ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

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

عم تحترق
بأمان

Digital immunity

“Computer security and privacy encompassing *technical & organizational factors*, and *privileges and immunities (P&I)*”

What practical factors influence use of security tech by humanitarian orgs?

Spyware in Mexico Targete
Investigators Seeking Stude

The Daily Telegraph
BRITAIN'S BEST-SELLING QUALITY DAILY

Hackers led warplanes to hospital, claims Syria surgeon

David Nott believes he was targeted by hackers while directing surgery in an underground Syrian hospital over Skype and WhatsApp

By Hayley Dixon, Aisha Majid *and* Steven Swinford

A BRITISH surgeon who helped carry out operations in Aleppo fears that the hacking of his computer led to a hospital being bombed by suspected Russian warplanes.

In a world first, David Nott, a renowned consultant, gave remote instructions via Skype and WhatsApp to doctors carrying out surgery in an underground hospital.

But, after footage was broadcast by the BBC, Mr Nott believes his computer was targeted, allowing hackers to gain coordinates of the M10 hospital.

Weeks later a "bunker buster" bomb destroyed the M10 when planes, believed to be Russian, delivered a direct hit to the operating theatre, killing two patients. The hospital had to close.

Mr Nott believes that the timing of the attack and the precise nature of the target meant the location could only have been gleaned from coordinates on his computer.

Mr Nott, who has carried out dozens of operations in person in Syria, said that following advice from those on the ground, he would not perform any more surgery over his computer.

It is understood the International Committee of the Red Cross will hold a meeting with staff next month to warn of the danger of hacking, using Mr Nott's fears as an example.

Last night Mr Nott said: "The thing that gets me is that we now cannot help doctors in war zones. If somebody is watching what we are doing and blows up the hospital then that is a war crime.

"It is a crime against humanity that you can't even help a doctor in another country carry out an operation. It is a travesty." Whitehall sources told *The Daily Telegraph* that technical experts believed that pinpointing a location by carrying out such a hack was plausible.

Aid workers and international watch groups have warned that hospitals have become a target in Syria, with some estimates suggesting that there have been 450 attacks since 2011.

Priti Patel, the former Cabinet minister, said: "It's a huge, huge issue. We should all pay an enormous tribute to David Nott. He is an amazing individual who in the most difficult circumstances has been saving lives in Syria while the bombs of Assad have been falling down.

"It would hardly be surprising if Russian interference was behind the bombing of this hospital. It speaks of the appalling regime and the lack of respect for human life. We need to put pressure on Russia and ask what has happened here."

Mr Nott has been nicknamed the "Indiana Jones of surgery" for his work in war zones. He has trained surgeons in Syria and has been appointed OBE.

His claims come at a time of heightened tensions between Russia and Britain after the poisoning of the former Russian spy Sergei Skripal and his daughter Yulia in Salisbury, Wilts. Vladimir Putin has long been at loggerheads with the West over his support for Bashar al-Assad's forces in Syria.

Experts believe that the sophistication of the bomb that hit the M10 suggests it was dropped by Russian jets.

During the remote operation, which was broadcast by *Newsnight* on Sept 13 2016, Mr Nott used a selfie stick to

Continued on Page 2

Editorial Comment: Page 19

Outline

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

Outline

- The International Commitee 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

