field practices at a delegation bordering an area in armed conflict.

A. Participants

We interviewed people from 8 out of the 11 operational units with direct contact with beneficiaries or arms carriers[2], among them several participants have experience in a variety of units. Although it might seem that our interviews only cover a small portion of the ICRC's delegations, our participants' experiences spanned virtually all regions in which the ICRC operates (Figure 1). This is because field workers typically operate in 9-24 month engagements (depending on the hardship of their missions) and are rotated to new delegations after a break period. Throughout the interviews, our participants mentioned 53 unique delegations where they have worked during their career. In total, the combined experience of our participants amounted to about 278 years at the ICRC (10 years on average). Most of the participants had additional years of experience in many other humanitarian organizations.

B. Recruitment and Participants' Profile

Our connection with the ICRC was formed after being contacted for advice on technology. Due to our mutual interest, our contacts at the ICRC enabled us to recruit participants within the organization both laterally (across divisions) and vertically (from deployed field workers to heads of divisions). We began interviews by focusing on employees with field experience: humanitarian workers involved directly in the collection and management of data. As organizational, technical, and legal aspects began to emerge, we observed the need to expand our subject profile to also include personnel with indirect relations to the collection and management of data (*e.g.*, ICT and DPO personnel), both because field workers did not always have subject matter expertise in areas beyond their duties and because these individuals had an effect on the practices of field workers. When new topics emerged and a participant lacked subject-matter knowledge to answer questions, we recruited participants with relevant expertise. For example, if a participant in ICT cited managerial constraints in technology deployment involving hospitals, we interviewed participants with a managerial role in the health division.

C. Interviews

1) Procedure: Following the recommendations from Baker et al. [1], we expected to conduct 15-25 interviews until we stopped observing the emergence of new topics. We exhausted new topics after 27 interviews. Similar studies in other areas have conducted similar amounts of interviews [31], [29], [25], [14]. When possible, we opted for in-person interviews at the ICRC headquarters in Geneva. We also performed on-site interviews at a delegation bordering a country under active armed conflict, as well as at two hospitals operated by the ICRC in that delegation. For all other interviews, we opted for VoIP meetings. We provide a summary in Table II.

[1] https://www.icrc.org/en/document/data-protection

[2] The four remaining units are: the Security and Crisis Management unit, which provides guidance and support for managing staff security, the Policy and Legal units, as well as the unit responsible for relations with arms carriers.

TABLE II
SUMMARY OF INTERVIEWS. TWO RESEARCHERS CONDUCTED ALL INTERVIEWS BETWEEN JULY AND NOVEMBER 2017.

Identifier	*Unit or Division*	*Regions*	*Language*	*Duration*
P0	Assistance	Europe and Central Asia	English	51 min
P1	Data Protection	Europe and Central Asia	English	60 min
P2	Data Protection	Europe and Central Asia	English	40 min
P3	Economic Security	Middle East	English	67 min
P4	Economic Security	Europe and Central Asia	English	188 min
P5	Forensics	Europe and Central Asia	English	50 min
P6	Forensics	Americas	Spanish	47 min
P7	Forensics	Middle East	English	46 min
P8	Health	Europe and Central Asia	English	N/A[1]
P9	Health	Middle East	English	53 min
P10	Health	Middle East	English	44 min
P11	Health	Middle East	English	74 min
P12	Health	Europe and Central Asia	English	43 min
P13	Health	Europe and Central Asia	English	53 min
P14	ICT	Middle East	English	60 min
P15	ICT	Europe and Central Asia	English	79 min
P16	ICT	Europe and Central Asia	English	45 min
P17	ICT	Europe and Central Asia	English	30 min
P18	ICT	Middle East	English	92 min
P19	Protection	N/A[2]	English	54 min
P20	Protection of Civilians	Europe and Central Asia	English	45 min
P21	Protection of Civilians	Europe and Central Asia	English	61 min
P22	Restoring Family Links	Europe and Central Asia	English	64 min
P23	Restoring Family Links	Europe and Central Asia	English	55 min
P24	Visit of Detainees	N/A	N/A	N/A[3]
P25	Water and Habitat	Europe and Central Asia	English	39 min
P26	Weapon Contamination	Europe and Central Asia	English	68 min

[1] The recording software crashed during P8's interview. While we were able to transcribe the interview from cached files, the length is unavailable.
[2] P19 retired from the ICRC six years ago after a long trajectory in the organization, hence the lack of regional information.
[3] P24 requested participation data to be erased; we consider P24 to have withdrawn from the study.

2) Interview Script: Through our inductive approach and the conduction of semi-structured interviews, we iteratively refined our questions as new topics of interest emerged [4]. Initially, we identified areas of interest, based on the review of the ICRC's data protection rules [45]. Subsequently, we refined the questionnaire in consultation with our liaison. Finally, we performed a "trial run" with a participant with 20 years of experience in a variety of roles in the ICRC, and we incorporated the feedback. We also supplemented our questionnaire by drawing from the instruments utilized by McGregor et al. [29] in overlapping areas: computer-security training and general security practices.

Our finalized questionnaire comprised seven categories: background, data collection, data processing, data transfers, data breaches and security, information security training, and general security practices. We provide our interview instruments in Appendix A. When topics of interest emerged during interviews (*e.g.*, context-specific information), we posed additional questions to explore them in more depth.

D. Data Preparation and Analysis

Two researchers recorded and transcribed all interviews. The recordings amount to over 25 hours and the transcription generated approximately 150,000 words. We employed a grounded theory approach when coding [4]. When possible, two researchers participated in an interview. One researcher lead the interview, while the other engaged in an initial coding phase so that themes of interest could be incorporated in following interviews. After an interview concluded, both researchers discussed the set of codes, adding more codes if consensus was not reached. If a researcher was not present, this process was done after the researcher listened to the recording.

Following the appearance of common themes, we began our focused coding phase by using our transcriptions and initial codes. Both researchers iteratively developed conceptual categories in which relevant excerpts of interviews were clustered. As new interviews were conducted, we revisited our transcripts and continued to modify our codes. For flexibility, we did not engage in a formal axial coding process. As we began to observe saturation in certain areas, we proceeded to theoretically combine our categories and subcategories, looking for relationships between them.

In this latter stage, we involved two more researchers for deliberation. We also used our liaisons and ongoing interviews to in/validate our inferences. In this way, we were able to reduce consensus problems between researchers, as most ambiguities could be resolved by the participant's input.

E. Survey

Following the identification of new areas of interest, specifically perceived sensitivity of data, comfort level with technology, and perceived importance of technological needs, to complement the interview data, we sent a follow-up survey to all of our participants. The survey was conducted by the ICRC

in October 2017 and it took about 10 minutes to complete. Participants completed an Excel form whose aggregate results were given to us, and we matched the responses of each participant with their interview information. We provide our survey instrument in Appendix B.

F. Validity

Validity in qualitative research is not as straightforward as in quantitative research [4], [28]. Hence, we only attempt to provide an evaluation of our study in this regard. We do this by following Maxwell's model for validity in qualitative studies [28], assessing our design against *descriptive validity* (factual accuracy of the accounts), *interpretative validity* (interpretation of the accounts), and *generalizability* (internal and external: generalizing within/beyond the group).

Our assessment is as follows:

- We ensure *descriptive validity* by saving the audio recordings of the interviews and by performing verbatim transcriptions.
- Due to our thorough coding methodology and the absence of significant disparities of the participants' accounts during the coding process, we argue *interpretative validity*.
- We argue *internal generalizability* on the practices of humanitarian workers within the ICRC. Our subject pool encompasses virtually all geographic areas of operation and over 278 combined years of experience. Furthermore, all employees adhere to the same practices and rules established by the organization, which limits variation in the practices hereby explored. However, beyond the ICRC, humanitarian work is large and varied. Through this study alone, we cannot assert that the results readily *externally generalize*.

