



DUBLIN

IRELAND

34th ANNUAL FIRST CONFERENCE
JUNE 26 - JULY 1

2022

#FIRSTCON22

Cybersecurity maturity in the Pacific Islands | Integrating CERT services in a regional framework

Anthony Adams (Monash University, Australia)

Tony Adams

PhD Candidate

Department of Software Systems and Cybersecurity,
Faculty of Information Technology

Monash University

Melbourne, Australia

anthony.adams@monash.edu.au

Twitter [@tony_adams1969](https://twitter.com/tony_adams1969)

LinkedIn <https://www.linkedin.com/in/tonyadams1>

Phone +614 0786 3600 (WhatsApp, Signal)



Contents

The Problem

Pacific Islands region

Research Scope

Conceptual Model (Initial)

Study One

Conceptual Model (Updated)

Implementation Approach

The Problem

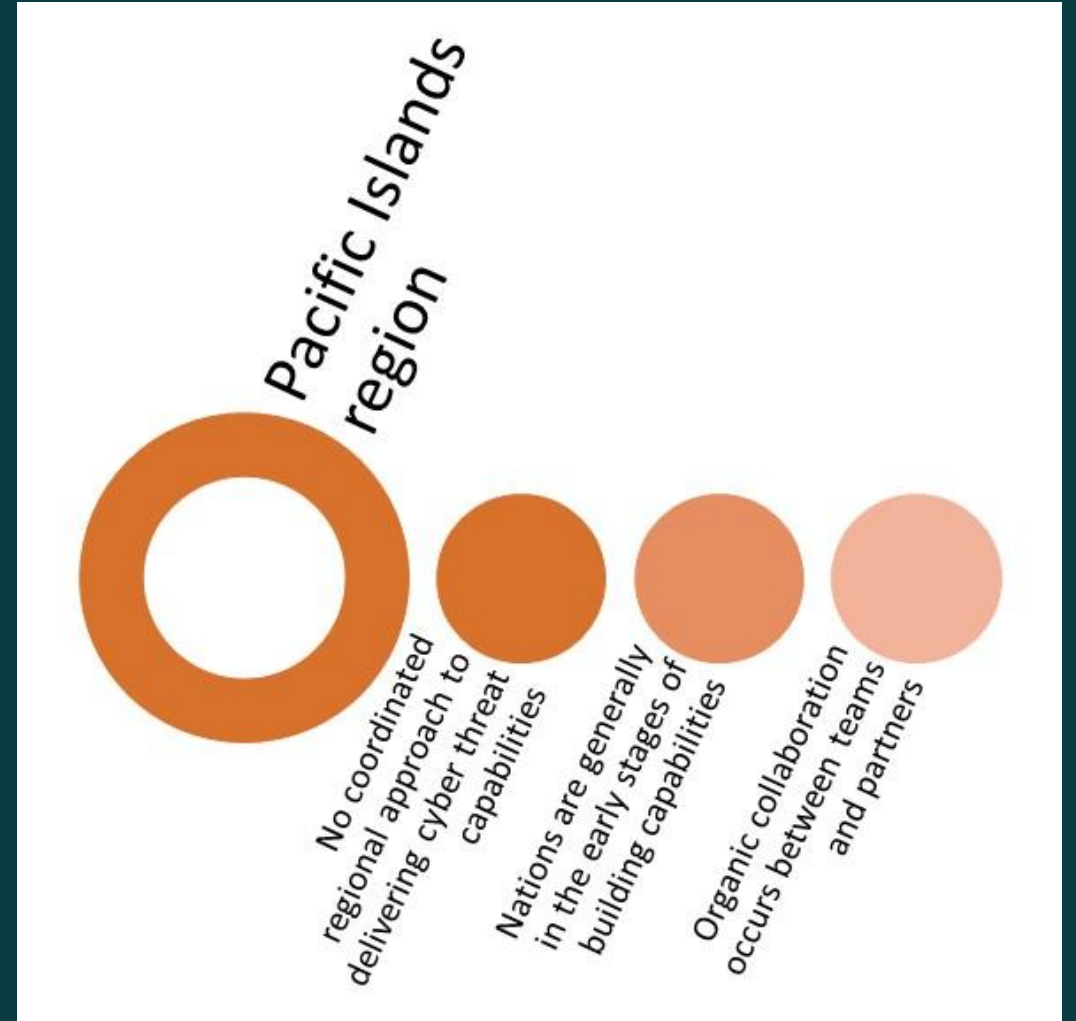
What is the Problem to be addressed?

Who is impacted?

Why should it be addressed?

How does this research contribute to a solution?

What is the problem to be addressed?