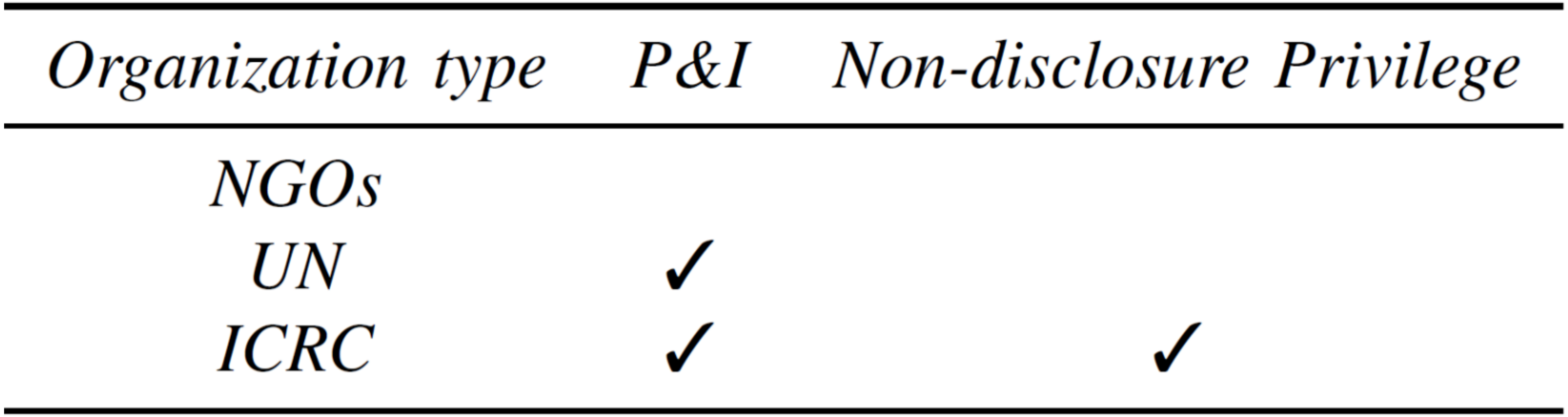
Bilateral agreement

Armed conflicts

Inviolability of premises

Freedom of communications

Privileges and Immunities (P&I) 2/2



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

Outline

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

Methodology

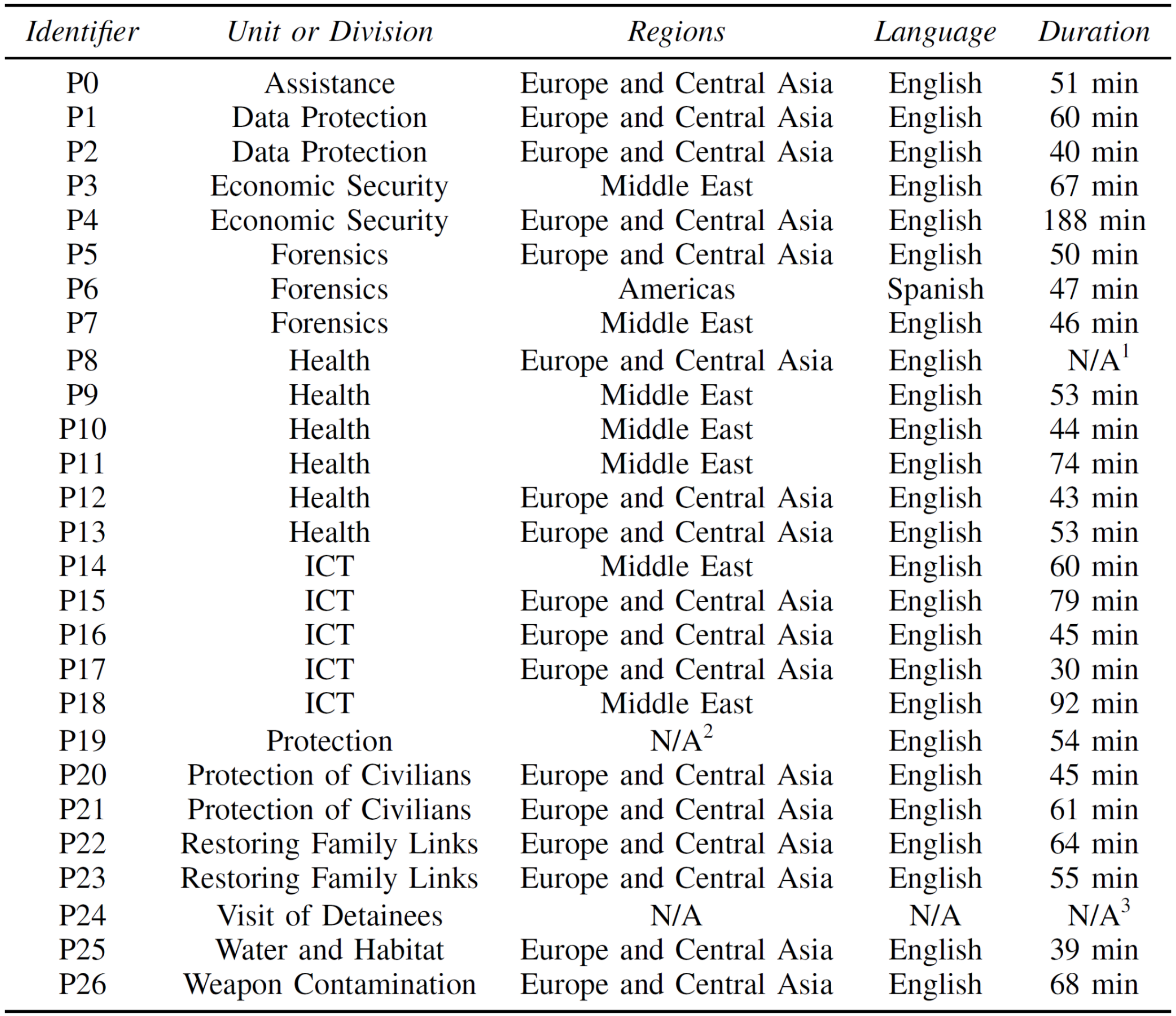
Inductive approach

Qualitative methods

27 interviews until topic exhaustion