We omit *theoretical validity* and *evaluative validity*, as we do not attempt to explain why these observed phenomena occur (theorization), nor do we seek to dis/credit the practices in place (evaluation)—we leave these aspects for areas of future study.

G. Bias

We proceed to outline factors that could have biased this study's results and the precautions we took to address them.

1) Self-Selection Bias: Participants who are better connected to our liaison, more privacy-conscious, and more interested in the study, are likely more represented in our sample. To address this, our liaison benefited from internal support of the ICRC direction and divisions for recruiting diverse participants. In addition, we asked questions that pertained to the participants' units (*e.g.*, about colleagues'/delegation's practices, etc.). When possible, we cross-checked the practices by interviewing the upper management of a unit to identify other practices that were not mentioned. As mentioned, we expect the large number of participants and units, as well as their geographical diversity and extensive experience, to be representative of the needs and practices of the ICRC.

2) Availability of Resources and Individuality: The ICRC is a large and established entity that operates internationally. The presence of in-house IT, IT security, and Data Protection offices, likely correlates to more mature data security infrastructure and training, leading to better practices as compared to other humanitarian organizations.Although these factors affect the generalizability of our study to other humanitarian organizations, our study is still valuable in that it sheds light on an important subgroup of humanitarian organizations with a mandate under international law that benefit from a variety of unique privileges and immunities, and it describes a set of challenges that could be shared by other humanitarian organizations. We refer to Annex D for a more detailed comparison between the ICRC and other humanitarian organizations.

3) Small Sample-Size: It is inherently challenging to define a specific number of interviews that will grant the study the same validity that's enjoyed by quantitative research [4], [1]. It is likely that some behaviors were less (or not) observed. Nonetheless, in considering both the geographic reach of our participants, their remarkable number of years of experience, and our rigorous methodology, we remain confident that our results largely capture the security challenges currently faced by humanitarian organizations.

H. Ethics

Our study was reviewed and approved by the Institutional Review Board (IRB) of our institution before any research activities began. We obtained informed written or verbal consent from all participants, both to participate in the study and to have the interviews' audio recorded. We transmitted and stored these audio files only in encrypted form and redacted all personal information that identified the interviewees. As humanitarian workers often work with vulnerable populations (*e.g.*, refugees, prisoners, etc.), we asked them not to reveal sensitive information to us about specific individuals with whom they had dealt with. Participants were free to withdraw from the study at any point during the interview and up to 30 days after the interview was conducted; P24 chose to do so. Furthermore, participants could request certain information to be redacted or omitted at their own discretion. We offered no incentives to participants for their involvement in our study.

IV. Results

In this section, we provide an in-depth qualitative analysis of the practical challenges of enforcing the computer security and privacy of humanitarian organizations and the non-disclosure privilege of the ICRC. First, we investigate the operational and legal frameworks in which the ICRC carries out its field work and identify practical factors that influence the deployment of security technology for humanitarian action (Section IV-A). Second, we describe the ICRC's current practices of data collection, the associated risks for field workers, beneficiaries, and states, and their mitigation techniques (Section IV-B). Third, we analyze the data flows resulting from the ICRC's activities regarding digitization, storage, access, and destruction and how

they are influenced by these practical factors (Section IV-C). Finally, we summarize our takeaways (Section IV-D).

We find that the ability of humanitarian field workers to carry out their mandate hinges on numerous operational and legal factors such as developing capacity by training local workers, operating in local, untrusted facilities, and negotiating and maintaining bilateral agreements with local authorities. These factors tend to differ from other at-risk groups such as political dissidents [23], [22], [27], [15], [26] and journalists [29], [30], [24] whose activities can be carried out individually, or in small groups, with no or little support from authorities. As a result, whereas journalists generally depend on their own security practices and that of their sources, humanitarian workers must consider a multitude of other factors such as the engagement, acceptance, and trustworthiness of the local actors and infrastructure, the confidentiality of their physical location, and the specific Privileges and Immunities (P&I) recognized in their delegation's bilateral agreement. We refer to Annex E for a more detailed comparison between humanitarian workers and journalists.

A. Operational and Legislative Factors

1) Operations: In this section, we discuss the operational factors governing the ICRC's computer security practices in the field and in particular: *(a)* the vulnerability of beneficiaries, *(b)* capacity building, *(c)* coercion resistance, *(d)* physical security, and *(e)* the usage of mobile devices.

a) Vulnerability of Beneficiaries: Beneficiaries influence data collection, based on whether they are able and capable to use technology freely. In environments such as detention facilities or in repressive countries, for example, the level of control imposed on beneficiaries is so high that technology cannot offer meaningful safeguards.

> "In many places, we are not allowed to have any electronic tools with us. When you go in a prison, you cannot even have your phone with you. You have to leave it at the entrance or at the car. Normally, collection is paper but once you go back to the office, you fill electronic forms and part of the data goes to specific databases." (P1)

b) Capacity Building and Collaborations: The ICRC, and in particular the Health and Forensics units, sometimes train ICRC or non-ICRC staff while carrying out their mission and/or collaborate with national societies. These activities can challenge the ICRC's independence due to the required interactions between the ICRC's delegates and the non-ICRC workers, and their potential embedding into local facilities such as hospitals or governmental institutions. For example, the Health unit occasionally occupies a dedicated space (*e.g.*, a floor) within a hospital building, where patients must first register before receiving treatment from the ICRC doctors; and their medical data is also stored in the hospital's database. Among other factors, capacity building raises concerns with respect to resident and non-ICRC workers' trustworthiness which should be carefully vetted.

> "I worked with someone who was a translator. [...] And then I heard someone accuse him of having taken part in the genocide [...] I didn't know what to do because this guy worked with me over weeks and then in a sense, he might have used the information that he had. We didn't know that it was really the end of the war. The war could have started again and anything could have happened." (P19)

c) Coercion Resistance: The ICRC personnel are often targets of coercion to disclose information. To protect resident staff and their families against these threats and mitigate insider threats, Protection units limit the exposure of their resident staff to sensitive material. Although mobile staff could also be coerced, it would likely be less productive: "the authorities will not be able to threaten me because I can leave the country the day after." (P22)

Furthermore, to mitigate insider threats, certain delegations grant administrative access rights only to mobile or regional staff. These decisions are made at the discretion of the delegation and are confidential. However, they generally depend on the perceived risks of coercion and the sensitivity of the operations in the country. For example, Protection units segregate their data per delegation; the person managing each database, which we refer to here simply as *system administrator*, has complete access to the delegation's database.

> "In countries where [... system] administrators should not have access, you have regional offices today in all continents, where [system] administrators that are foreigners, or mobile, deal with the parts of the database that [resident system] administrators should not have access to." (P20)

d) Physical Security: As the ICRC operates in unstable and conflict-affected areas, threats to physical security and damage/theft of equipment are common. In delegations, IT infrastructure is kept within the offices of the delegation (which most of the time benefit from P&I). All laptops and desktop devices have full-disk encryption. In addition, the staff is instructed to store data in servers or cloud-based services hosted in ICRC premises (at delegations or HQ). Whenever possible, these servers are located in a dedicated room that is always locked and accessible only to specific staff (*e.g.*, mobile system administrators). Capacity building, as sometimes done by the Health and Forensics units, does not always permit such level of physical security. In instances where the ICRC operates in locally supported facilities, the access and management of data is regulated by local rules.

e) Usage of Mobile Devices: There are no standard protocols for using and securing mobile devices. Although the use of short-range radio devices is standardized, mobile phones "[are] more a matter of ad-hoc negotiations than a protocol that we would apply [systematically]." (P0) For safety reasons, delegates must establish a radio contact every one or two hours to notify the delegation of their position. In addition, they are also provided with a professional mobile phone upon arriving in the country. However, these devices are considered

untrustworthy and should never be used to communicate confidential information. Several participants reported being asked by armed groups to surrender their mobile phones during meetings. Furthermore, leaving the phone at the entrance of a detainment facility is also a common practice. Beyond the ICRC's own interest in adopting a strong posture with respect to mobile security, it also appears critical to maintain the trust of certain beneficiaries.