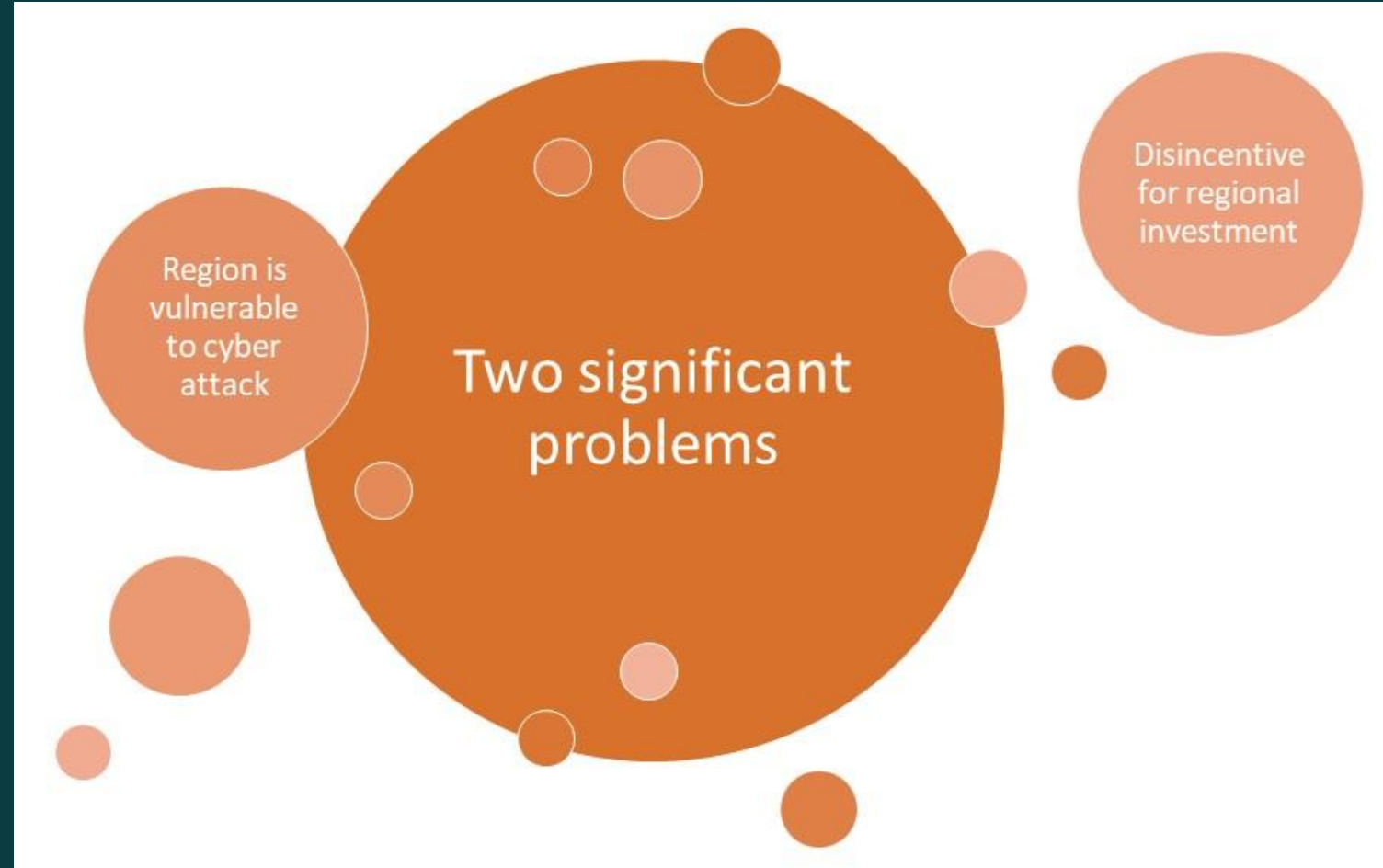


Pacific Island nations do not use a coordinated regional approach to manage their cybersecurity threat responses.

Who is impacted?

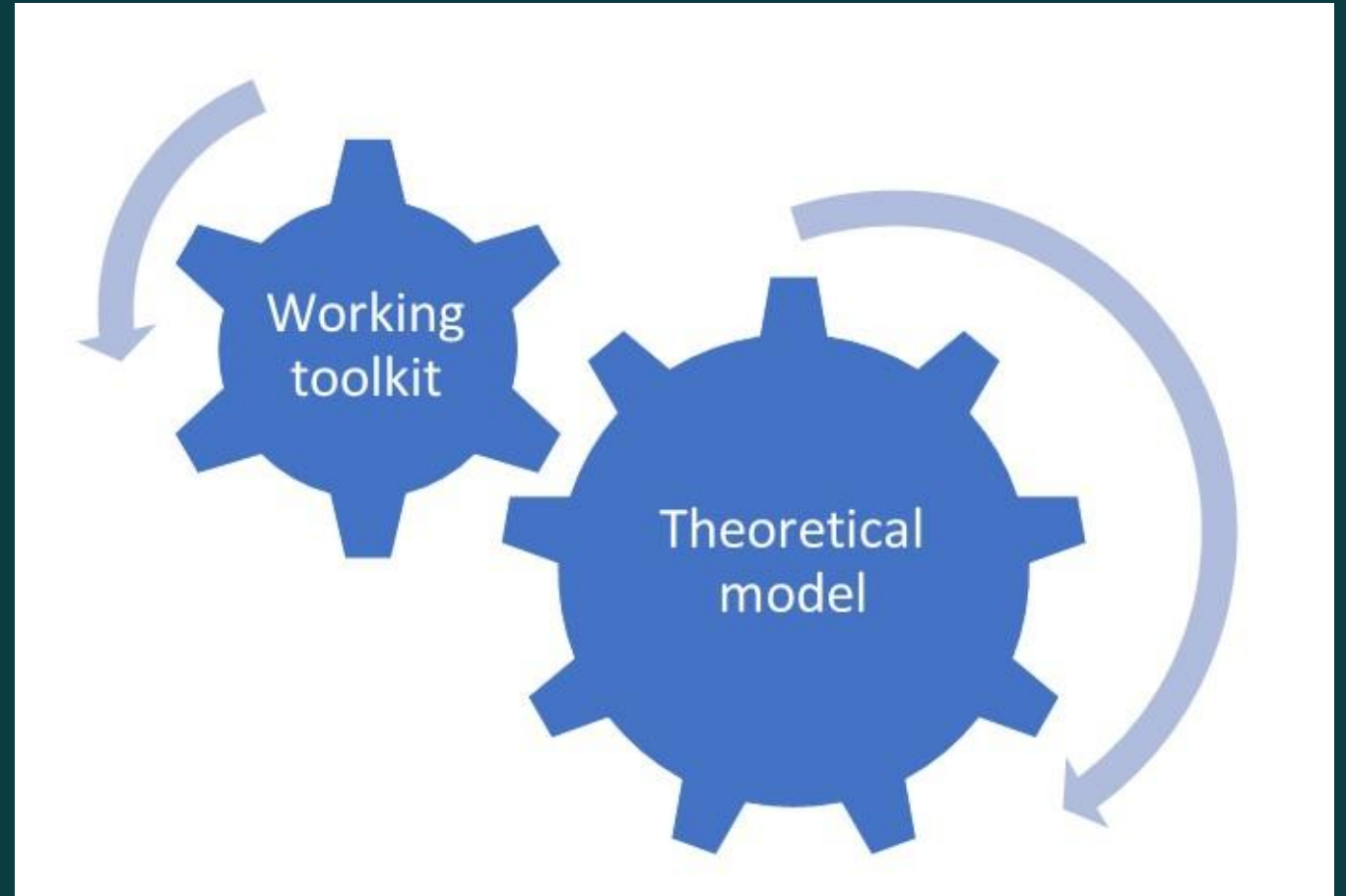


Why should it be addressed?



The lack of regional CERT framework creates two significant problems for the Pacific Islands region.

How does this research contribute to a solution?