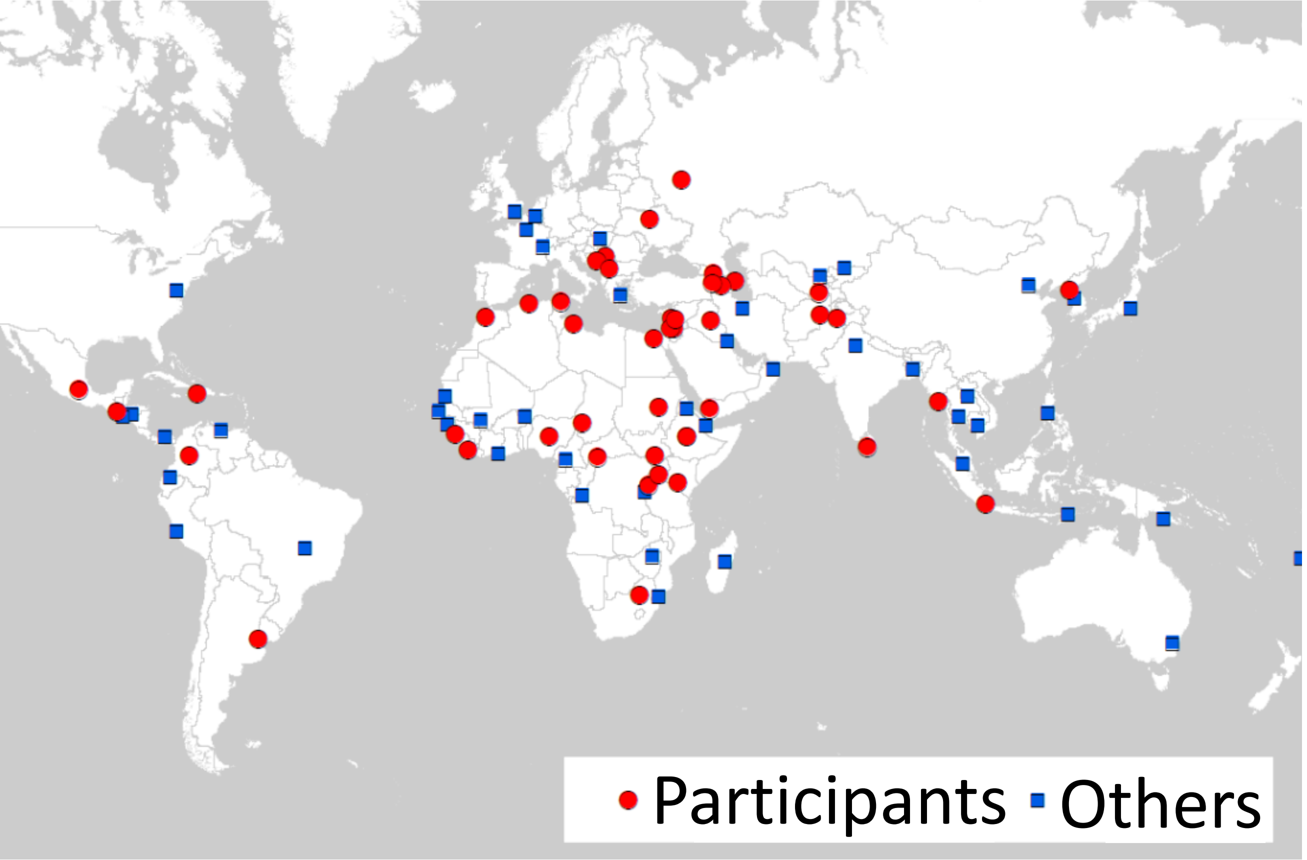
278 years of experience

Summary of interviews



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

Location of ICRC delegations



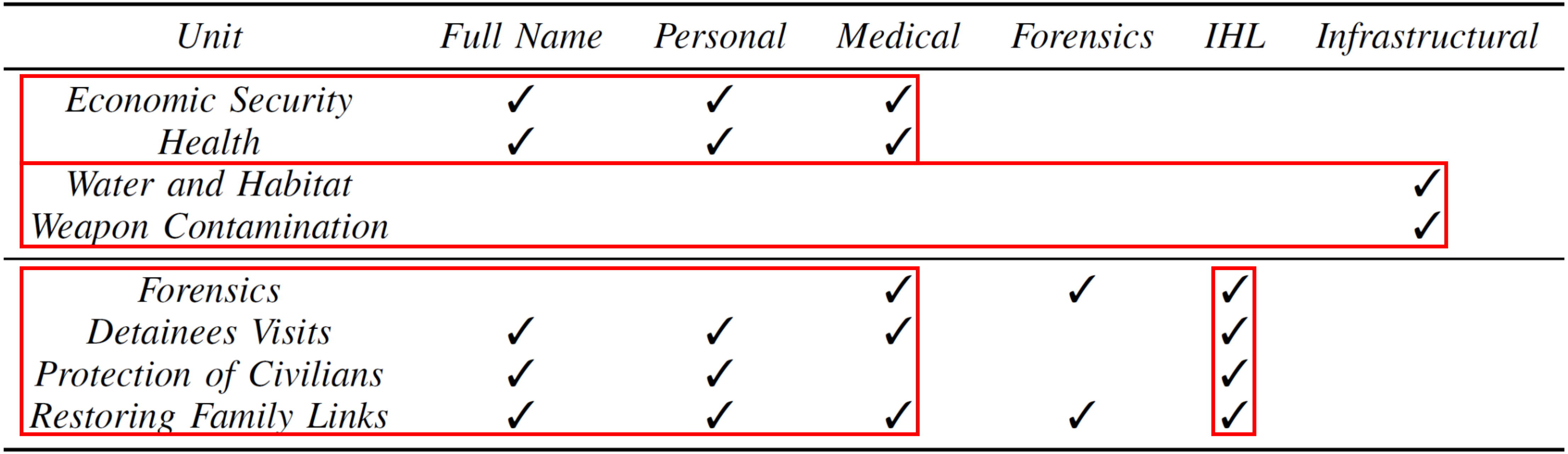
Outline

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

Outline

- The International Commitee of the Red Cross (ICRC)
- Methodology
- Results
  - Data collected
  - Data flows
  - Operational and legal factors
- Future work