> "We are also preoccupied because [...] we put our interlocutors at risk, if we meet with them. And we have been [wrongly] accused in the past of driving authorities to places and then people being attacked after meeting with us. It is something that is very much on our mind." (P20)

f) Summary: In summary, the ICRC's ability to protect the confidentiality of the data it collects with technological safeguards is sometimes limited by the beneficiaries and their degree of freedom. As we will discuss in Section IV-B3, to mitigate some of the risks for vulnerable beneficiaries, the ICRC sometimes pseudonymizes the data it collects. In addition to weakening the extent to which the ICRC's processed information can continue to benefit from P&I (see Section IV-A2), capacity building also creates challenges in terms of physical security and coercion resistance. Finally, the ICRC's field workers sometimes need to adopt ad-hoc usage of mobile phones to protect the physical location of their beneficiaries.

2) Legislation: In addition to operational factors, the ICRC's computer security practices are also subject to legislative factors including: *(a)* loopholes in legislations, *(b)* asymmetric legislation, and *(c)* legal pressure and P&I.

In most of the delegations where the ICRC operates, it is backed by strong legal guarantees at multiple levels. Data stored by the ICRC is protected from States by legal provisions in both international and domestic laws of the jurisdictions in which they operate, as introduced in Section II-A. Furthermore, the ICRC has taken significant steps to adopt strong data-protection rules, taking as a baseline the EU General Data Protection Regulation for the creation of their own regulatory system for data protection [45]. These strong and uniform rules would guarantee a uniform level of rights across operations and help address coercion attempts by State authorities, according to P2. Yet, despite these efforts, we found that the situation could become problematic if/when States take advantage of loopholes, do not recognize the legal immunity, or seek to acquire the data forcefully through legal and illegal coercion.

a) Loopholes in Legislation: The main legal issue faced by the ICRC comes from situations in which States take advantage of loopholes in the ICRC's P&I coverage. The previously introduced privileges conferred to the ICRC as an institution grants the inviolability of ICRC premises, properties, and assets. However, in situations where the ICRC has to operate with facilities that are in a State's premises, such benefits are nullified. With the shift towards capacity building *i.e.*, training locals in the services provided by the ICRC, (see Section IV-A1), these ICRC services are offered within a State's infrastructure. For example, in certain countries, the ICRC doctors operate within State-owned hospitals, hence data collected during these engagements (whether by ICRC or non-ICRC staff) are not legally protected by the aforementioned P&I but are managed as per the local legislation.

> "If we are using a government healthcare facility, we need to be transparent with them in all ways." (P2)

b) Asymmetric Legislation: Variation in legislation across delegations can also have an effect on data-security practices. For example, delegations and national societies under the regulations imposed by the EU data-protection legislation cannot share data with delegations in third countries not bound by EU law. Recently, as a response of the migration crisis in Europe, there was an initiative between 25 national societies and 4 delegations within the EU, and bound by EU law, to share data that would help restore family links for people who were separated when migrating from non-EU countries (not bound by EU law) under a code of conduct.[3] However, the situation became problematic when a family member returned to their home country that does not provide guarantees established under EU law and they opened an inquiry about their lost family member. For instance, a tracing request opened in ICRC Kabul—for somebody lost when migrating into the EU—cannot be fulfilled by delegations within the EU because the Kabul delegation might not have the EU data protection guarantees. This is not only a source of distrust across delegations because it is seen as discrimination, but it is also seen as a concern because it "reduces the area of action" and it is seen as an impairment for the deployment of new uniform technologies, says P23. Thus, there is a perception that following the stipulated data-security practices can become a hindrance and a source of conflict.

> "If we follow EU regulation today, you can do nothing more with data. So we found it quite difficult to find the right balance between applying the right standards of data security while still doing our work of helping people." (P22)

c) Legal Pressure and Immunity: Non-recognition of the P&I conferred to the ICRC is among their most difficult challenges. Despite 196 States having ratified the importance of the humanitarian mission of the ICRC expressed in the Geneva Conventions, as of 2016, the ICRC has obtained the legal status, privileges, and immunities with only 103 countries, including states where the ICRC does not operate, through either bilateral status agreements (95 countries) or direct modification of domestic legislation (8 countries) [9].

Even in jurisdictions where the ICRC has immunity from jurisdiction and legal proceedings, it could still receive court orders such as subpoenas. In such cases, the ICRC can refer to the status agreement as necessary. For example, in the case of an order to testify in a case, the ICRC can refer to its impartiality and neutrality; countries often respect the humanitarian mandate and abide to the status agreements.

[3] https://www.icrc.org/en/document/rfl-code-conduct

TABLE III
SUMMARY OF DATA TYPES COLLECTED BY VARIOUS UNITS OF THE ASSISTANCE (TOP) AND PROTECTION (BOTTOM) DIVISIONS.

Unit	*Full Name*	*Personal*	*Medical*	*Forensics*	*IHL*	*Infrastructural*
Economic Security	✓	✓	✓			
Health	✓	✓	✓			
Water and Habitat						✓
Weapon Contamination						✓
Forensics			✓	✓	✓	
Detainees Visits	✓	✓	✓		✓	
Protection of Civilians	✓	✓			✓	
Restoring Family Links	✓	✓	✓	✓	✓	

However, the same scenario can be problematic when the host country does not have a system of judicial guarantees, a bilateral status agreement does not exist, the country does not recognize the P&I, and/or rule of law is not obeyed. In such cases, diplomatic negotiation could be the first step and termination of operations the last resort.

d) Summary: For the most part, the ICRC's P&I constitute a strong first layer of digital security that most humanitarian organizations do not have (See Appendix D-2). For States that want to misappropriate data, the legal protections raise the stakes, because bypassing these protections translates to going directly against the status agreements and international law that safeguard the ICRC. Additionally, we found that legal guarantees might be weakened when the ICRC operates within public infrastructure (because the P&I do not apply to the data in the same way). Nevertheless, states could take advantage of this. Finally, variations of data protection legislation are seen as an impairment as they might hinder data-sharing capabilities within and beyond the organization, hence we offer a discussion of potential mitigations in V-C.

B. Data Collection

In this section, we describe the data types collected by the various ICRC units, the perceived sensitivity of these data, and the risk mitigation techniques used.

1) Data Types:

a) Personal Data: to enable continued assistance or protection (Table III), most units that are in direct contact with beneficiaries collect personal data, including full names, and use certain procedures (*e.g.*, pseudonymization) to mitigate the risks. Although the personal data collected differ from one unit to another, the most common ones include phone number and address of the beneficiary and contact person, age, gender, ID number, and place of birth. In addition to this general personal data, some contexts require the collection of additional contextual data. As discussed in Section IV-B3, units with especially vulnerable beneficiaries systematically rely on pseudonyms instead of full names.

b) Medical Data: Many of the units collecting personal data also collect medical data when their activities require it. Apart from one of the Health programs related to Primary Health Care, which collect only aggregate data, other Health programs collect medical data.

c) Forensics Data: In the humanitarian context of forensics identification, the ICRC collects two types of forensic data: post-mortem and ante-mortem data. The former are collected by the Forensics unit and include details of the grave sites and bodies; the latter are collected in partnership with the Restoring Family Links (RFL) unit and include the circumstances of disappearance, physical description, medical history, and dental records. The Forensics unit can either collect data independently or in cooperation with the local authorities as part of capacity building (Section IV-A1).

d) International Humanitarian Law (IHL) Data: All Protection units collect details on potential IHL violations as part of their normal data collection. Due to the contextual nature of IHL data, they are collected as free-form text.

e) Infrastructural Data: Finally, the Water and Habitat and Weapon Decontamination units collect data, among others, pertaining to critical infrastructure and the damage resulting from military attacks on that infrastructure, respectively.

