

# e-Resilience in support of Emergency Communication: “best-practices”

3rd Session of the Asia Pacific Information Superhighway (AP-IS) Steering Committee and  
WSIS regional review

26-29 August 2018

United Nations Conference Center, Bangkok, Thailand

Nuwan Waidyanatha

Senior Research Fellow

[nuwan@lirneasia.net](mailto:nuwan@lirneasia.net)



# Emergency Communication



## 1. Reporting (indecent/relief)

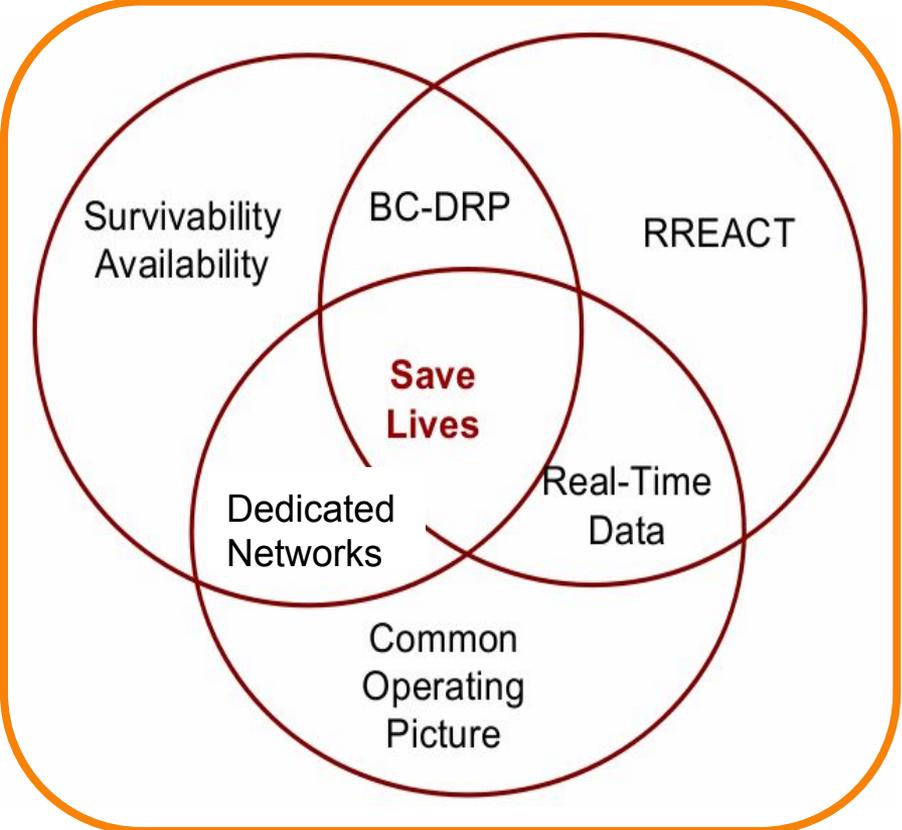
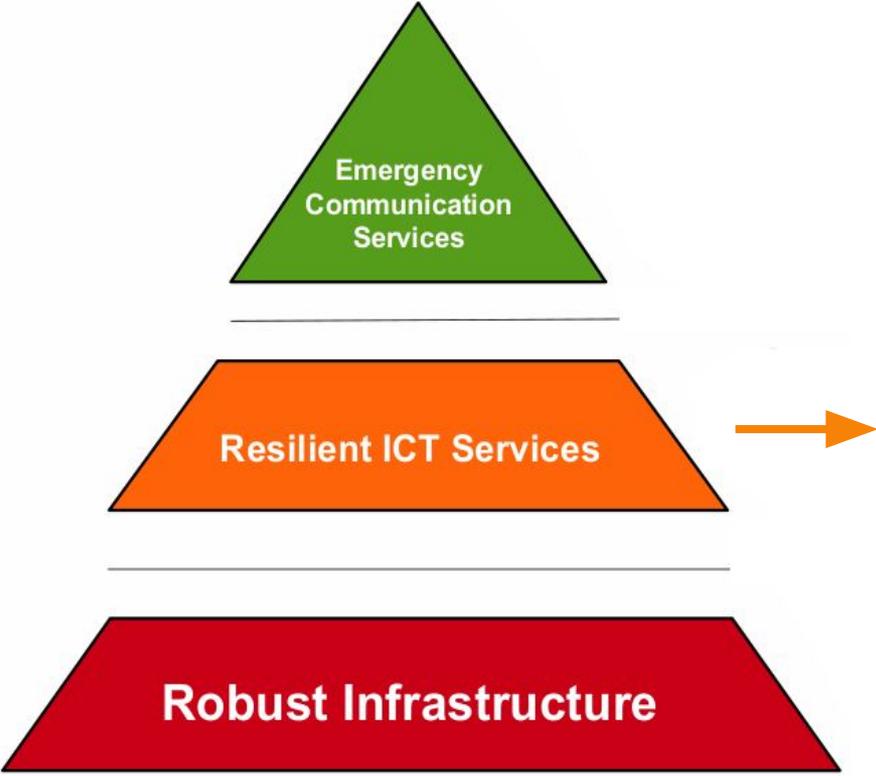
Person asking for help from the Emergency Management Services indicating hazard (threat) and immediate needs