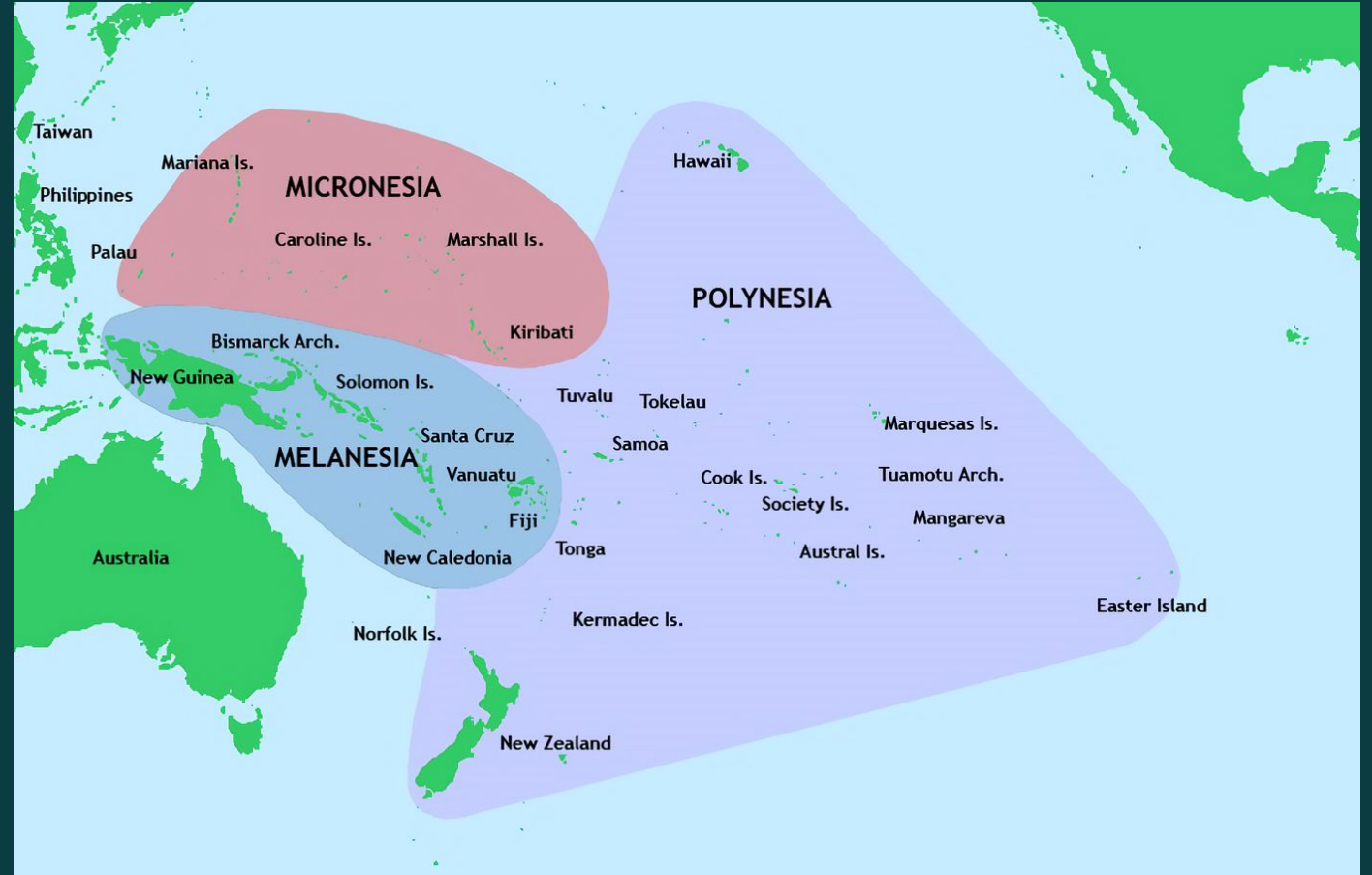


Two key contributions to our understanding of how national CERT services can be delivered in the Pacific Islands region

Pacific Islands region

18 member nations of the Pacific Islands Forum

3 ethnic and cultural sub-regions (excluding Australia)