2) Sensitivity of Collected Data: We have discussed the various types of data collected by the ICRC. Below, we present a qualitative analysis of the perceived sensitivity of these data. At a high level, participants reasoned about data sensitivity in terms of the risks of an unauthorized data-leakage, that the beneficiaries, the ICRC, and States face.

a) Risks for Beneficiaries: Medical and protection-related data are among the most sensitive, often because the data contains important information for non-humanitarian purposes (*e.g.*, intelligence). In situations of conflict, armed groups and State actors might want to use this information to track whether high-profile targets have received medical care or have been detained and are in a certain prison/hospital.

In other contexts, such as in the Americas, members of organized crime or armed groups track individuals who report missing family members or have information about murders and burial sites, because these can be used as criminal evidence. Furthermore, stolen files have been used to find and silence individuals and their relatives.

b) Risks for the ICRC: The ICRCs position as a confidant heavily relies on trust and their ability to safeguard the information they are entrusted with. Failure to ensure their impartiality or confidentiality poses a great risk to the ICRC, as it could hamper their dealings with countries or regions as distrust spreads. In terms of relationships with States, bilateral agreements will be at stake, and the ICRC

might lose the ability to operate in a region, according to P1. Furthermore, access to beneficiaries and interlocutors (and privileged information they may share) is another risk. P11 mentions that, following the alleged involvement of other humanitarian organizations in the identification of Bin Laden, there was a general unrest towards these organizations as they were seen as "external forces that collect data and use it for negative purposes," or as P2 mentions, "in many countries, they still [wrongly] believe the ICRC does spy work."

> "It is a trusted, confidential relationship. Imagine if all this information is released publicly, the authorities will not trust us anymore, nor will the people. In fact, we wont be able to work anymore. If someone can access all this data, the damage will be so huge because, what will be the perception in other countries where ICRC works?" (P23)

c) Risks for States: Finally, the disclosure of data can become politically harmful to states, in particular, data related to humanitarian consequences of armed conflicts. The Weapon Contamination unit mainly deals with the presence of unexploded ordinances. This work produces information on particular methods used in conflicts. These data, translated into humanitarian consequences, are used by the ICRC in its discussions with arms carriers. This is also the case in contexts such as: prisoner treatment, mass graves, etc. Failure to protect the information can have consequences for both the ICRCs ability to operate, as well as the states reputation.

> "Where it becomes very political, very sensitive is when we are talking about missing persons that authorities, governments are using. You can imagine today, what would it mean for the [redacted] government to know how many people are supposed to be missing because of their actions. It is a highly political question and it can really put the ICRC in a difficult situation[4] if people were able to say how many people had been arrested by the [redacted] forces." (P0)

3) Risk Mitigation: In light of the risks that a data leakage poses, there are several mitigation mechanisms that the ICRC implements and that can be divided in pseudonymization and obfuscation, minimization, and destruction.

a) Pseudonymization and Obfuscation: Although the unit responsible for visits to detainees also collects full names, it systematically relies on pseudonyms at the time of data collection in prison facilities in order to protect its beneficiaries; the mappings between pseudonyms and full names are kept under key. Other units have reported occasionally omitting the collection of certain data, or relying on pseudonyms, to protect the identity of their beneficiaries, but such practices are the exception rather than the norm.

b) Data Minimization: The unit responsible for detainees always avoids transmitting any information that could single out a person. The collected information that the person allows to be processed also undergoes a decision mechanism to determine whether it should not be used in case re-identification could be feasible under some circumstances. Conversely, the collection process for the protection of civilians causes a need to input a maximum amount of data to the database in order to enable the understanding of the broader context instead of information limited to individual cases. "With time, everything will be collected electronically, in the database." (P20).

Finally, data can be destroyed and/or archived in the HQ data center when the ICRC's operation in a delegation comes to an end, including emergency evacuations (see Section IV-C3).

C. Overview of the ICRC Data Flows

The data collected by the ICRC field workers are then processed in order to enable humanitarian action: data are digitized, stored, managed, and potentially destroyed, as discussed in Sections IV-C1 to IV-C3. Figure 2 shows simplified dataflows resulting from the ICRC activities, the place where each step takes place, and whether they consequently benefit from Privilege and Immunities (P&I). For simplicity, we exclude assessment and registration steps that take place prior to collection, and optional steps such as patient transportation.

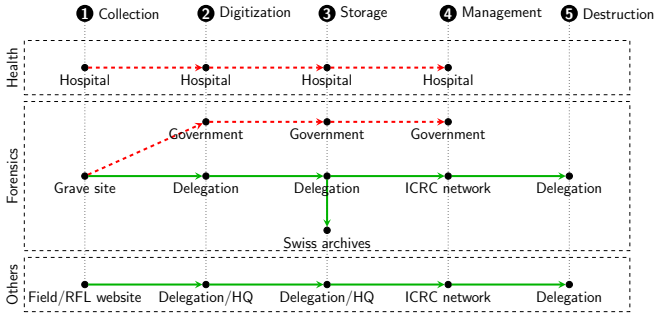

Fig. 2. Overview of the data flows for the Health, Forensics, and other ICRC units. The solid lines correspond to flows benefiting from the privilege of non-disclosure and the dashed lines to flows that do not.

In contrast with data flows resulting from traditional journalist work involving one journalist communicating with one anonymous source [29], [30], [24], the ICRC data flows involve several field workers: those are subject to the operational and legal factors discussed in Section IV-A and they often remain vulnerable throughout the steps of humanitarian action.

1) Collection and Digitization: Although most of the units that we have interviewed still collect data forms on paper, virtually all of them digitize these forms upon returning to the delegation's offices, for book keeping and to enable humanitarian action. Field workers and office staff collect data on paper for logistical and cultural reasons (*e.g.*, electronic devices can be considered invasive by beneficiaries who experienced a trauma). At the time of writing, only two units use digital data collection: The Economic Security unit collects assessment data on mobile devices; and the Restoring Family Links (RFL) unit hosts a website to collect tracing requests.

[4]Disclosure of information relating to International Humanitarian Law can violate the ICRCs impartiality and neutrality if used as evidence.

> "[The beneficiary] can go on the RFL website, open a tracing request, and then can go to the Red Cross. [...] We will have always both because not everybody is connected today [...] and sometimes these people who are not connected are the most vulnerable so it is important that we can offer a personal service in the office." (P22)

2) Storage and Management: As mentioned in Section IV-A1, units store data within the offices of their delegations or at the HQ in Geneva. For example, all the data collected by the Protection units are stored at the HQ, but those of the Assistance units are generally stored at the delegation's offices. As the data collected by the Assistance units are not federated, we focus on the management of the Protection data.

a) Data Isolation: Although the Protection data are centralized, they are segregated by parties in a conflict and/or by delegations to prevent the unauthorized leakage of data among potentially belligerent countries. There is one database per country with the RFL, detainees, and PCP data to which access is granted on a need-to-know basis, as indicated by P23. A side effect, however, is that this anti-coercion policy also prevents legitimate sharing of information among delegations.

> "When you have crises for example in Lake Chad today, it concerns four countries: Nigeria, Niger, Cameron and Chad. They have all their own database but when you need to aggregate the common case load, it starts to be difficult. Sometimes, in crises or situations where there is more than two ICRC delegations, we found a limitation of the information sharing where they all have their own silo." (P22)

b) Data Sharing: The ability to match and share collected data is central to most ICRC units. For example, to be effective, the RFL unit must be able to match tracing requests with reports from witnesses, and to share these data with Forensics or even with other organizations with similar mandates. Data sharing within the same unit in the same delegation is already in place across the Protection units; but the exchange of data across Assistance and Protection units, as well as units in different delegations, or between the ICRC and other organizations is more challenging.