## Emergency Management Services

## 2. Alerting / Warning

Emergency Management Center Warning the Public in the area indicating hazard and required response actions

# Emergency Communication Resilience Enablers

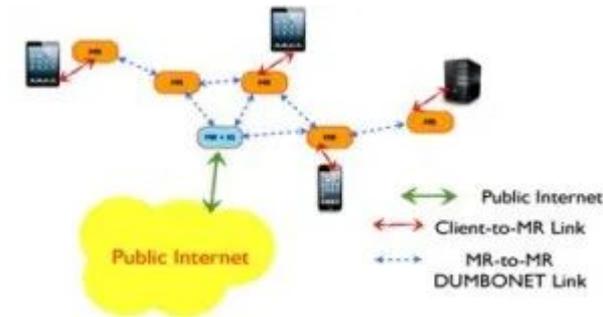
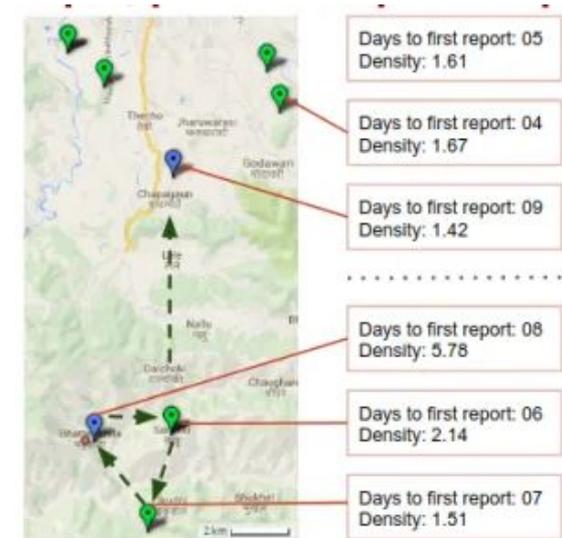


# 2nd AP-IS Steering Committee Meeting - recapitulation

1. [Report](#) - 2015 Gorkha earthquake - evaluation of Nepal's emergency communication systems
2. Introducing BC-DRP objectives with preparedness (securing ICT business continuity) and response (rapid restoration of access to telecommunications)
3. Offer tools to diagnose (survivability, availability, & BCP readiness) and remediate (strategies to build back better)

Resources:

<https://lirneasia.net/2018/09/unescap-apis-emcomm>



# Evaluation of UN-ESCAP's e-Resilience Toolkit

1. Toolkit does address “ICTs as enablers of community resilience”; i.e. ICT4D definition of E-Resilience
2. Does not provide an E-Resilience toolkit for diagnosis and remediation; basis for bouncing forward, in the wake of shocks
3. There is a need for a toolkit that specifically supports the E-Resilience objectives:
  - a. resilient ICT networks,
  - b. support to disaster management systems, and
  - c. ensuring last-mile disaster communication



