On Enforcing the Digital Immunity of a Large Humanitarian Organization

**Stevens Le Blond, Alejandro Cuevas, Juan Ramon Troncoso-Pastoriza, Philipp Jovanovic, Bryan Ford, Jean-Pierre Hubaux**
“Computer security and privacy encompassing technical & organizational factors, and privileges and immunities (P&I)”
Hackers led warplanes to hospital, claims Syria surgeon

Spyware in Mexico Targets Investigators Seeking Stud...
Outline

• The International Committee of the Red Cross (ICRC)
• Methodology
• Results
  • Data collected
  • Data flows
  • Operational and legal factors
• Proposed architecture
Outline

• The International Committee of the Red Cross (ICRC)
• Methodology
• Results
  • Data collected
  • Data flows
  • Operational and legal factors
• Proposed architecture
Characteristics of the ICRC

- x3 Nobel Peace Prices
- 16,000 employees
- 2.1 billion annual budget
- At-risk operations
- Privileges & Immunity (P&I)
Privileges and Immunities (P&I) 1/2

- Bilateral agreement
- Armed conflicts
- Inviolability of premises
- Freedom of communications
<table>
<thead>
<tr>
<th>Organization type</th>
<th>P&amp;I</th>
<th>Non-disclosure Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGOs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UN</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>ICRC</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Outline

• The International Committee of the Red Cross (ICRC)
• Methodology
• Results
  • Data collected
  • Data flows
  • Operational and Legal factors
• Proposed architecture
Methodology

Inductive approach

Qualitative methods

27 interviews until topic exhaustion

278 years of experience
<table>
<thead>
<tr>
<th>Identifier</th>
<th>Unit or Division</th>
<th>Regions</th>
<th>Language</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>P0</td>
<td>Assistance</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>51 min</td>
</tr>
<tr>
<td>P1</td>
<td>Data Protection</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>60 min</td>
</tr>
<tr>
<td>P2</td>
<td>Data Protection</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>40 min</td>
</tr>
<tr>
<td>P3</td>
<td>Economic Security</td>
<td>Middle East</td>
<td>English</td>
<td>67 min</td>
</tr>
<tr>
<td>P4</td>
<td>Economic Security</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>188 min</td>
</tr>
<tr>
<td>P5</td>
<td>Forensics</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>50 min</td>
</tr>
<tr>
<td>P6</td>
<td>Forensics</td>
<td>Americas</td>
<td>Spanish</td>
<td>47 min</td>
</tr>
<tr>
<td>P7</td>
<td>Forensics</td>
<td>Middle East</td>
<td>English</td>
<td>46 min</td>
</tr>
<tr>
<td>P8</td>
<td>Health</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>N/A³</td>
</tr>
<tr>
<td>P9</td>
<td>Health</td>
<td>Middle East</td>
<td>English</td>
<td>53 min</td>
</tr>
<tr>
<td>P10</td>
<td>Health</td>
<td>Middle East</td>
<td>English</td>
<td>44 min</td>
</tr>
<tr>
<td>P11</td>
<td>Health</td>
<td>Middle East</td>
<td>English</td>
<td>74 min</td>
</tr>
<tr>
<td>P12</td>
<td>Health</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>43 min</td>
</tr>
<tr>
<td>P13</td>
<td>Health</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>53 min</td>
</tr>
<tr>
<td>P14</td>
<td>ICT</td>
<td>Middle East</td>
<td>English</td>
<td>60 min</td>
</tr>
<tr>
<td>P15</td>
<td>ICT</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>79 min</td>
</tr>
<tr>
<td>P16</td>
<td>ICT</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>45 min</td>
</tr>
<tr>
<td>P17</td>
<td>ICT</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>30 min</td>
</tr>
<tr>
<td>P18</td>
<td>ICT</td>
<td>Middle East</td>
<td>English</td>
<td>92 min</td>
</tr>
<tr>
<td>P19</td>
<td>Protection</td>
<td>N/A²</td>
<td>English</td>
<td>54 min</td>
</tr>
<tr>
<td>P20</td>
<td>Protection of Civilians</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>45 min</td>
</tr>
<tr>
<td>P21</td>
<td>Protection of Civilians</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>61 min</td>
</tr>
<tr>
<td>P22</td>
<td>Restoring Family Links</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>64 min</td>
</tr>
<tr>
<td>P23</td>
<td>Restoring Family Links</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>55 min</td>
</tr>
<tr>
<td>P24</td>
<td>Visit of Detainees</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A³</td>
</tr>
<tr>
<td>P25</td>
<td>Water and Habitat</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>39 min</td>
</tr>
<tr>
<td>P26</td>
<td>Weapon Contamination</td>
<td>Europe and Central Asia</td>
<td>English</td>
<td>68 min</td>
</tr>
</tbody>
</table>
Location of ICRC delegations
Outline