This is due to the operational and legal factors (Section IV-A) as well as technological challenges. For example, other humanitarian organizations, such as United Nations High Commissioner for Refugees (UNHCR) and United Nations Children's Fund (UNICEF), have developed their own systems to restore family links. As all these systems currently do not interoperate, RFL activities often require a substantial amount of inter-organizational e-mail and/or telephone communications, as mentioned by P20. Another example are Red Cross messages involving postal letters between detainees and their families and that the ICRC must locate, potentially via national societies.

> "I would collect [Red Cross messages] in [redacted], transfer them to the [redacted] Red Cross who would dispatch them to the different national societies where they believe the families of these prisoners are located. But you may also have the case where it is the ICRC that would dispatch the Red Cross messages without transferring them to the national societies of the country because the file is too sensitive [...]." (P1)

3) Destruction: As a data-protection precaution, non-processed data is destroyed whenever (a) there is no need to process all the collected data, (b) the data cannot be used for follow-up, or (c) the processed information can be unlinked from collected personal data. Additionally, when a conflict is about to end, the collected personal data are sometimes destroyed. Health data that require close monitoring is also destroyed after the doctor leaves the field, to avoid unnecessary leakages; but this might create potential problems when trying to follow up on the treated cases. Finally, it is worth mentioning that the units have a "kill button" mechanism to destroy data in case of an emergency, to avoid that data be stolen if they "have to leave in a rush [...] because there is an attack" (P19).

D. Takeaways

In this section, we summarize the lessons learnt in this paper so that the security and privacy community can use them as guidelines when designing systems for adversarial environments. First, we found that coercion resistance was an important aspect of the ICRC's operational security and that it was addressed at three levels: *(a)* staff's access is granted on a need-to-know basis, *(b)* staff and system administrators' access might also be based on their citizenship, and *(c)* delegations do not have access to each others' data (Takeaway 1). Second, in practical situations, such as when performing capacity building or when negotiating bilateral agreements, the ICRC needs to tradeoff P&I, coercion-resistance, and/or physical security in order to enable humanitarian action (Takeaway 2). Third, despite the ICRC's P&I to employ secure communications, this protection is not always possible for beneficiaries or third parties depending on their vulnerability, and technical capacity (Takeaway 3). Fourth, asymmetric legislation can hamper humanitarian action by disabling the sharing of necessary data between jurisdictions (Takeaway 4). Finally, we find that, in order to be effective despite these legal and operational factors, the ICRC's P&I should be complemented with novel security technologies (Takeaway 5).

V. Consequences for Technological Solutions

Although digitization of information has great potential for streamlining work processes and enforcing stricter quality assurances, the risks of making sensitive data available through electronic means can also be a potential barrier for the overarching adoption of digital technology. The evaluation of a survey taken by non-ICT participants showing that there is currently a gap between the need for secure data digitization and its fulfillment (Figure 3) forms the basis of our discussion. Out of the 22 non-ICT participants, 18 took the survey.

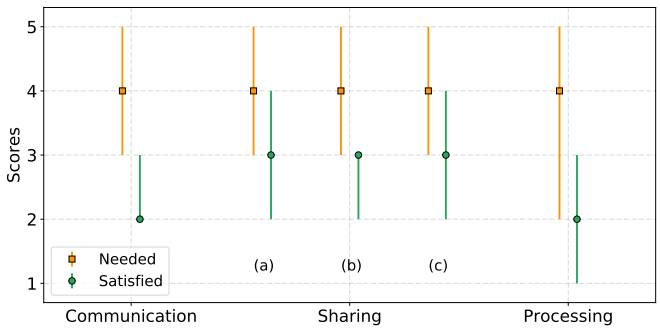

Fig. 3. Evaluation of our ICRC survey (see Appendix B). The figure compares perceived data digitization need and fulfillment with respect to secure communication, sharing ((a) same unit/team in same delegation; (b) different unit/team in same delegation; (c) same unit/team in different delegation), and processing. The scores range from "not at all" for 1 to "highly" for 5. The graphs show medians as reference points and 10th and 90th percentile as upper and lower errors, respectively.

In the case of the ICRC, many challenges have to be considered when attempting to deploy such a secure digital infrastructure. In this section, we discuss the security challenges pertaining to the protection of data in transit and at rest (Sections V-A and V-B, respectively), and to secure data sharing and processing (Section V-C).

A. Secure Communication

The availability of secure communication channels is a fundamental prerequisite enabling several of the applications discussed in this section. Humanitarian organizations, and the ICRC in particular, present unique challenges for secure communications. First, staff and beneficiaries need to communicate in a multitude of adverse environments that are often susceptible to eavesdropping, to physical attacks on the infrastructure, and to coercion of the personnel. In particular, staff can operate in different types of facilities with different levels of trustworthiness (*e.g.*, HQ, offices of the delegation or sub-delegation, local hospitals), or in the field (Takeaway 2). Furthermore, staff and beneficiaries can be located in one of many delegations, or at ICRCs HQ in Geneva (Takeaway 3). Finally, staff and beneficiaries can use various endpoints, *e.g.*, laptops, desktop computers, or mobile devices such as smartphones.

Traditional messaging applications featuring end-to-end encryption (*e.g.*, Signal[5]) provide confidentially but expose the accruing metadata to third parties (*e.g.*, in the case of Signal, their operators and Amazon EC2), as well as to network eavesdroppers. As these third parties can be compelled to record and disclose metadata (*e.g.*, via subpoenas), such messaging applications are inappropriate for usage in humanitarian action. Furthermore, any network eavesdropper could analyze the time series of encrypted traffic to link communicating users to each other. It is therefore crucial for the ICRC, and other organizations with similar needs, to employ traffic-analysis-resistant anonymity networks.

One way to resist traffic analysis is through the use of anonymity networks; however, no existing anonymity network is tailored to the different environments and behaviors cited above. More specifically, existing anonymity networks do not fulfill the ICRCs need for strong anonymity within a delegation; nor do they provide robust anonymization of the traffic among the delegations and the HQ in Geneva in a way that is agnostic about the characteristics of this traffic. Existing anonymity network designs typically achieve either strong anonymity or efficiency: For example, the popular Tor anonymity network is relatively efficient but does not defend against an attacker observing ingress and egress traffic [10]. Dissent, the state-of-the-art Dining Cryptographers network, is resilient under a strong threat model but requires one broadcast channel per group of private clients [6]. And Aqua [21] and Herd [20] assume that endpoints exchange padded traffic (chaff) at all times, which is also inadequate for mobile devices. Therefore we need to develop traffic-analysis-resistant networks tailored to complex organizations distributed worldwide, resilient to both local and global cyber threats, and adapted to mobile users operating in adverse environments.

B. Identity and Data Management

The data management application integrates the secure data-sharing and processing applications, which we discuss in Section V-C, and enforces strict security policies. In addition to the above challenges pertaining to the establishment of secure communications, secure identity and data management is also challenging in decentralized settings and, in particular, for complex organizations such as the ICRC with different levels of clearance and compartmentalization (Takeaway 1).

Existing decentralized solutions for private data sharing either forfeit access control or rely on a centralized service. For example, we could envision a data-sharing system where the sender knows the public keys of the recipients and publishes an encrypted copy for every one of them on a decentralized platform such as Bitcoin [33] or BitTorrent[6]. However, in this approach, the access control is enforced before the creation of the encrypted data as every publicly release encrypted ciphertext can be stored forever and can be decrypted by anyone that later compromises the private key. Hence, the system cannot be combined with on-the-fly logging or revocation, because even if a revocation request is published, the encrypted data might have been already accessed. Even worse, it is impossible to be aware of such a leakage as there is no auditability functionality. An alternative would be to decouple the policies from the secrets, thus making the access lists immutable on the blockchain and entrusting the data with some centralized non-blockchain storage service, that holds the encryption keys and checks the on-blockchain access control policy for each access attempt. However, this re-introduces a single point of failure as the logging and delivery of data are not done atomically.