Summary of collected data types by units



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	✓	✓	✓	✓	✓	

Sensitivity of Collected Data

Beneficiaries

ICRC

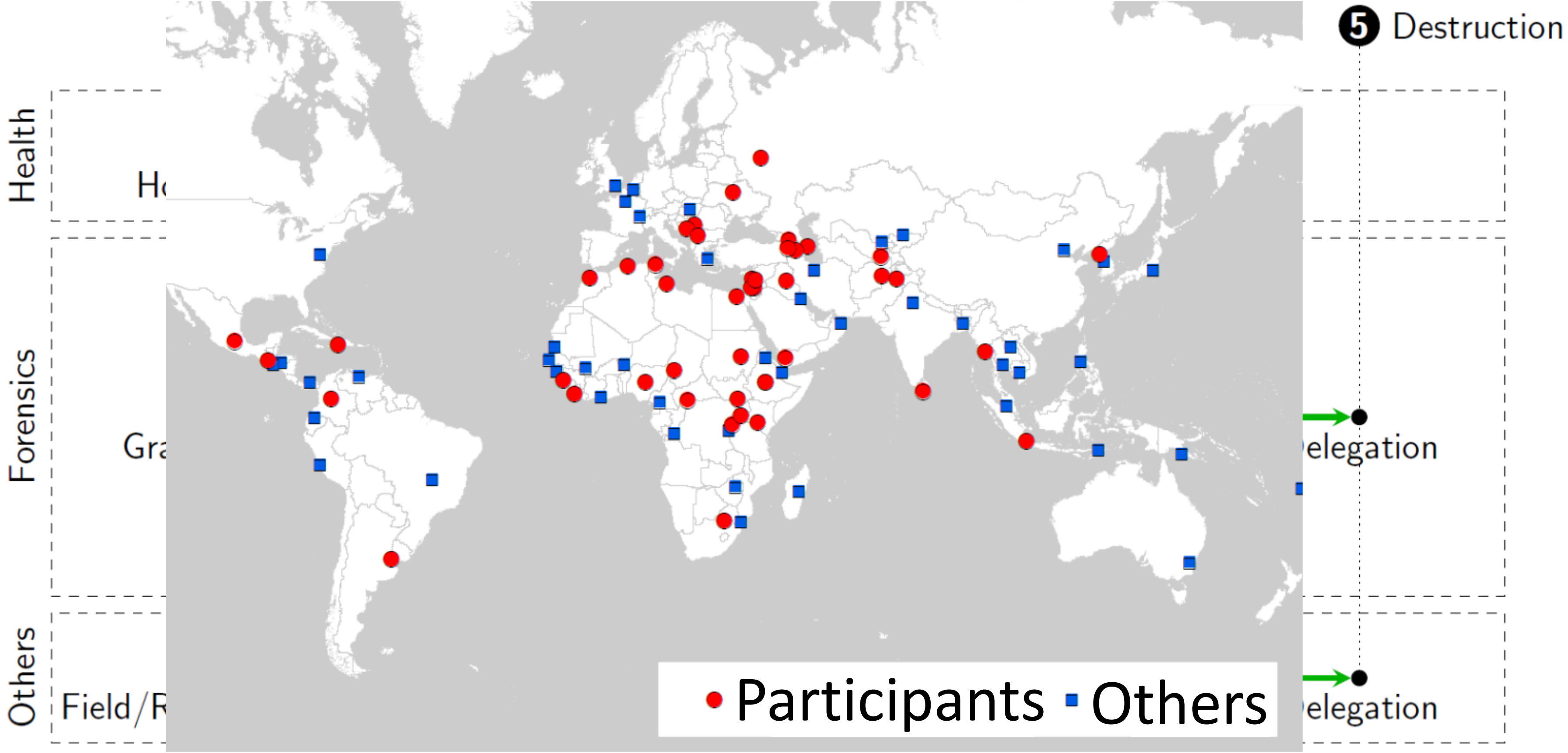
Organization

Governments

Outline

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

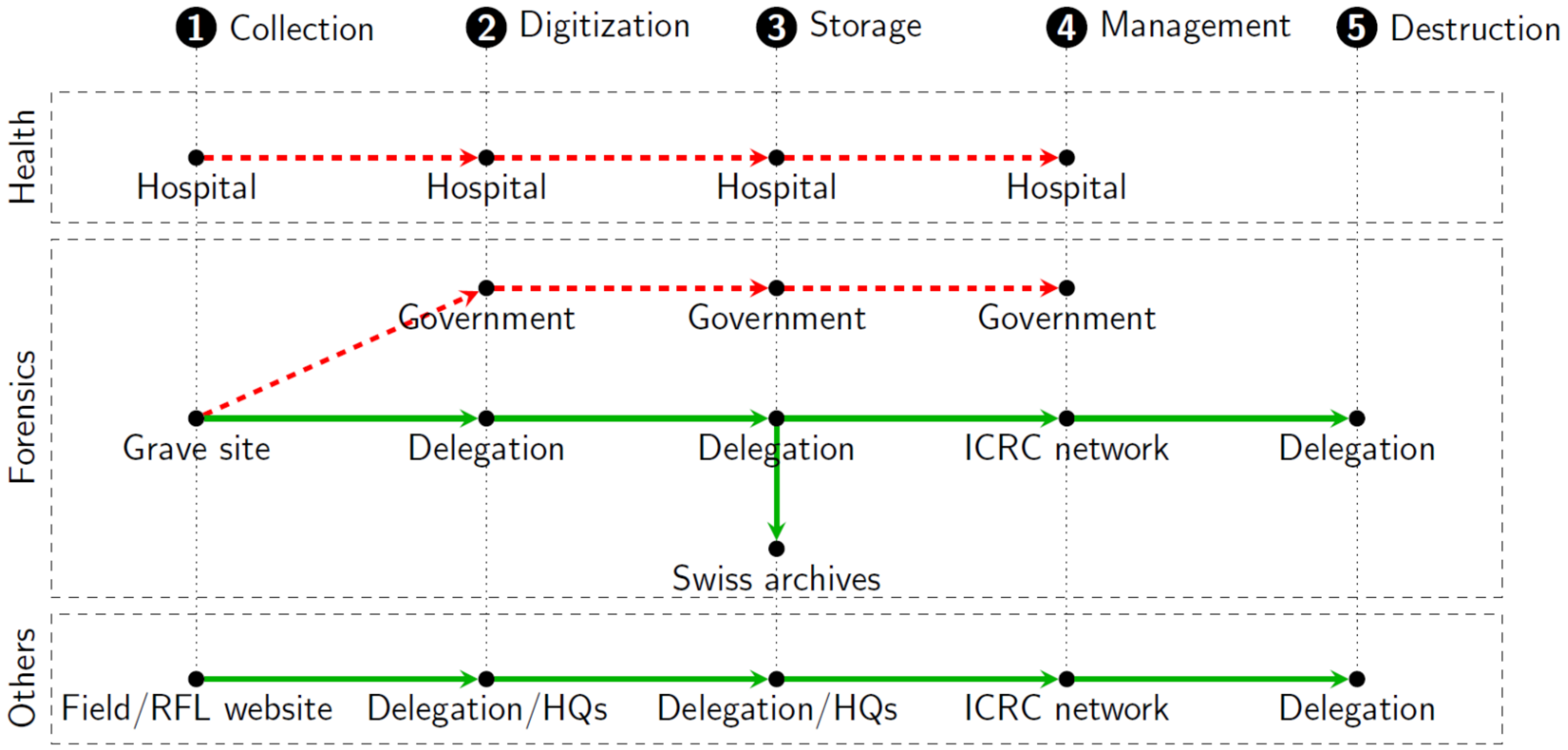
Overview of data flows



Outline

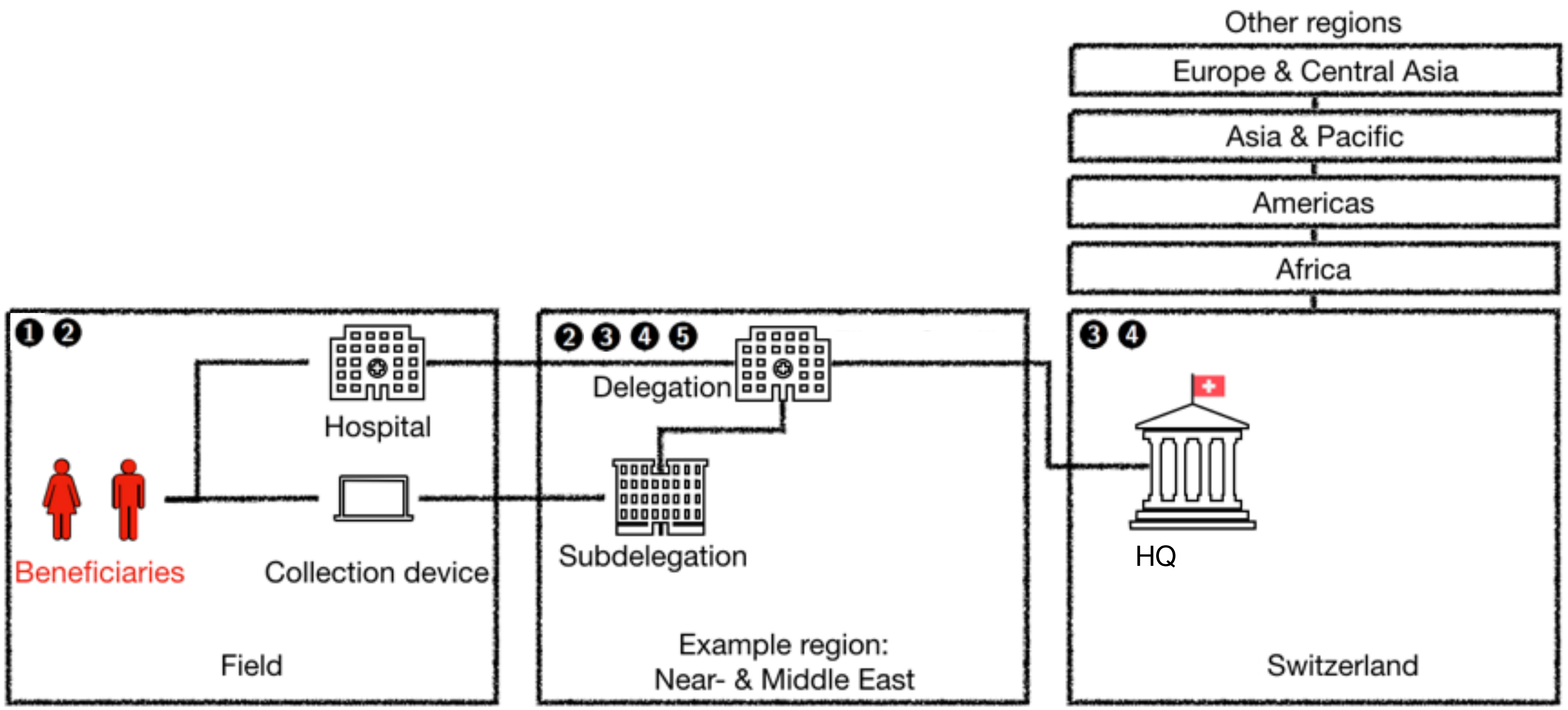
- The International Commitee of the Red Cross (ICRC)
- Methodology
- Results
  - Data collected
  - Data flows
  - Operational and legal factors
- Proposed architecture