Research Scope

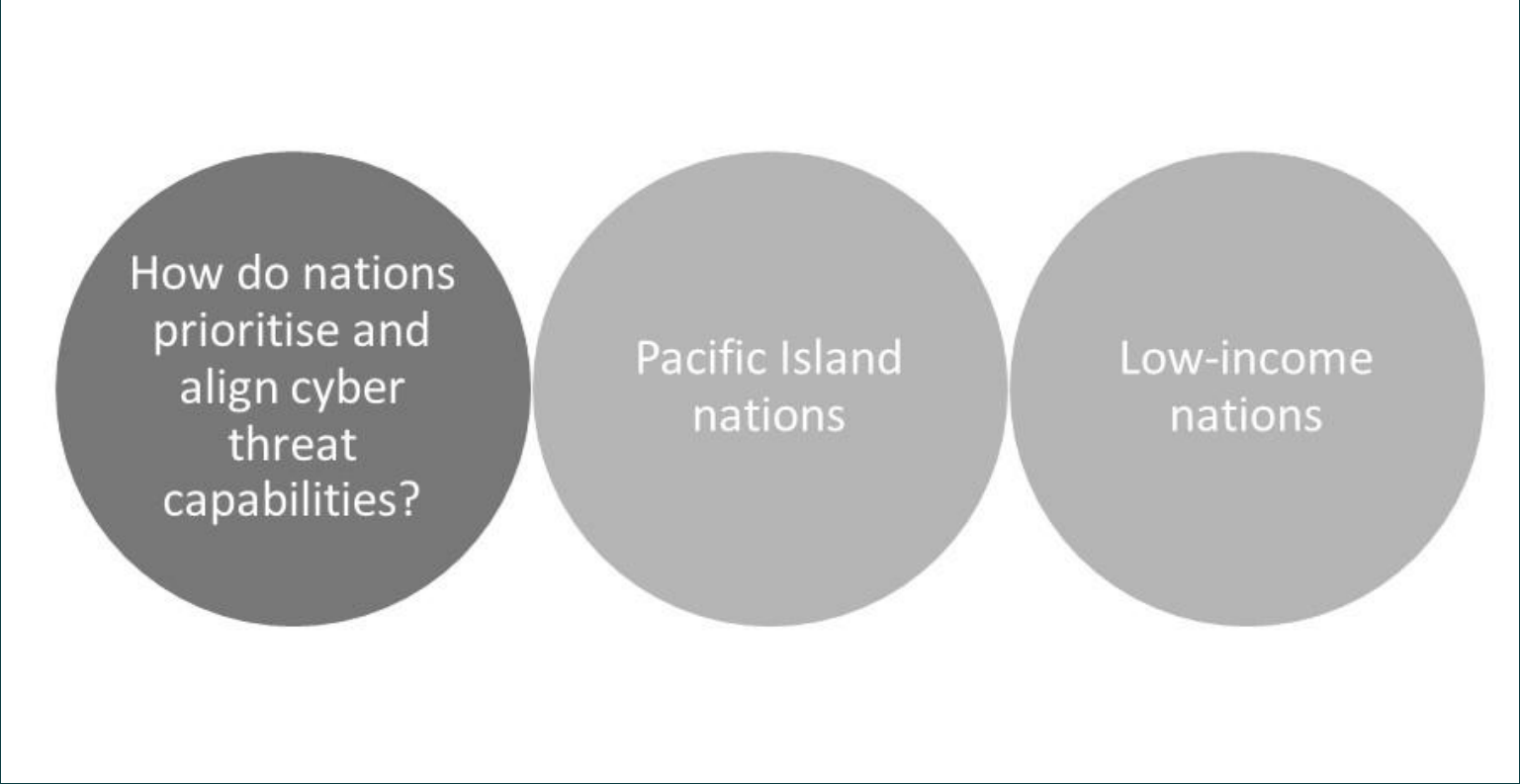
Research Aim

Research Questions

Research Objectives

Research Aims

Understand how nations prioritize and align cyber threat capabilities, within a multi-stakeholder regional CERT framework




How do nations prioritise and align cyber threat capabilities?

Pacific Island nations

Low-income nations

Research Questions



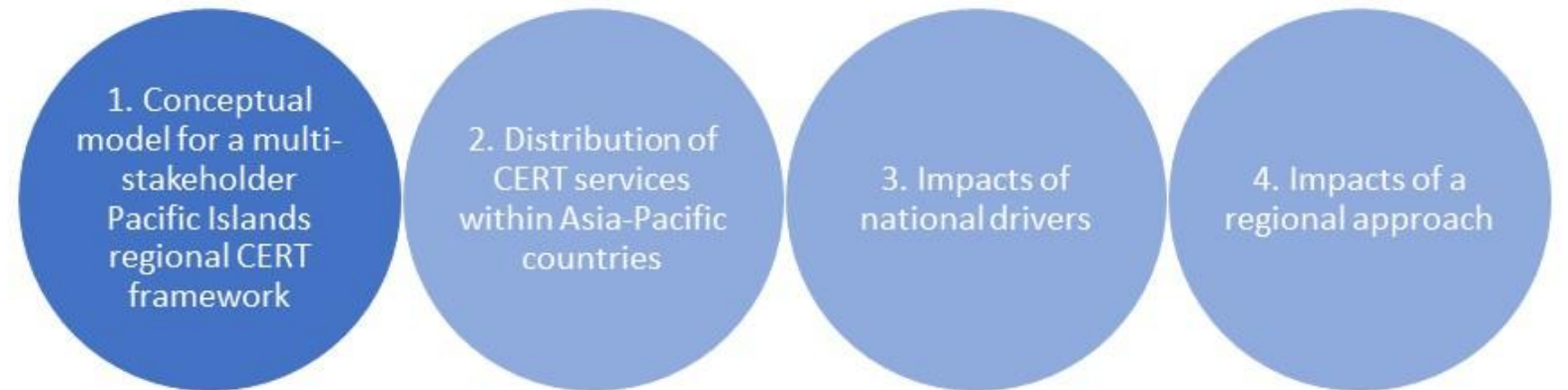
1. How do Pacific Island national CERTs select cybersecurity threat response capabilities, within a regional framework?

2. How are these choices impacted by national drivers?

3. How are these choices impacted by regional approaches?

To meet these aims, this research addresses three questions.

Research Objectives



To address these questions, the research has four objectives

Conceptual Model (Initial)

Conceptual Foundation

Initial Conceptual Model

Theoretical Framework (CHAT)

Updated Conceptual Model

Conceptual Foundation



The foundation for a regional CERT model has three pillars (Adams, 2020)

Conceptual Foundation

The foundation is enacted by four action-based drivers (Adams, 2020)



Initial Conceptual Model

The initial Conceptual Model is built on the Conceptual Foundation.

It contains three key themes.

Global | Centralised CERT capability

- International behavioural norms
- Regional cooperation
- Institutional frameworks

Regional | Regional Framework

- Integration with regional bodies
- Decision making
- Remediation approach

National | National Drivers

- Architecture
- Internal governance
- Critical infrastructure
- Capability maturity

Initial Conceptual Model

The three themes are linked by enablers.

National Governance

- Determines how a national government will choose to engage with a global “best practice” approach to CERT delivery