[5] https://signal.org/

[6] http://www.bittorrent.com/

A mix of well-known and novel cryptographic / security tools for data integrity, trust splitting, accountability, and key/identity management could form the basis of such a decentralized data-management system, including scalable and failure-resilient multi-signature schemes [3], [39], [40], secret sharing [37], [38], or next-generation blockchain technologies [18], [19], [32], [33]. Combining and adapting these technologies to design a data-management system that satisfies the needs of the ICRC and other humanitarian organizations is left for future research.

C. Secure Sharing and Processing

Secure data-sharing and -processing plays a key role in enabling humanitarian action and maximizing the impact of research. One of the main barriers for data sharing between the ICRC and other organizations, including national societies, comes from asymmetric legislations and the lack of a homogeneous legal data-protection framework under which data can be securely shared (Takeaway 3). Data protection should not be perceived as a barrier, but as an enforcement of citizen's rights. And technology can help bridge this gap by means of privacy-conscious systems that enable data sharing according to the minimization and proportionality principles of the European GDPR (Takeaway 4) and restrict the leakage of personal identifiable information. There is a need for deploying distributed secure data-processing systems to enable data sharing across asymmetric legislations, in order to provide a homogeneous technological protection that can conform to the most stringent regulations. The possibility of performing requests on secure databases that do not disclose identifiable information would enable more precise and effective humanitarian actions, that are commonly blocked due to the lack of a technological enforcement of data protection.

Secure processing techniques can bring about substantial benefits in terms of operations management for the ICRC and other humanitarian organizations (Takeaway 3). Adapting either software-based approaches (involving cryptographic primitives such as homomorphic encryption [7] and multiparty computation [8]), or hardware-based approaches (involving trusted execution environments such as Intel SGX [17]) to the ICRC scenarios described in Section IV can bring about substantial benefits in terms of operations management. Nevertheless, in order to be readily applied in these scenarios, the aforementioned technologies must address, among others, the following four challenges: (a) scalability to cope with a big number of units/sites/delegations with no options of direct raw data sharing across them, (b) efficiency/versatility to tackle complex analyses or machine learning techniques for processing humanitarian data adequately, (c) big data elastic processing to deal with large volumes of data comprising all the needed contextual information to produce relevant results, and (d) avoiding inference so that the results of processing do not accidentally single out an individual; proper countermeasures must be designed against inference attacks on the results, by taking advantage of frameworks such as differential privacy [12].

Relevant recently proposed systems for privacy-conscious data sharing fall short on some of these challenges and require further research to perfectly match the requirements of secure humanitarian-data processing. For example, distributed database-access approaches [2], [5] do not scale well to a large number of data sources; scalable systems for securely aggregating distributed data [36], [13] present a limited functionality and hardware-enabled machine-learning computations on sensitive data [34] centralize the processing and suffer from single points of failure/trust, and privacy-preserving set operations [16] cannot efficiently cope with large data sets. As there is no one-size-fits-all solution, further research into properly combining and adapting these technologies is needed in order to enable efficient, scalable and versatile secure data-processing able to cope with the needs of the ICRC and other humanitarian organizations.

VI. Conclusion

We presented a qualitative analysis of the security needs and practices of humanitarian field workers, ICT and DPO staff, and managers of the ICRC, a large organization with activities in 80 countries and international immunities. Our study highlights the challenges faced by the ICRC with respect to operational and legal factors and, in particular, the adversity of environments where beneficiaries and infrastructure are located, namely coercion resistance, physical security, usage of mobile devices, and legal loopholes, asymmetric legislation, and legal pressure, respectively. We discussed how these factors influence the ICRC's humanitarian action with respect to data collection and data flows, and drew five takeaways pertaining to (1) coercion resistance, (2) operational security, (3) secure communications, (4) legislation, and (5) technological safeguards. Finally, we contextualized these takeaways with respect to the related work on computer security and privacy, and discussed potential avenues of future work.

Once the appropriate immunity protection systems have been designed, prototyped, and deployed as field tests, we foresee that production will raise additional research, development, deployment, and maintenance hurdles. Although the ICRC, as an early adopter, could assist with the integration of these systems into its workflow, we believe that research, development and maintenance should be delegated to an independent organization such as a non-profit. Delegating production to a non-profit organization could also facilitate adoption by other organizations with similar needs (*e.g.*, NGOs), as well as the interoperability of these systems, increasing their overall utility. Finally, to achieve decentralized trust in practice, the designs of these systems should be peer-reviewed and their implementations open sourced and audited by independent security researchers.

We are in the process of involving more humanitarian and other at-risk organizations to validate the insights gained from the ICRC and to identify potential synergies in the technological solutions needed by different vulnerable communities. Our interlocutors currently include Médecins Sans Frontières and the Freedom of the Press Foundation.

Acknowledgements. This study would not have been possible without the active involvement of the ICRC and in particular Vincent Graf, Massimo Marelli, Charlotte Lindsey-Curtet, and the 27 anonymous participants. The authors are also thankful to the anonymous reviewers, our shepherd Sascha Fahl, Randall Zindler, and Holly Cogliati-Bauereis for their useful feedback; and Yves Lopes and Marc-André Lüthi for their IT support. Finally, the first author warmly thanks the "delegation bordering an armed conflict" for welcoming him as their own.

References

[1] S. E. Baker and R. Edwards, "How Many Interviews Are Enough?" vol. 18, pp. 59–82, 2006.

[2] J. Bater, G. Elliott, C. Eggen, S. Goel, A. Kho, and J. Rogers, "SMCQL: Secure Querying for Federated Databases," *VLDB Endowment*, vol. 10, no. 6, pp. 673–684, Feb. 2017.

[3] A. Boldyreva, "Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme," in *Public Key Cryptography – PKC 2003*. Springer, 2002.

[4] K. Charmaz, *Constructing Grounded Theory*. Sage, 2014.

[5] H. Corrigan-Gibbs and D. Boneh, "Prio: Private, Robust, and Scalable Computation of Aggregate Statistics," in *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)*. USENIX Association, 2017.

[6] H. Corrigan-Gibbs and B. Ford, "Dissent: Accountable Anonymous Group Messaging," in *2010 ACM Conference on Computer and Communications Security (CCS 2010)*. ACM, 2010.

[7] A. Costache and N. P. Smart, "Which Ring-Based Somewhat Homomorphic Encryption Scheme is Best?" in *Topics in Cryptology - CT-RSA 2016*. Springer, 2016, vol. 9610.

[8] I. Damgrd, M. Keller, E. Larraia, V. Pastro, P. Scholl, and N. P. Smart, "Practical Covertly Secure MPC for Dishonest Majority – Or: Breaking the SPDZ Limits," in *ESORICS 2013*. Springer, 2013, vol. 8134.

[9] E. Debuf, "Tools to do the job: The ICRC's legal status, privileges and immunities," *International Review of the Red Cross*, pp. 319–344, 2016.

[10] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," in *13th USENIX Security Symposium*, 2004.

[11] I. Düsterhöft, "The Protection of Journalists in Armed Conflicts: How Can They Be Better Safeguarded?" *Utrecht Journal of International and European Law*, vol. 29, no. 76, 2013.

[12] C. Dwork, "Differential Privacy," in *Automata, Languages and Programming*. Springer, 2006, vol. 4052, pp. 1–12.

[13] D. Froelicher, P. Egger, J. S. Sousa, J. L. Raisaro, Z. Huang, C. Mouchet, B. Ford, and J.-P. Hubaux, "UnLynx: A Decentralized System for Privacy-Conscious Data Sharing," *Privacy Enhancing Technologies*, vol. 2017, no. 4, Jan. 2017.

[14] G. Gebhart and T. Kohno, "Internet Censorship in Thailand: User Practices and Potential Threats," in *2nd IEEE European Symposium on Security and Privacy*, 2016.