Organizational structure



Practical factors

Vulnerability

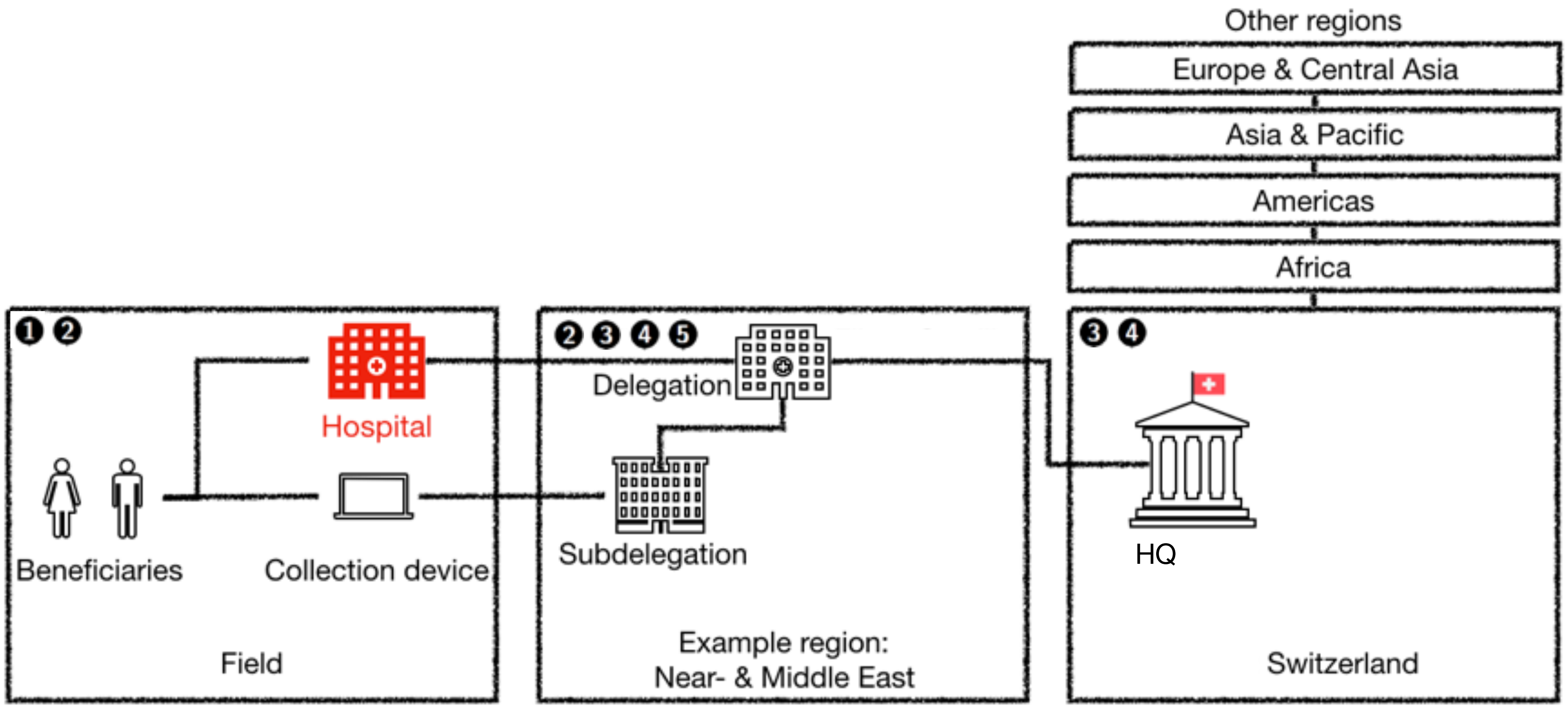


Practical factors

Vulnerability

Capacity building

Coercion



Other regions

Europe & Central Asia

Asia & Pacific

Americas

Africa

❶ ❷

Hospital

Beneficiaries

Collection device

Field

❷ ❸ ❹ ❺

Delegation

Subdelegation

Example region:
Near- & Middle East

❸ ❹

HQ

Switzerland

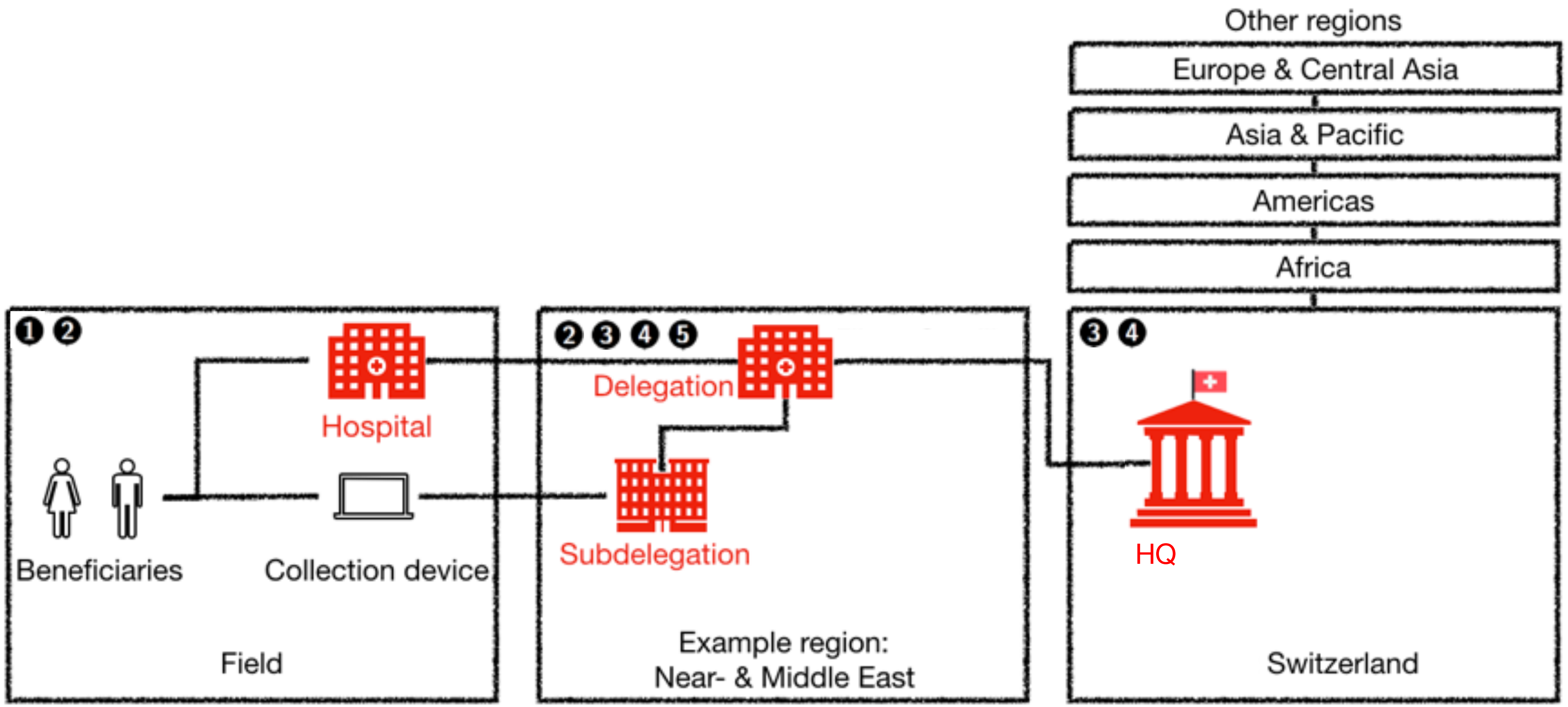
Practical factors

Vulnerability

Capacity building

Coercion

Physical attacks



Practical factors