**ICT & DRR  
GATEWAY**

 E-RESILIENCE TOOLS BY SUBREGION

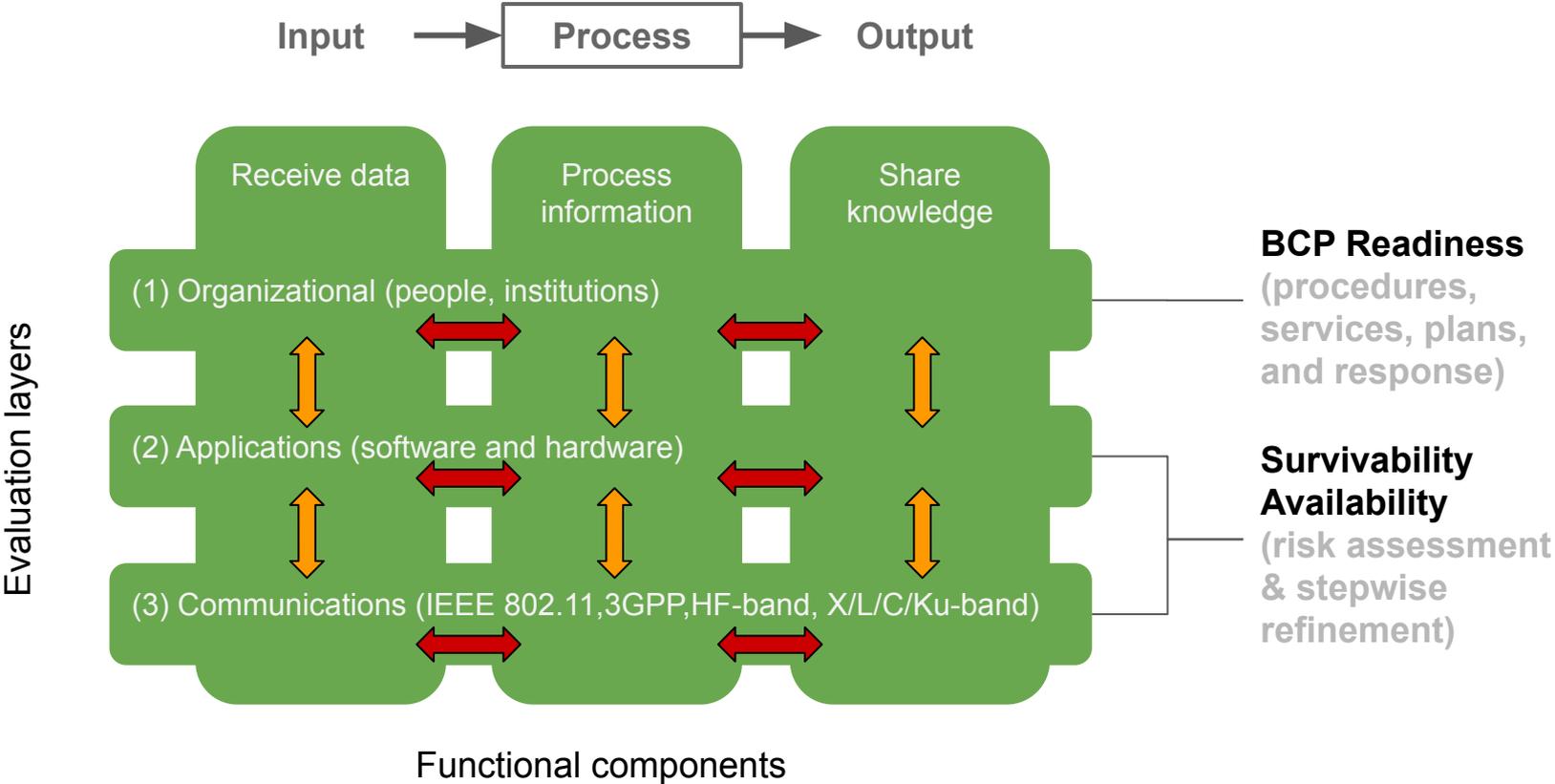


Find e-resilience tools and best practices relevant to:

- > North and Central Asia
- > East and North-East Asia
- > South and South-West Asia
- > South-East Asia
- > Pacific

<http://drrgateway.net/e-resilience>

# E-Resilience Evaluation (incl. Interoperability)



# Applying the method for Pacific Islands

- Subregional workshop on the implementation of the AP-IS and SDGs in Pacific Islands (19-23 Nov 2018, Nadi, Fiji).
- Participants were exposed case studies, theory, tools, and methods on E-Resilience. Within the scope of emergency communication
- They exercised three activities:
  - Sharing participant experiences of telecom outages during disasters.
  - BCP readiness to realize the necessary components of a working and effective Business Contingency Plan (BCP)
  - Hands-on with the RASTER tool