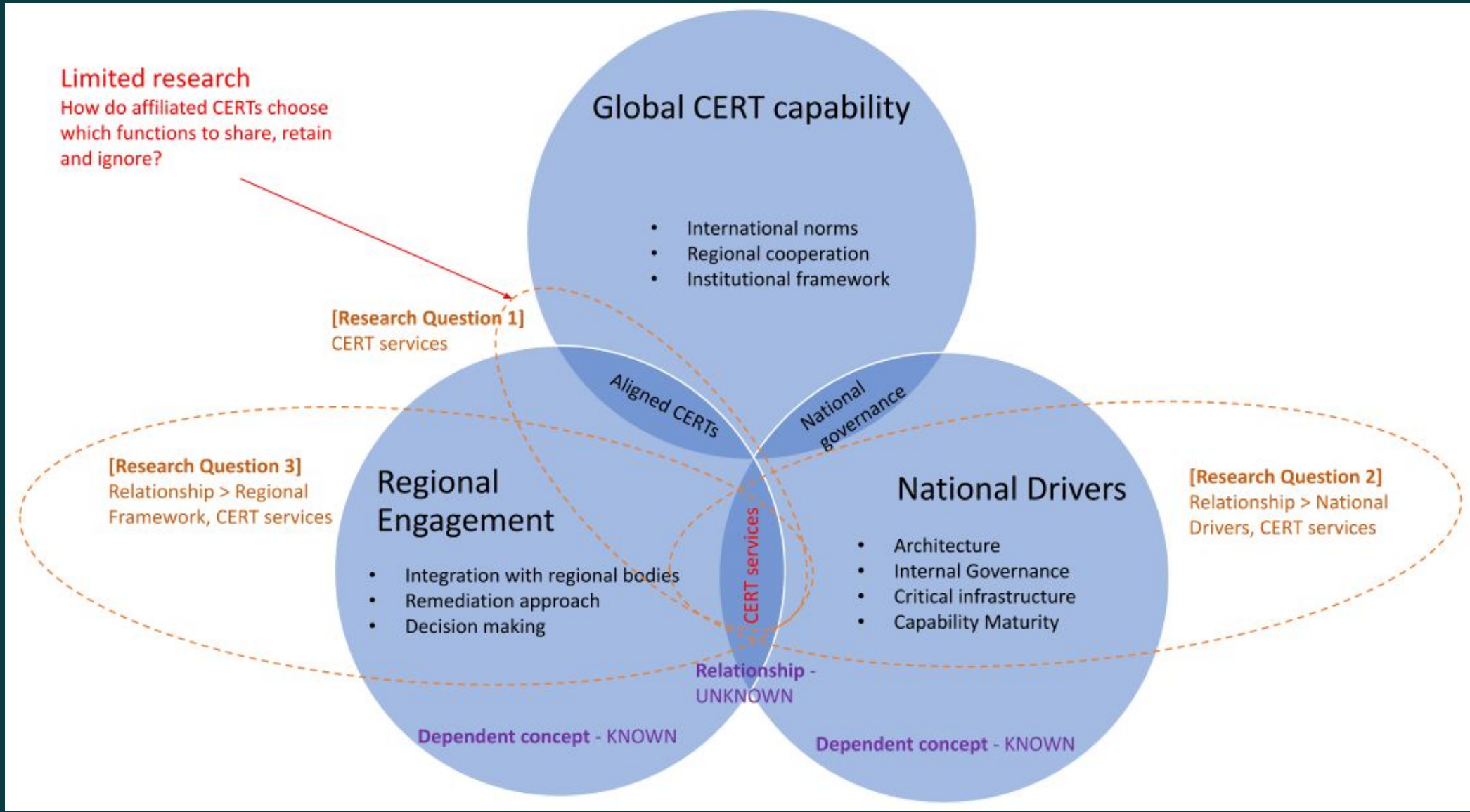
CERT services

- Connects the national government’s policy approach and priorities with a regional community

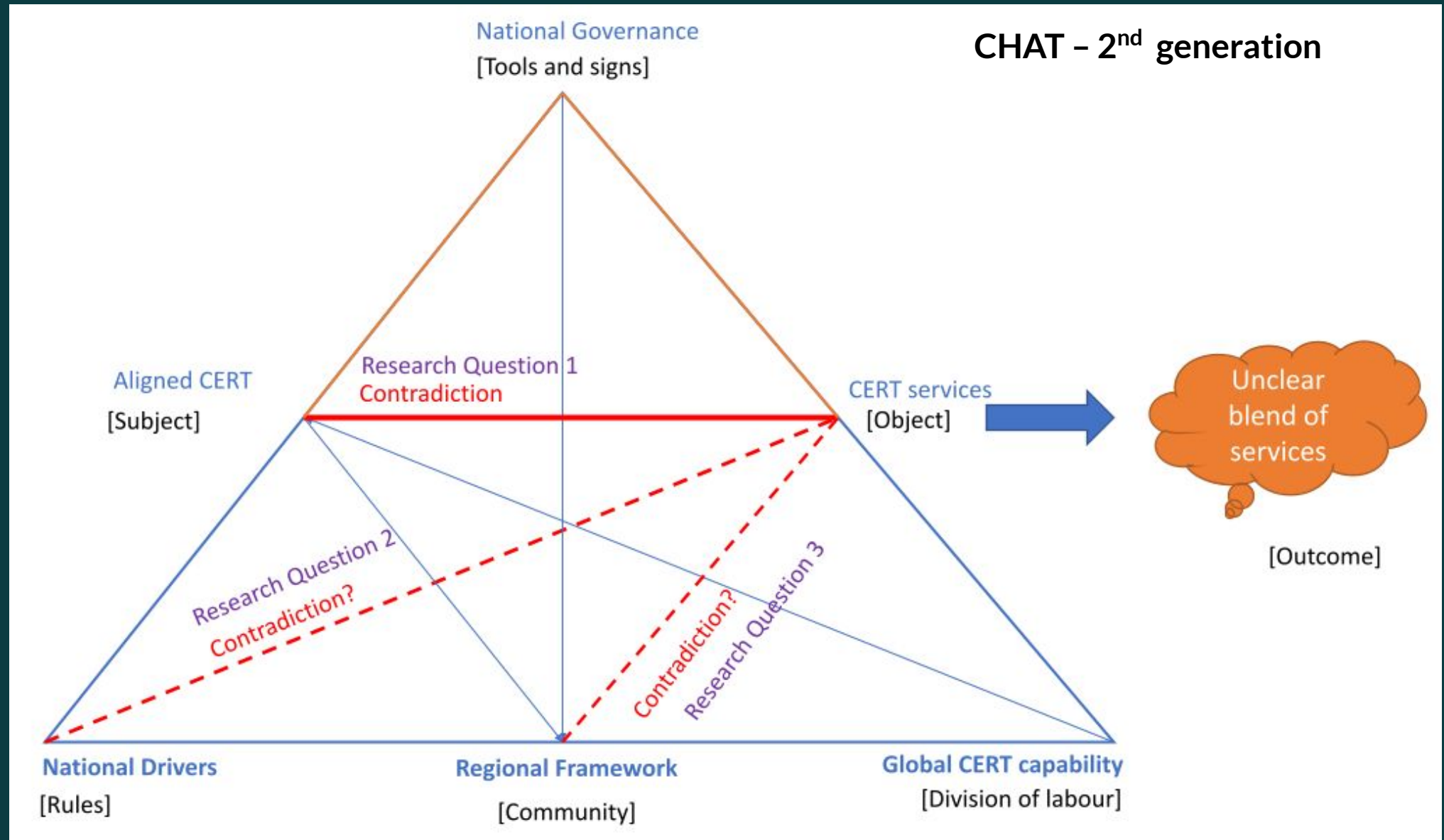
Aligned CERTs

- National CERTs present their interests through a regional framework, using global institutions and practices