• The International Committee of the Red Cross (ICRC)
• Methodology

• Results
  • Data collected
  • Data flows
  • Operational and legal factors
• Proposed architecture
Outline

• The International Committee of the Red Cross (ICRC)
• Methodology
• Results
  • Data collected
  • Data flows
  • Operational and legal factors
• Future work
Summary of collected data types by units

<table>
<thead>
<tr>
<th>Unit</th>
<th>Full Name</th>
<th>Personal</th>
<th>Medical</th>
<th>Forensics</th>
<th>IHL</th>
<th>Infrastructural</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economic Security Health</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Water and Habitat Weapon Contamination</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Forensics
Detainees Visits
Protection of Civilians
Restoring Family Links
Sensitivity of Collected Data

Beneficiaries

ICRC Organization

Governments
Outline

• The International Commitee of the Red Cross (ICRC)
• Methodology
• Results
  • Data collected
  • Data flows
  • Operational and legal factors
• Proposed architecture
Overview of data flows
Outline

• The International Committee of the Red Cross (ICRC)
• Methodology
• Results
  • Data collected
  • Data flows
    • Operational and legal factors
• Proposed architecture
Organizational structure

1. Collection
2. Digitization
3. Storage
4. Management
5. Destruction

Health
- Hospital
- Hospital
- Hospital
- Hospital

Forensics
- Grave site
- Delegation
- Delegation
- Swiss archives
- ICRC network
- Delegation

Others
- Field/RFL website
- Delegation/HQs
- Delegation/HQs
- ICRC network
- Delegation

Red lines represent the Health section, while green lines represent the Forensics and Others sections.
Practical factors
Practical factors

Vulnerability

Capacity building

Coercion

Other regions
- Europe & Central Asia
- Asia & Pacific
- Americas
- Africa

1 2
Beneficiaries
Collection device
Field

Hospital

2 3 4 5
Delegation
Subdelegation

Example region: Near & Middle East

3 4
HQ

Switzerland
Practical factors

Vulnerability

Capacity building

Coercion

Physical attacks

Other regions
- Europe & Central Asia
- Asia & Pacific
- Americas
- Africa

Field

Example region: Near & Middle East

Hospital

Collection device

Subdelegation

Delegation

HQ

Switzerland
Practical factors

Vulnerability

Capacity building

Coercion

Physical attacks

Legal factors

Other regions
- Europe & Central Asia
- Asia & Pacific
- Americas
- Africa

Example region: Near & Middle East

Switzerland
Lessons learnt

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.

2. Operational security might need to be traded off to accommodate the needs and requirements of beneficiaries, field workers, and local authorities.

   • The ability of establishing secure communications among field workers and beneficiaries depends on their P&I, physical locations, and technological capability (or IT service).

   • Data protection can hamper humanitarian action; in particular, jurisdictions with conflicting legislations can preclude data sharing.

3. P&I enable humanitarian activities in adversarial environments; however, to be effective, they must be complemented with operational and technological safeguards.
Outline

• The International Committee of the Red Cross (ICRC)
• Methodology
• Results
  • Data collected
  • Data flows
  • Operational and legal factors
• Proposed architecture
Needs of ICRC staff

- **Processing**
  - Satisfied: 2
  - Needed: 4

- **Management**
  - Satisfied: 3
  - Needed: 5

- **Communication**
  - Satisfied: 2
  - Needed: 4
Problems with existing communication technology

- no end-to-end encryption
- Meta-data leakages
- Personal smartphones

Need for privacy-enhancing network for organizational communications
Organizational structure and practical factors