Resources: <https://lirneasia.net/2018/11/ESCAP-APIS-subregional-workshop-Fiji>



# BCP readiness evaluation

- ❑ A [questionnaire](#) was presented to a group of participants:
  - ❑ Belonging to Government and Non-governmental Organizations,
  - ❑ Were affiliated with their ICT apex bodies, telecom regulatory bodies, private sector operators
  - ❑ From countries in the Oceania region
- ❑ Realize their actual readiness to resilient ICT services; namely, determining the effectiveness of their Business Contingency Plans (BCPs)
- ❑ The questionnaire evaluated their management procedures, identification of critical communication services, contingency plans, emergency response protocols, and monitoring & activation of response
- ❑ The likert scale adopted a scoring method: yes = 2.0, work-in-progress = 1.0, no = 0 (no actions), and don't know = -1 (lack of awareness).
- ❑ The UNOFFICIAL [results](#) present themselves as an indicator of the current state of their institutional readiness for practicing effective BCPs

# Implementation of Management Procedures

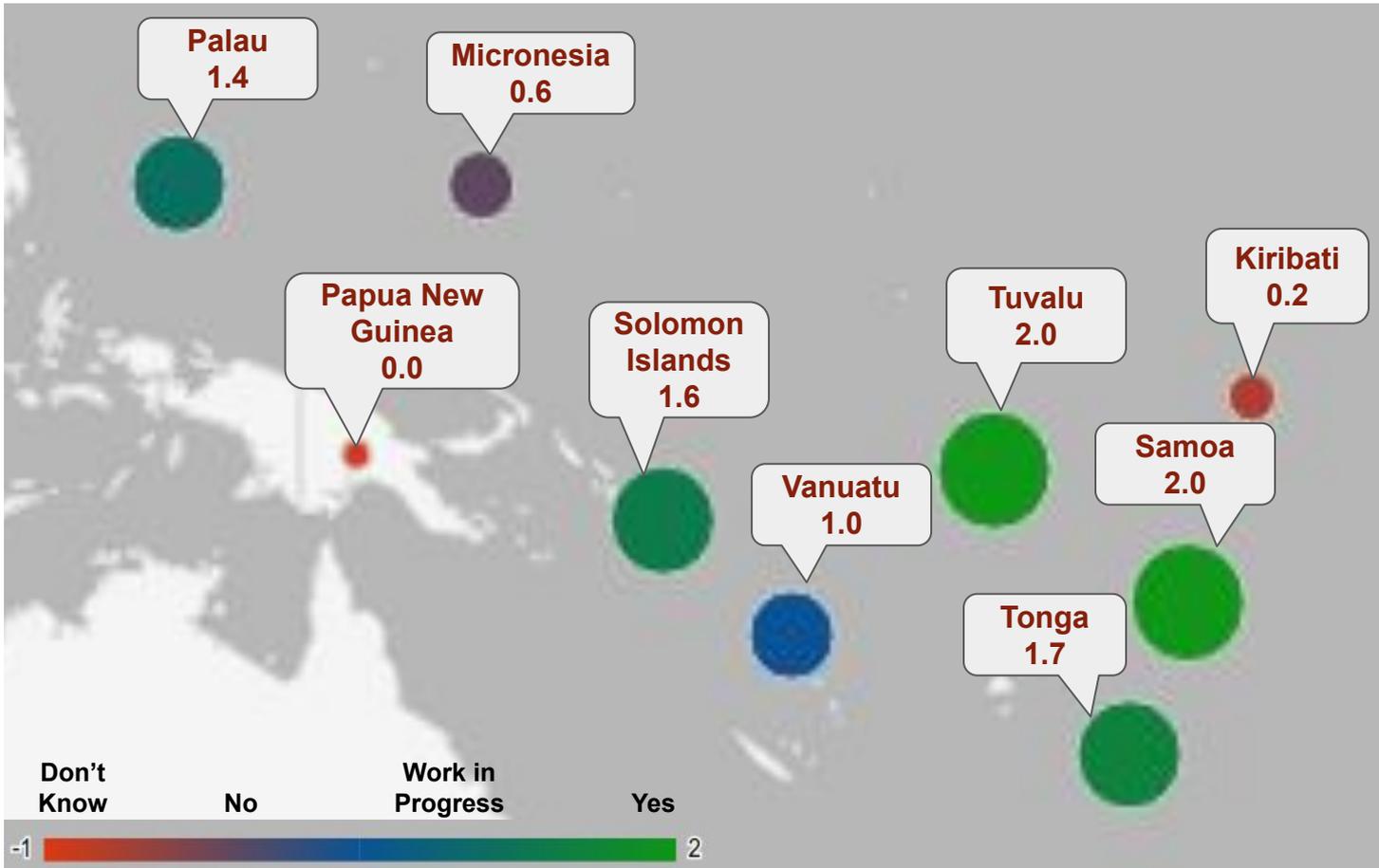
Have you done a risk assessment?