Initial Conceptual Model

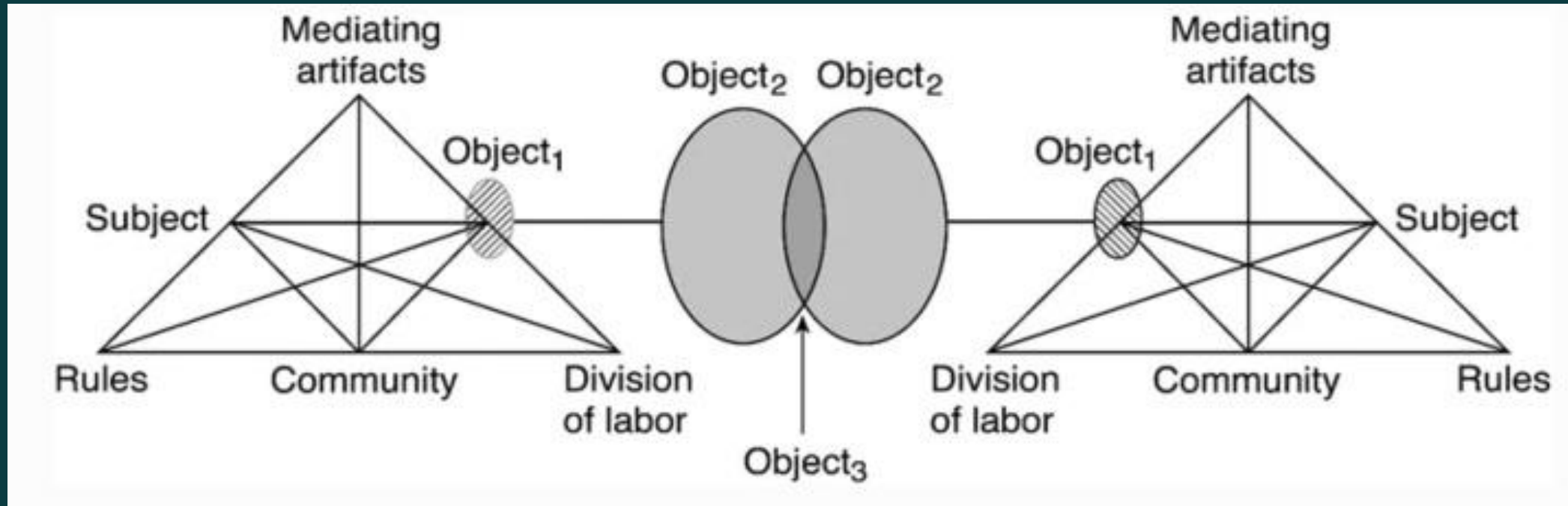


Theoretical Framework



Theoretical Framework

CHAT - 3rd generation



Object 1 – the services that a national CERT will provide

Object 2 – the individual interests of a national CERT, reflected in a regional CERT

Object 3 – the shared interests of different participants, reflected in a regional CERT

Study One

Study One

10 participants

Partners

Australia
Switzerland
Lithuania
Bosnia
APNIC

CERT

USA – commercial
USA – CERT/CC
New Zealand
Kiribati
Malaysia

CERT

Samoa
Tonga

Goals

To set the scene.

To understand the current distribution of CERT services and capabilities in the Asia-Pacific region

Nov 2021 – Mar 2022

Key Services

Threat Detection
Incident Response
Forensic Analysis
Advisories
Community awareness

Key Themes

Trust as an enabler of success
People, not technology
National CERTs – their role in raising community awareness
National CERTs – support national priorities, areas of shared regional interest
Partners – promoting increased national cyber resilience

Conceptual Model (Updated)