Vulnerability

Capacity building

Coercion

Physical attacks

Legal factors

HQ

Capacity building

Other regions
Europe & Central Asia
Asia & Pacific
Americas
Africa

Vulnerability

Hospital

Collection device

Delegation

Subdelegation

Example region: Near & Middle East

HQ

Switzerland
Proposed architecture

Legend
A. Needs, Practices & Trainings

Vulnerability
Capacity building
Coercion
Physical attacks
Legal factors

Example region: Near- & Middle East

Other regions
Europe & Central Asia
Asia & Pacific
Americas
Africa

Switzerland

HQ
Proposed architecture

Vulnerability
A. Needs, Practices & Trainings
B. Communication

Capacity building

Coercion

Physical attacks

Legal factors

Legend

Delegation building

Secure server
Access point
Floor 2
Floor 1

Other regions
Europe & Central Asia
Asia & Pacific
Americas
Africa

Field
Hospital
Beneficiaries
Collection device

HQ
Subdelegation
Delegation
Example region: Near- & Middle East
Switzerland
Proposed architecture

Legend
A. Needs, Practices & Trainings
B. Communication
C. Data Management
D. Processing

Delegation building
Secure server
Access point
Floor 2
Floor 1
Access point

Hospital
Collection device
Field

Subdelegation
Example region: Near- & Middle East

Internal blockchain (for access control)

Other regions
Europe & Central Asia
Asia & Pacific
Americas
Africa

Public cloud
HQ: Switzerland

HQ

Vulnerability
Capacity building
Coercion
Physical attacks
Legal factors
Take home messages

• Need for secure communications, data management, and processing robust to coercion, lack of physical security and asymmetric legislations

• Deploy a technological platform tailored to these legal and organizational factors

• Create a foundation combining academic and industrial capability to deploy security tech at ICRC and other humanitarian organizations

stevens.leblond@epfl.ch
How did you recruit participants?

- Recruited participants both laterally (across divisions) and vertically (from field workers to heads of divisions)

- Began interviewing employees with experience collecting & managing humanitarian data

- As organizational, technical, and legal aspects emerged, we included managers, ICT and DPO personnel
How did you prepare and analyzed the interview data?

- Two researchers recorded and transcribed all interviews (25 hours of recording and 150,000 words of transcriptions)

- One researcher lead the interview while the other did an initial coding so new themes could be quickly incorporated

- After interview both researchers discussed the set of codes adding more codes if consensus wasn’t reached

- Interactively developed conceptual categories in which relevant excerpts were clustered
What is your assessment of the validity of your study?

• Following Maxwell model for validity in qualitative studies:
  • *Descriptive validity* by saving audio recording of the interviews & performing verbatim transcriptions
  • Absence of significant disparities of the participants’ accounts during coding (*interpretative validity*)
  • *Internal generalizability* on the ICRC practices due to diversity of geographical areas of operations (no *external generalization*)
  • Omit *theoretical* and *evaluative validity* as we do not attempt to explain why observed phenomena occur nor dis/credit practices in place
What are the potential biases of your study?

• Many participants and units and extensive experience likely representative of the needs and practices of the ICRC (*self-selection bias*)

• Availability of ICT and DPO likely correlate to better practices (*availability of resources and individuality*)

• Geographic reach, years of experience, and rigorous methodology make us confident that our results capture security challenges (*small sample-size*)
What was your interview script?

• Identified areas of interest by reviewing the ICRC’s data protection rules & refined it with our liaison

• Trial run with participant with 20 years of experience and incorporated feedback

• Drew from instruments utilized by related work

• Our questionnaire comprised seven categories (cf. Appendix A):
  • Background
  • Data collection
  • Data processing
  • Data transfers
  • Data breaches and security
  • Information security training
  • General security practices
How does the ICRC compare with other humanitarian organizations?

• ICRC is an International Organization (IO) whose mandates follow from the Geneva conventions

• Benefits from better *Privileges and Immunities* than most humanitarian NGOs

• Operates both within government-provided infrastructure and its own privately-owned *infrastructure*
How does the ICRC compare with journalistic organizations?

- Both *threat models* involve governments, armed forces, and criminal organizations.

- *Operational security* of journalists is tailored to one or few individuals, although ICRC often has dozens or more field workers.

- Unlike freedom of the press, the ICRC’s *legal protection* is captured in bilateral agreements with host countries.
How did you ensure that interviews were conducted ethically?

- Study approved by IRB

- Informed consent from all participants to participate in the study and record the interviews’ audio

- Audio files were transmitted and stored only in encrypted form and some information was redacted

- Possibility to withdraw from study up to 30 days after the interview (P24 chose to do so)
What precautions will you take before deploying your proposed platform?

• Designs will be peer-reviewed

• Implementations will be open sourced and audited by independent experts

• Integration will be delegated to a foundation based in Switzerland