[15] S. Hardy, M. Crete-Nishihata, K. Kleemola, A. Senft, B. Sonne, G. Wiseman, and P. Gill, "Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware," in *23rd USENIX Security Symposium*, August 2014.

[16] C. Hazay and M. Venkitasubramaniam, "Scalable Multi-party Private Set-Intersection," in *Public-Key Cryptography PKC 2017*. Springer, 2017, vol. 10174, pp. 175–203.

[17] Intel Corporation, "Intel Software Guard Extensions (Intel SGX)," accessed Oct. 31, 2017.

[18] E. Kokoris-Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing," in *Proceedings of the 25th USENIX Conference on Security Symposium*, 2016.

[19] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding," Cryptology ePrint Archive, Report 2017/406, 2017.

[20] S. Le Blond, D. Choffnes, W. Caldwell, P. Druschel, and N. Merritt, "Herd: A Scalable, Traffic Analysis Resistant Anonymity Network for VoIP Systems," in *ACM SIGCOMM 2015 Conference*, 2015.

[21] S. Le Blond, D. Choffnes, W. Zhou, P. Druschel, H. Ballani, and P. Francis, "Towards Efficient Traffic-analysis Resistant Anonymity Networks," in *ACM SIGCOMM 2013 Conference*, August 2013.

[22] S. Le Blond, C. Gilbert, U. Upadhyay, M. G. Rodriguez, and D. Choffnes, "A Broad View of the Ecosystem of Socially Engineered Exploit Documents," in *Network and Distributed System Security Symposium (NDSS)*, 2017.

[23] S. Le Blond, A. Uritesc, C. Gilbert, Z. L. Chua, P. Saxena, and E. Kirda, "A Look at Targeted Attacks Through the Lense of an NGO," in *23rd USENIX Security Symposium*, August 2014.

[24] A. Lerner, E. Zeng, and F. Roesner, "Confidante: Usable Encrypted Email - A Case Study With Lawyers and Journalists," in *2nd IEEE European Symposium on Security and Privacy*, 2016.

[25] C. F. Maitland, H. F. Thomas, and L. M. Ngamassi Tchouakeu, "Internet Censorship Circumvention Technology use in Human Rights Organizations: An Exploratory Analysis," *Journal of Information Technology*, vol. 27, no. 4, pp. 285–300, dec 2012.

[26] W. R. Marczak and V. Paxson, "Social Engineering Attacks on Government Opponents: Target Perspectives," in *17th Privacy Enhancing Technologies Symposium*, 2017.

[27] W. R. Marczak, J. Scott-Railton, M. Marquis-Boire, and V. Paxson, "When Governments Hack Opponents: A Look at Actors and Technology," in *23rd USENIX Security Symposium*, August 2014.

[28] J. A. Maxwell, "Understanding and Validity in Qualitative Research," *Harvard Educational Review*, vol. 62, no. 3, pp. 279–300, 1992.

[29] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner, "Investigating the Computer Security Practices and Needs of Journalists," in *24th USENIX Security Symposium*, 2015.

[30] S. E. McGregor, F. Roesner, and K. Caine, "Individual versus Organizational Computer Security and Privacy Concerns in Journalism," in *16th Privacy Enhancing Technologies Symposium*, 2016.

[31] S. E. McGregor, E. Watkins, M. N. Al-Ameen, K. Caine, and F. Roesner, "When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers," in *26th USENIX Security Symposium*, 2017.

[32] M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman, "CONIKS: Bringing Key Transparency to End Users," in *Proceedings of the 24th USENIX Conference on Security Symposium*. USENIX Association, 2015, pp. 383–398.

[33] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[34] O. Ohrimenko, F. Schuster, C. Fournet, A. Mehta, S. Nowozin, K. Vaswani, and M. Costa, "Oblivious Multi-Party Machine Learning on Trusted Processors," in *25th USENIX Security Symposium (USENIX Security 16)*. USENIX Association, 2016, pp. 619–636.

[35] Privacy International, "Aiding Surveillance."

[36] J. L. Raisaro, J. R. Troncoso-Pastoriza, M. Misbach, J. S. Sousa, S. Pradervand, E. Missiaglia, O. Michielin, B. Ford, and J.-P. Hubaux, "MedCo: Enabling Privacy-Conscious Exploration of Distributed Clinical and Genomic Data," in *4th International Workshop of Genome Privacy and Security*, Oct 2017.

[37] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in *IACR International Cryptology Conference (CRYPTO)*, 1999, pp. 784–784.

[38] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[39] E. Syta, P. Jovanovic, E. Kokoris-Kogias, N. Gailly, L. Gasser, I. Khoffi, M. J. Fischer, and B. Ford, "Scalable Bias-Resistant Distributed Randomness," in *38th IEEE Symposium on Security and Privacy*, May 2017.

[40] E. Syta, I. Tamas, D. Visher, D. I. Wolinsky, P. Jovanovic, L. Gasser, N. Gailly, I. Khoffi, and B. Ford, "Keeping Authorities "Honest or Bust" with Decentralized Witness Cosigning," in *37th IEEE Symposium on Security and Privacy*, May 2016.

[41] The Citizen Lab, "Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware."

[42] The Guardian, "GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief."

[43] The Intercept, "The Million Dollar Dissident: NSO Groups iPhone Zero-Days used Against a UAE Human Rights Defender."

[44] ——, "The NSA Plan to Find Bin Laden by Hiding Tracking Devices in Medical Supplies."

[45] The International Committee of the Red Cross (ICRC), "Handbook On Data Protection In Humanitarian Action."

[46] ——, "Reinforcing Red Cross / Red Crescent Cooperation in Emergencies: The Seville Agreement."

[47] ——, "Geneva Conventions and Commentaries."

[48] Wikipedia, "Directorate-General for European Civil Protection and Humanitarian Aid Operations)."

APPENDIX A
INTERVIEW QUESTIONNAIRE

A. Background

- What is/was your [humanitarian/technical] background add/or main area of responsibility at ICRC?
- Did you work in any humanitarian organization prior to joining ICRC? If so, can you tell us a little bit about how your work at ICRC differs from these earlier employments?

B. Data Collection

- What type of data do/did you collect in the field?
- Do you use electronic devices to collect these data? If so, please tell me a little bit about your experience with the collection process:
  1) Could you elaborate on any procedures used to protect the data's confidentiality (i.e., prevent from it being disclosed)?
  2) Were these data shared more broadly within ICRC or with third parties, and if so, how was this sharing done?
- Have you ever experienced the loss or theft of data or electronic devices in the field and if so what was the context of these incidents?
- Could you elaborate on any instances in which these data were transferred to electronic devices? Were any precautions taken to prevent these data from being disclosed?
- Could you elaborate on an instance in which you had to discuss electronically any sensitive information related to these data?
- What were your phone usage practices in situations where your location was confidential?
- What problems might arise if these data were disclosed? Please elaborate on the short term and long term consequences.

C. Data Processing

Are you aware of instances where:

- collected data was left unprocessed because of the risk to the rights and freedoms of the subjects. If so why?
- the risk assessment was done after processing the data? If so, could you elaborate on them as well as the assessment outcome?
- mitigating measures were recommended prior to data processing and if so what they were?

D. Data Transfer

- Did you ever need to access data from ICRC or third-parties requiring additional approvals? If so, could you elaborate on your experience with seeking these approvals?
- Were you ever denied access to data that you needed? If so, why and could you comment on the consequences this denial had on your work?
- Is there a record of all data collected, processed, and/or transferred by ICRC and if so who is responsible of it?