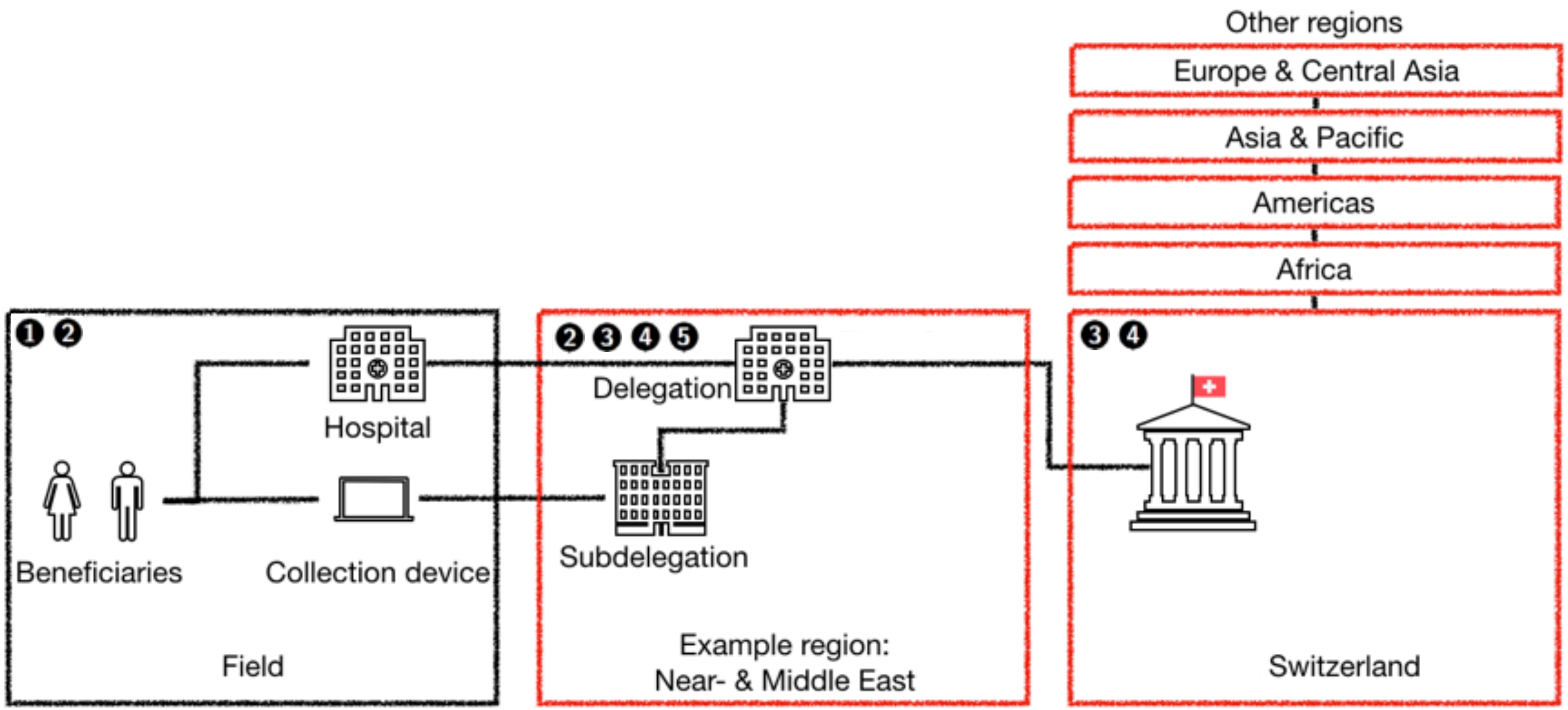
Vulnerability

Capacity building

Coercion

Physical attacks

Legal factors



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).

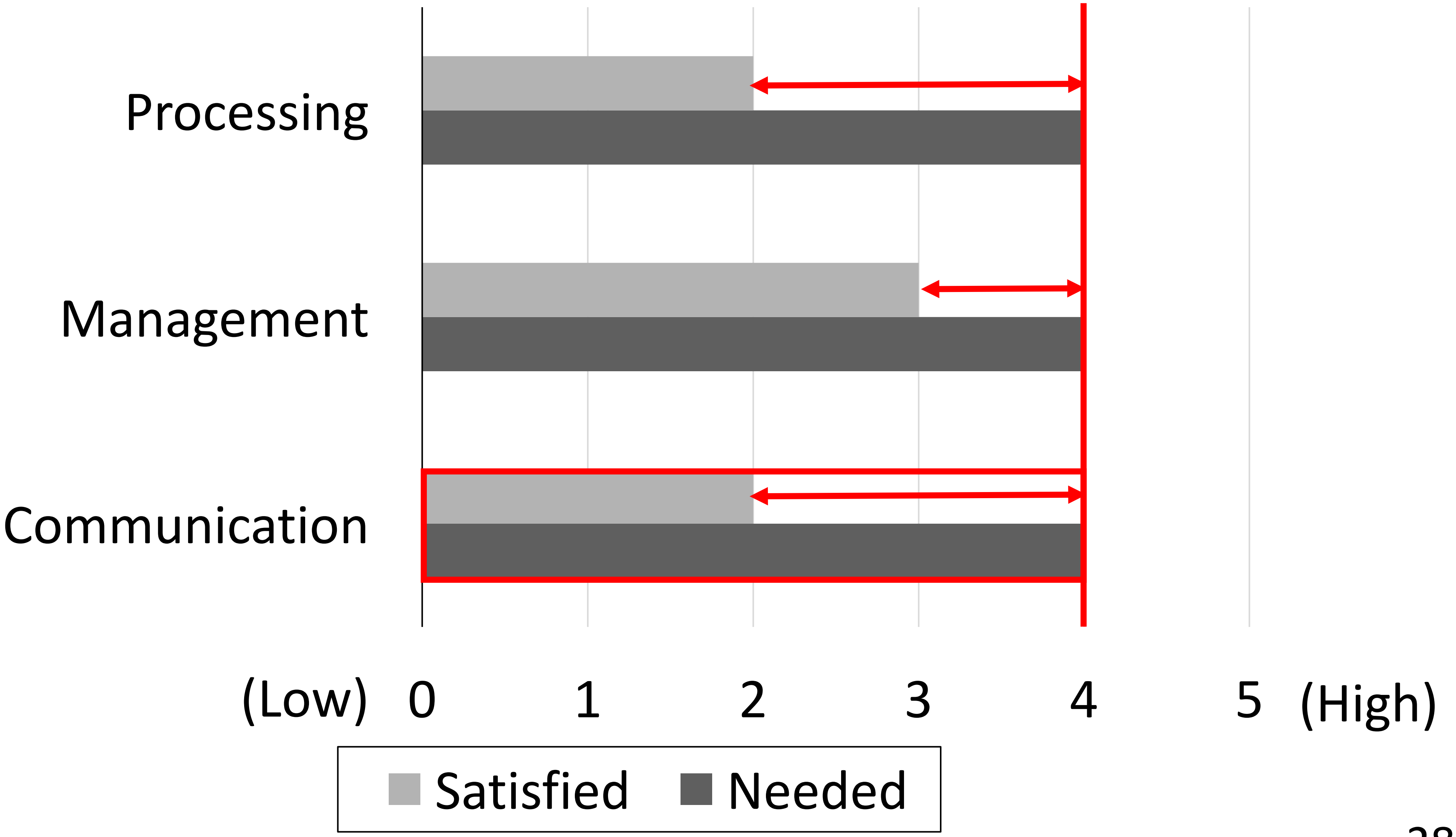
   - Data protection can hamper humanitarian action; in particular, jurisdictions with conflicting legislations can preclude data sharing.

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 Commitee of the Red Cross (ICRC)
- Methodology
- Results
  - Data collected
  - Data flows
  - Operational and legal factors
- Proposed architecture