Updated Conceptual Model

Study One highlights key elements
of the Conceptual Model

Themes

Global | CERT capability

- International behavioural norms

Regional | Regional Framework

- Integration with regional bodies

National | National Drivers

- Capability maturity

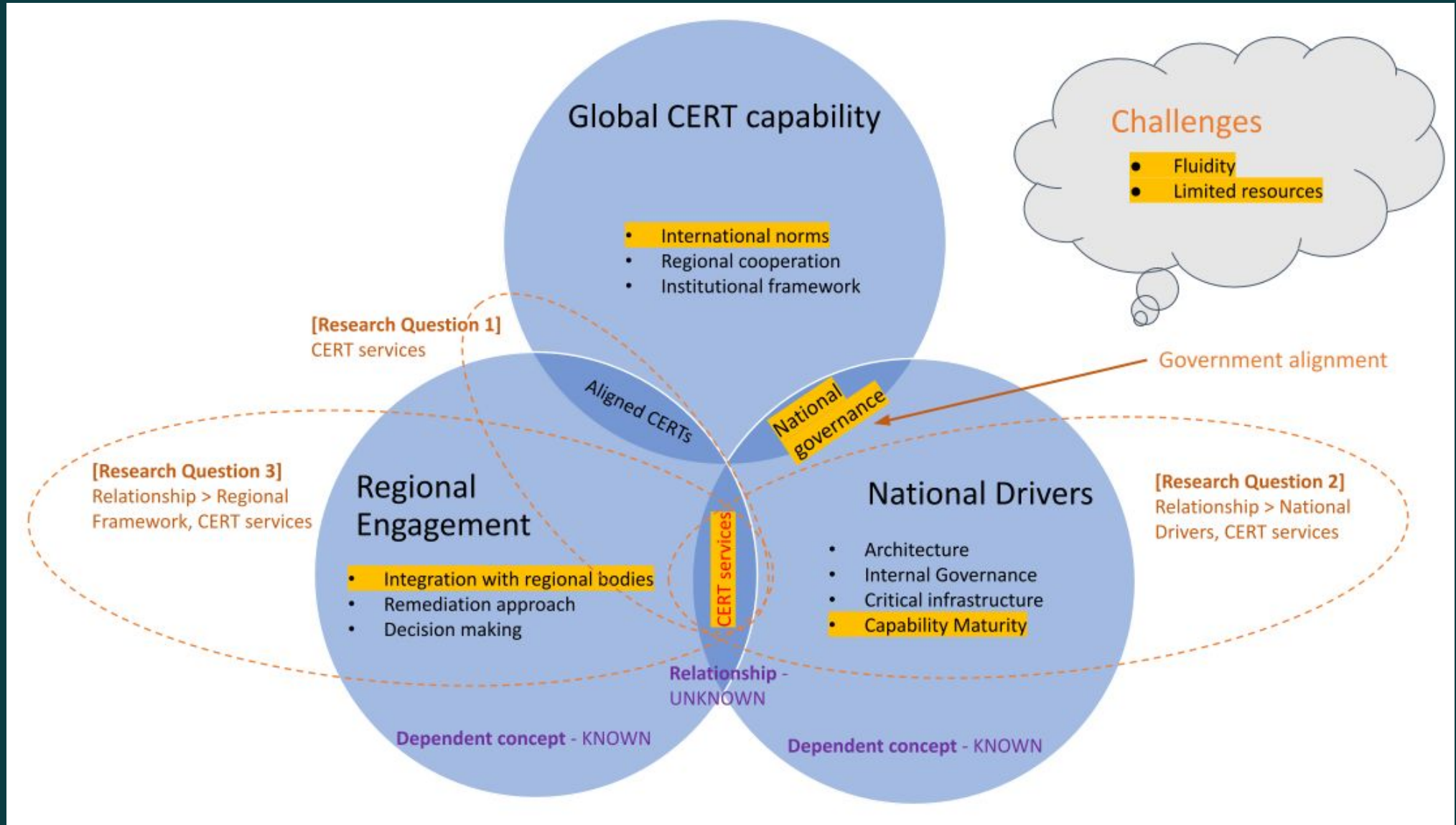
Enablers

- National Governance
- CERT services

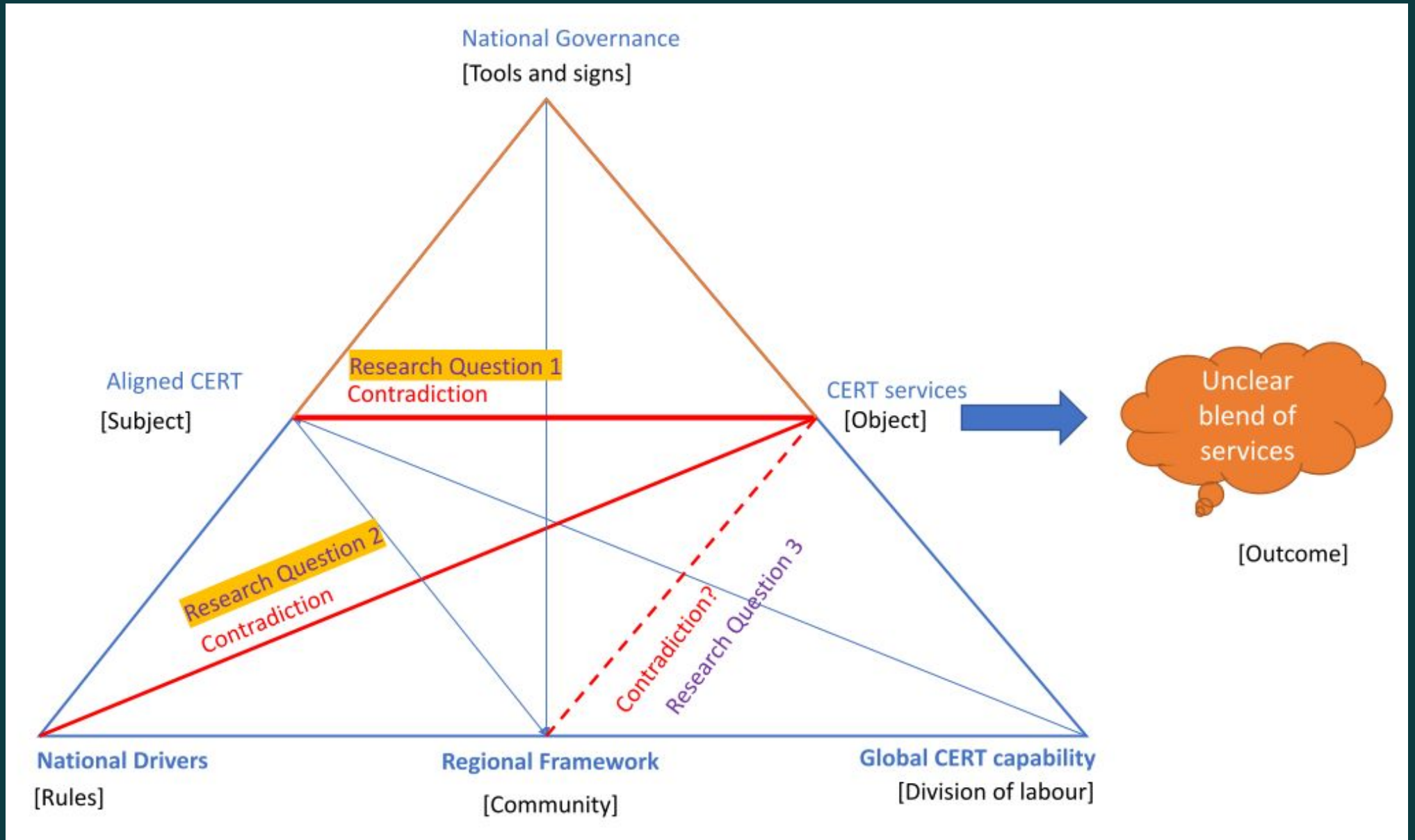
Challenges

- Fluidity, lack of resources

Updated Conceptual Model

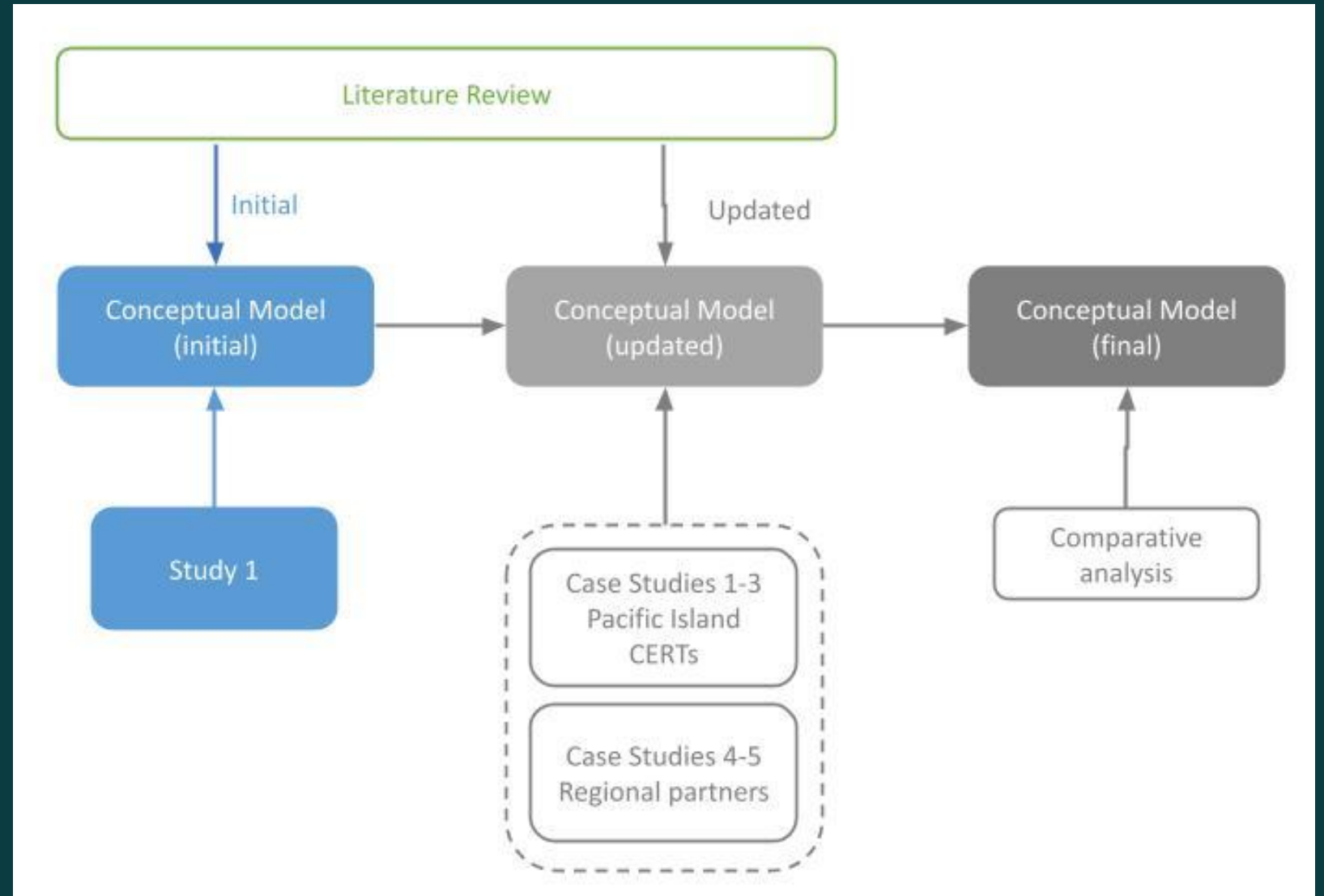