E. Data Breaches and Security

- Do you have a protocol for reducing the risk of data being lost, altered, or disclosed at any stage of its management?
- Is data generally encrypted at rest or prior to being transferred and if so, who is responsible of the decryption keys?
- Where are data stored? If they are sometimes stored in different locations, what is the policy to determine where to store a piece of data?
- How long are data generally stored before being destroyed or anonymized?
- How are subpoenas dealt with? Does ICRC sometimes operate in countries that do not recognize its immunity from jurisdiction and if so, have any complications ever arisen?
- Without revealing specifics that could compromise continued use of computer systems, can you share a general sense of what kind of security incidents happened, and how they were handled?
- Is there a record of all data breaches reported at ICRC and if so who is responsible of it?

F. Information Security Training

- Does [humanitarian/technical] staff generally receive computer security trainings?
  If so, please tell me a little bit about how they were delivered and what content they contained:
- Were they "live" (e.g., streamed) or recorded?
- Did they involve hands-on exercises?
- Was there any type of evaluation/grading of participants? Could a "failing" grade have negative consequences?
- Do you feel these trainings were successful? Would you change anything in those trainings?

G. General Security Practices

- Tell us about your experience with security-related technology. Please describe any recommendations you received regarding these technologies.
- Describe any technological or security-related problems you have encountered for which you wish you had a solution.
- What kinds of devices do you use and who owns and/or administers them?
- For field workers only: How do you obtain assistance when you encounter issues with technology and computer security at work?
- For field workers only: How would you describe your comfort level when utilizing technology? How about security-related technology?
- Is there anything else about your work that you'd like to tell us or think we should know?

APPENDIX B
SURVEY QUESTIONS

- What is your Unit?
- What is the sensitivity of the data collected by your current unit?
- What is your comfort level with technology and computer security?
- In your opinion, what is the importance of the following needs within your unit and to what extend are they currently fulfilled?

1) digital data collection
2) secure communication
3) data sharing
   a) same unit, same delegation
   b) different unit, same delegation
   c) same unit, different delegation
4) research on data collected by all delegations
5) security of your electronic devices

APPENDIX C
ICRC'S ORGANIZATIONAL DIAGRAM

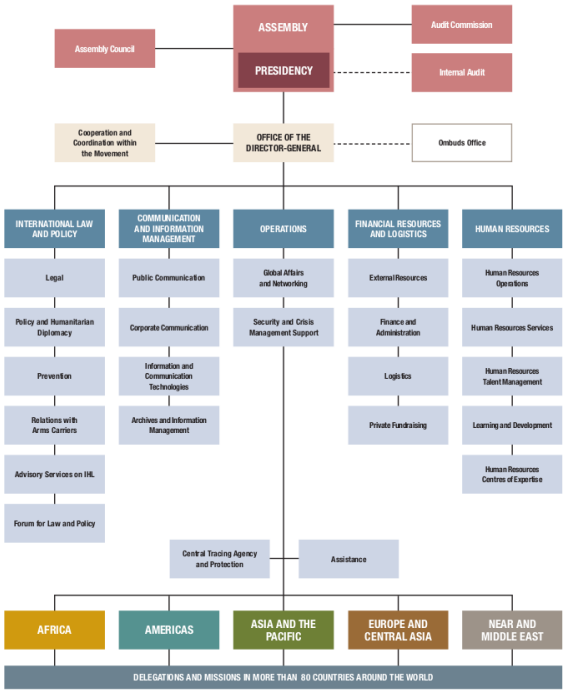

Fig. 4. Detailed Organizational Diagram of ICRC.

APPENDIX D
COMPARISON WITH OTHER HUMANITARIAN ORGANIZATIONS

The ICRC shares some similarities with other humanitarian organizations. However, there are some key factors that set the ICRC apart, the most relevant of which are discussed in this appendix: *mandates*, *Privileges and Immunities (P&I)*, and *independence of infrastructure*.

1) Mandates: Based on the mandates established on the Geneva Conventions, the ICRC has acquired a legal status similar to that of an International Organization (IO) such as the UN. These mandates were the main drivers in propelling the ICRC's transition from being a Swiss private association to acquiring its observer status in the UN as an IO, and all the Privileges and Immunities (P&I) necessary for carrying out its treaty-based mandate [9]. Contrary to other humanitarian IOs, however, the ICRC is bound to follow the mandates established in the Geneva Conventions and not the mandates and governance of specific States, such as the UN. Humanitarian NGOs and private associations, which were not established under similar international treaties, will simply not benefit from the same international legal framework under which the ICRC operates.

2) P&I: Closely tied to its mandate, the ICRC enjoys a significantly better legal position than most non-governmental humanitarian organizations. National and international NGOs, along with similar private associations, do not enjoy the same international legal P&I as the ICRC; they remain subject to both the laws in their country of origin, as well as the full legal framework of their host country [9]. This lack of P&I strips off an important first layer of protection and exposes humanitarian organizations to subpoenas, search and seizure orders, etc. Although the ICRC still receives court orders (see Section IV-A2), they are able to deflect most court orders by referring to the status agreements or to their coverage under international law, whereas an organization without the same P&I would be forced to comply.

3) Independence of Infrastructure: Across the world, the ICRC operates both within government-provided infrastructures and on its own privately-owned premises (*e.g.*, state hospitals and ICRC hospitals). The same is true for other humanitarian organizations. As described by P12, the decision to use public or private infrastructure is often related to the mission of the organization and the costs (independent being more expensive according to P12). For example, organizations that are more focused on capacity building will prefer to be embedded within government structures. It is important to note, however, that the implications of choosing between in/dependent structures between traditional humanitarian NGOs and the ICRC are not exactly the same. An independent structure has certain legal guarantees for the ICRC (See Section IV-A2), whereas the same guarantees do not apply to traditional NGOs.

APPENDIX E
COMPARISON WITH JOURNALISTIC ORGANIZATIONS

In this section, we compare the ICRC to journalistic organizations by contrasting our study to the literature on (digital) security of journalism [11], [24], [29], [30], [31] in terms of threat models, operational security, and legal protection.

1) Threat Models: Generally, both types of organizations are confronted with similar threat actors on their missions including local and foreign governments, armed forces, and criminal organizations. However, although the threat models are similar, our understanding of particularly sensitive journalistic activities (*e.g.*, whistleblowing), whose threat models include state-sponsored attackers, is lacking.

2) Operational Security: Both journalistic and humanitarian organizations operate at extremely high stakes in general, as they aim to protect their clients, collaborators, and personnel under extreme situations.However, it can be argued that humanitarian personnel face much greater risks due to their direct exposure to the perils of armed conflicts when rescuing individuals in danger [11]. In highly adversarial environments, humanitarian work involves the protection of their clients' identities and any data collected and shared about them. Any violation of this trust can have severe consequences for any of the involved parties (*e.g.*, imprisonment or death), and easily leads to the loss of the organization's credibility, thus depriving it of its working foundation (see Section IV-B3). Therefore, protection of the involved parties is of foremost importance for humanitarian organizations, and to ensure the operational security of their daily work, the ICRC has developed extensive and strict protocols and rules for their personnel [45].

> "The ICRC [...] views confidentiality as a [...] dogma. You're kind of brainwashed when you join to always be extremely cautions of sharing data with others [...]." (P19)

There exist of course similar means to ensure the digital security of journalistic operations [24], [29], [30], [31].

3) Legal Protection: The International Humanitarian Law (IHL) discusses legal protection in armed conflicts, for which it forms the baseline of legal protection for both humanitarian and journalistic personnel. Beyond that, there are some noteworthy differences: on the one hand, the *freedom of the press* is commonly enshrined in the constitutions of democratic states, such a protection is basically non-existent or only minimal at best in many non-democratic countries, as can be witnessed in the annual *Press Freedom Index*[7] compiled by the *Reporters Without Borders* NGO. The mission of the ICRC, on the other hand, is enshrined in the Geneva Conventions, and the P&I for the ICRC personnel, contrary to journalists, are captured in bilateral agreements between the ICRC and the host countries. In general, however, it is important to remember that legal protection can only be provided if the host country recognizes domestic and/or international laws (see Section IV-A2).

[7] https://rsf.org/en/ranking