Needs of ICRC staff



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

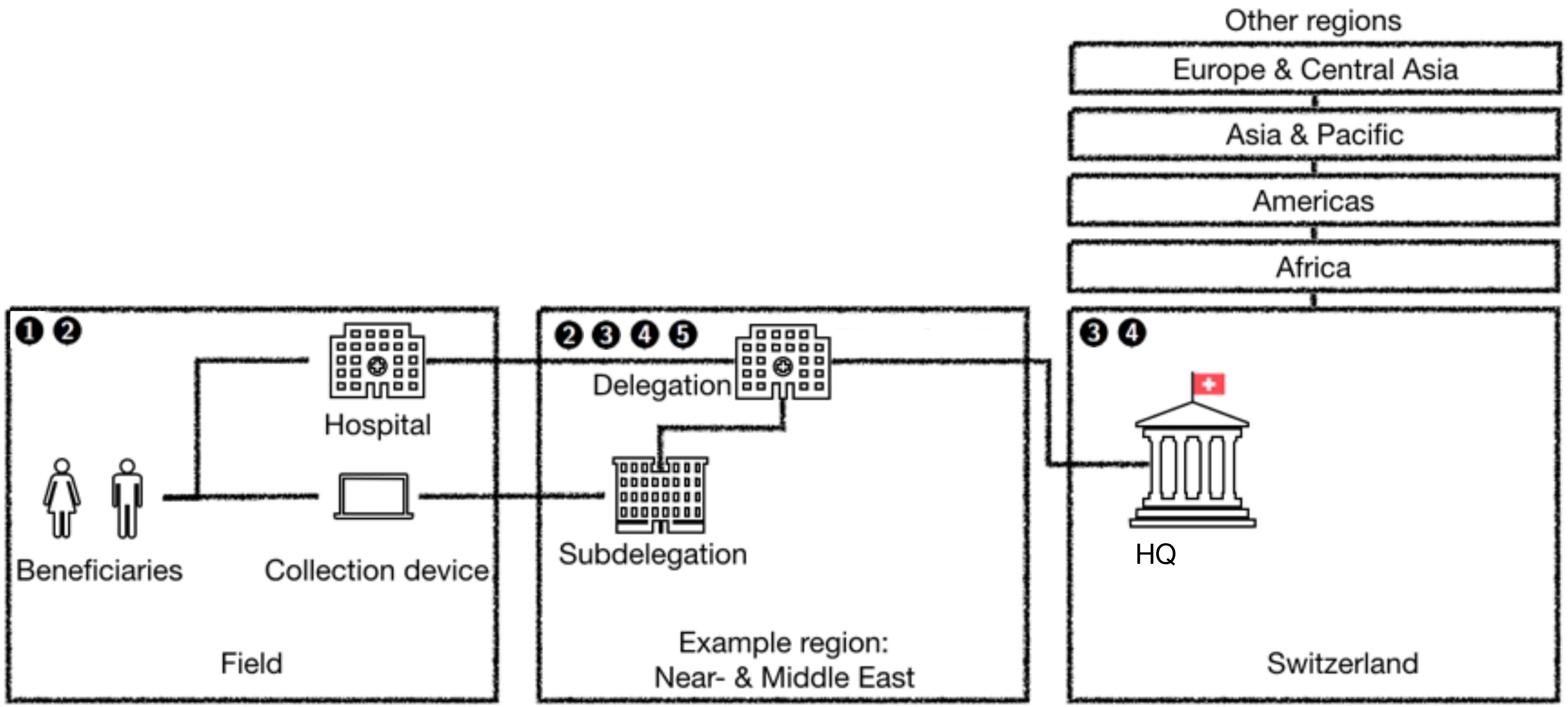
Vulnerability

Capacity building

Coercion

Physical attacks

Legal factors



Proposed architecture

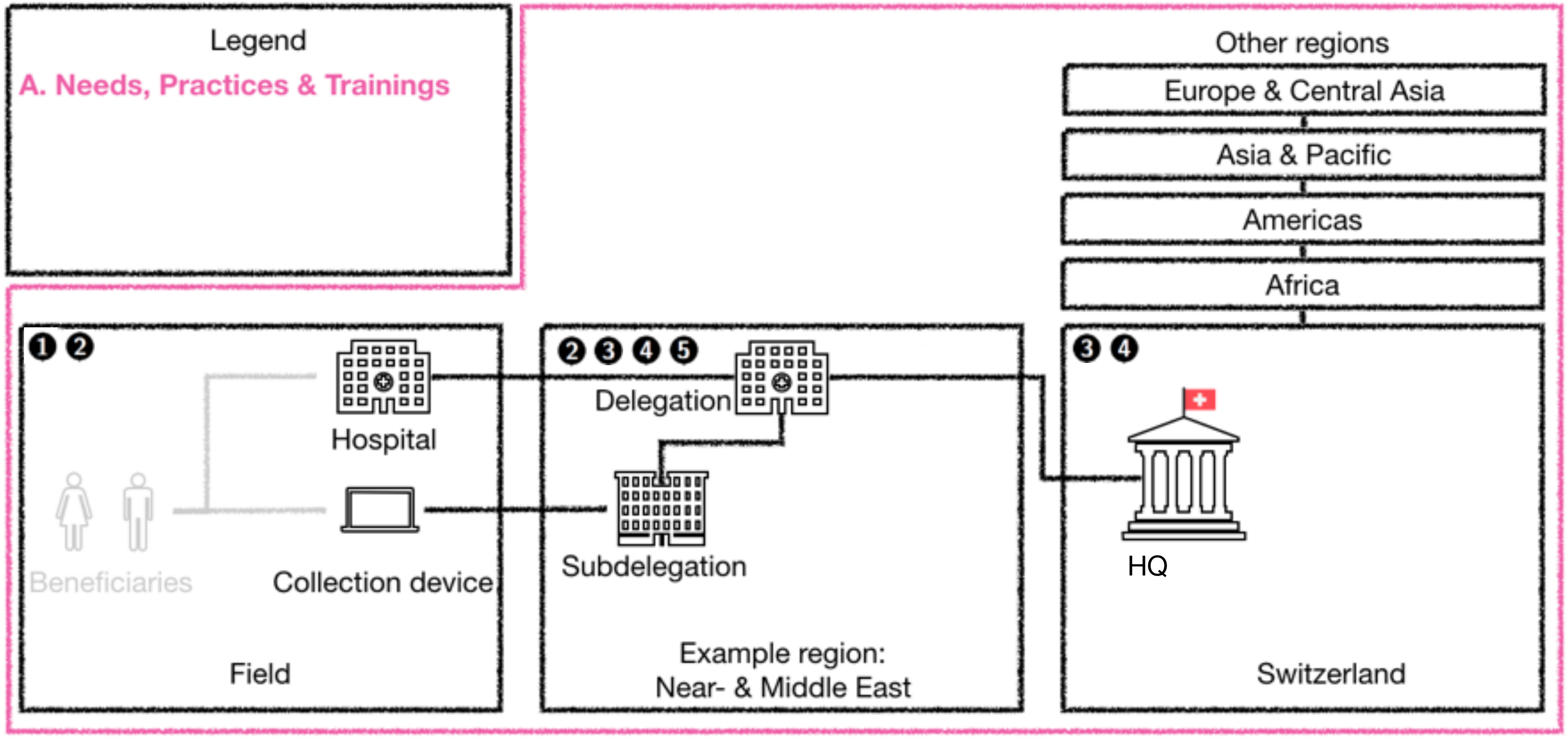
Vulnerability

Capacity building

Coercion

Physical attacks

Legal factors



Proposed architecture

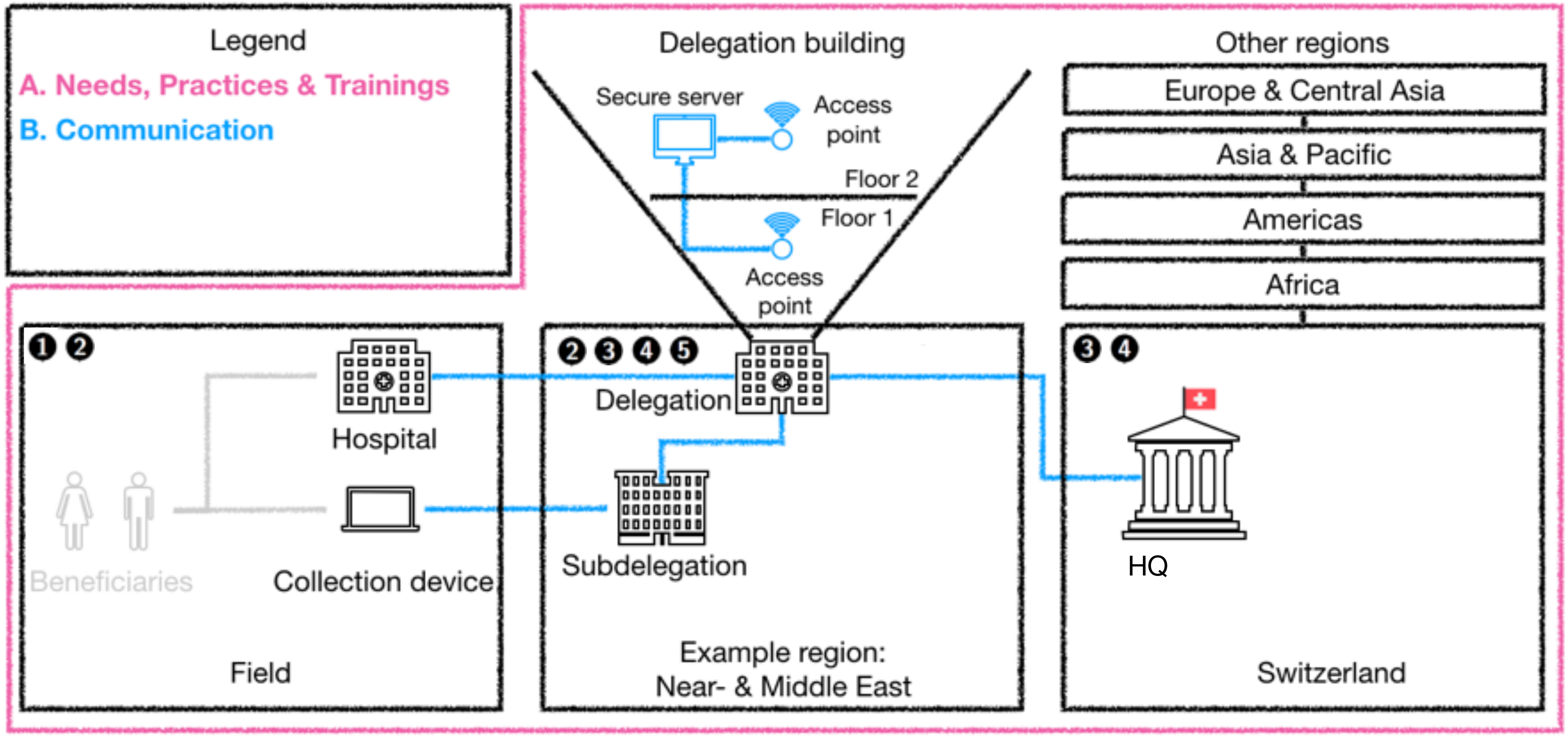