Updated Conceptual Model

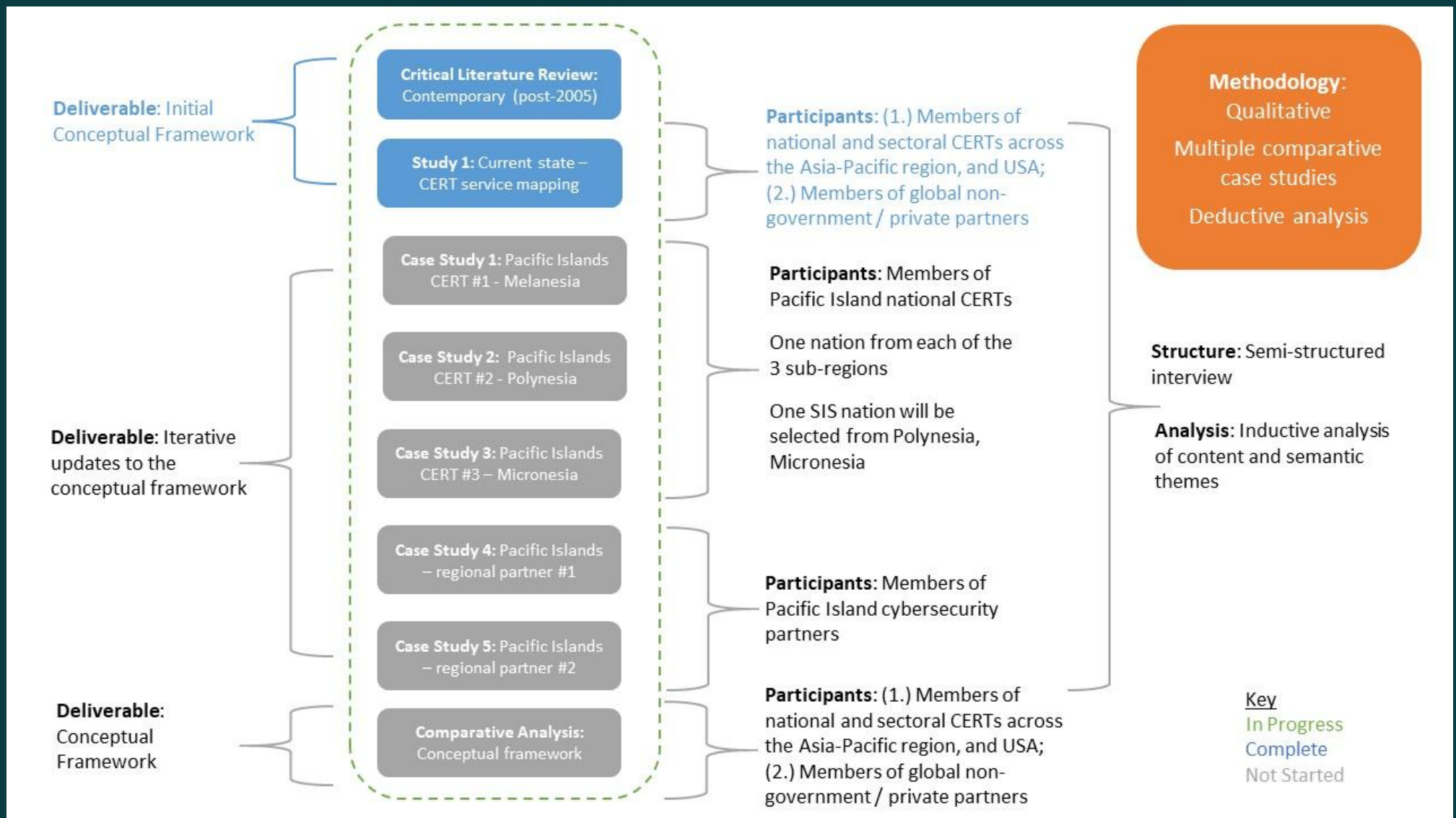


Implementation Approach

Implementation Approach



Implementation Approach



Tony Adams

PhD Candidate

Department of Software Systems and Cybersecurity,
Faculty of Information Technology

Monash University

Melbourne, Australia

anthony.adams@monash.edu.au

Twitter [@tony_adams1969](https://twitter.com/tony_adams1969)

LinkedIn <https://www.linkedin.com/in/tonyadams1>

Phone +614 0786 3600 (WhatsApp, Signal)