Vulnerability

Capacity building

Coercion

Physical attacks

Legal factors



Proposed architecture

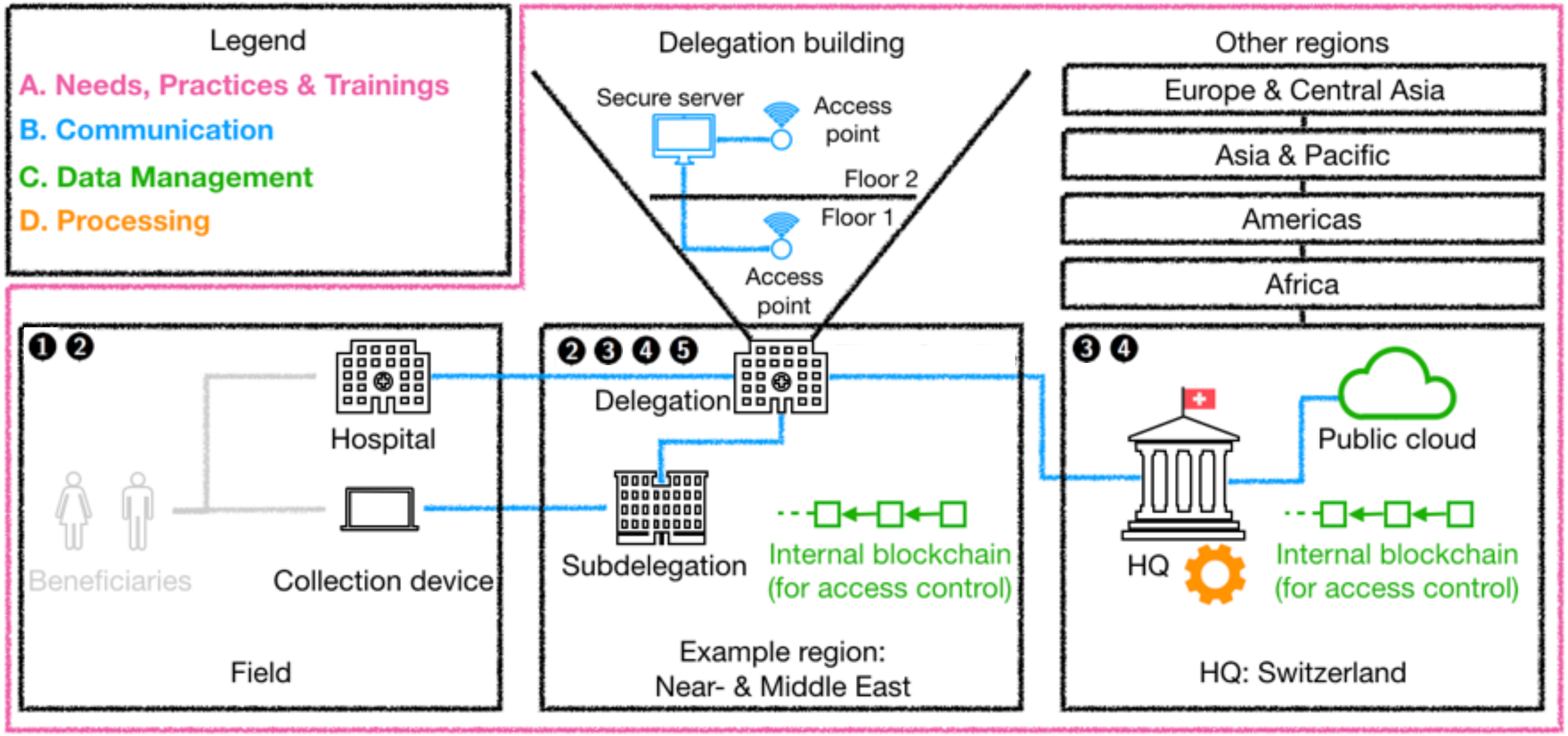
Vulnerability

Capacity building

Coercion

Physical attacks

Legal factors

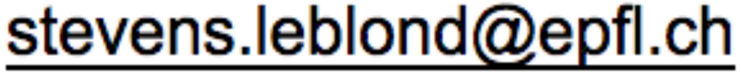


Take home messages

- 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 bi-lateral 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