Do you have a communications operation plan?

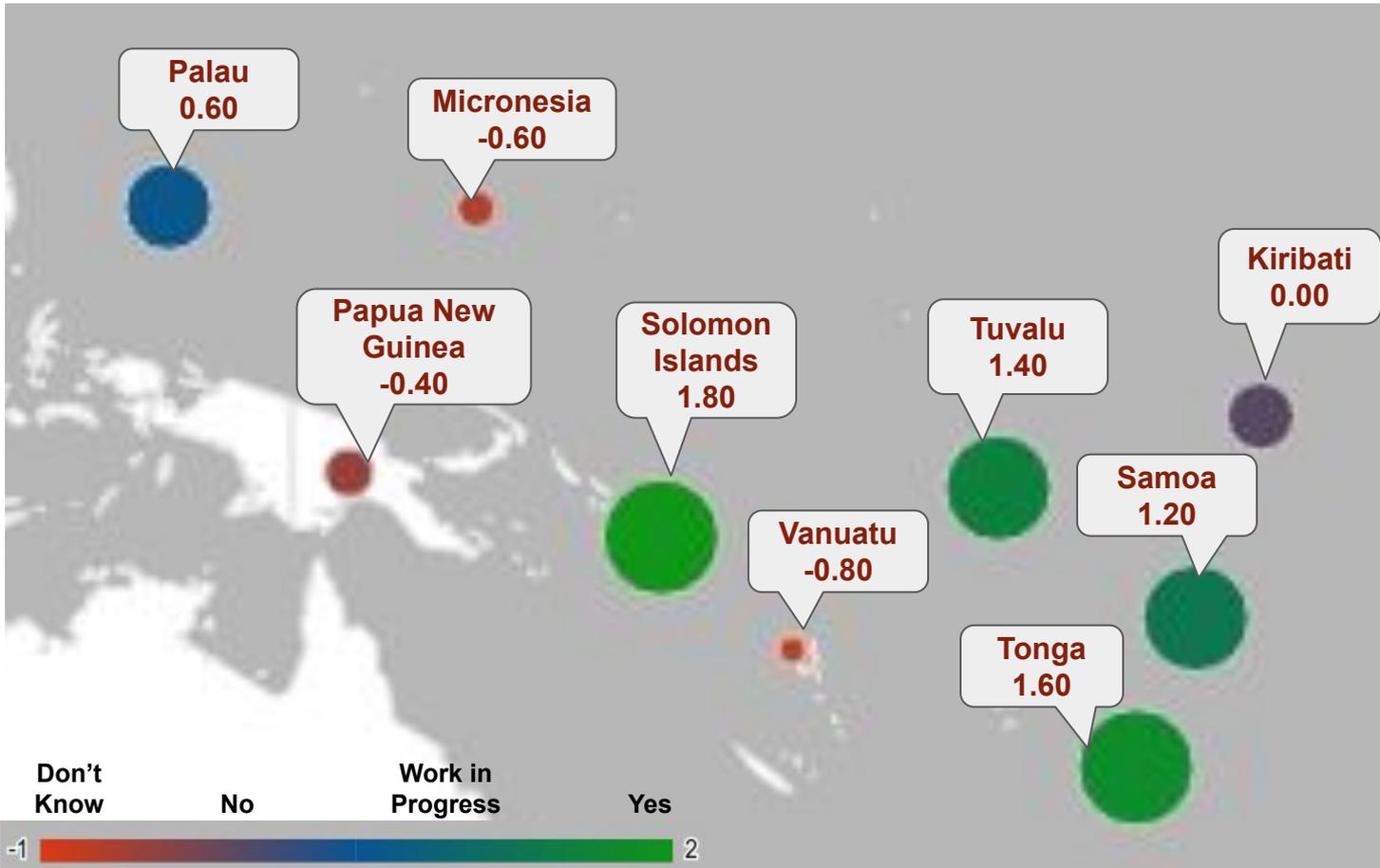
Are there designated recovery coordinators?

Are recovery teams defined, staffed, & trained?

Is there a procedure for damage assessment?



# Identification of Critical Communication Services



Are communication services prioritized?

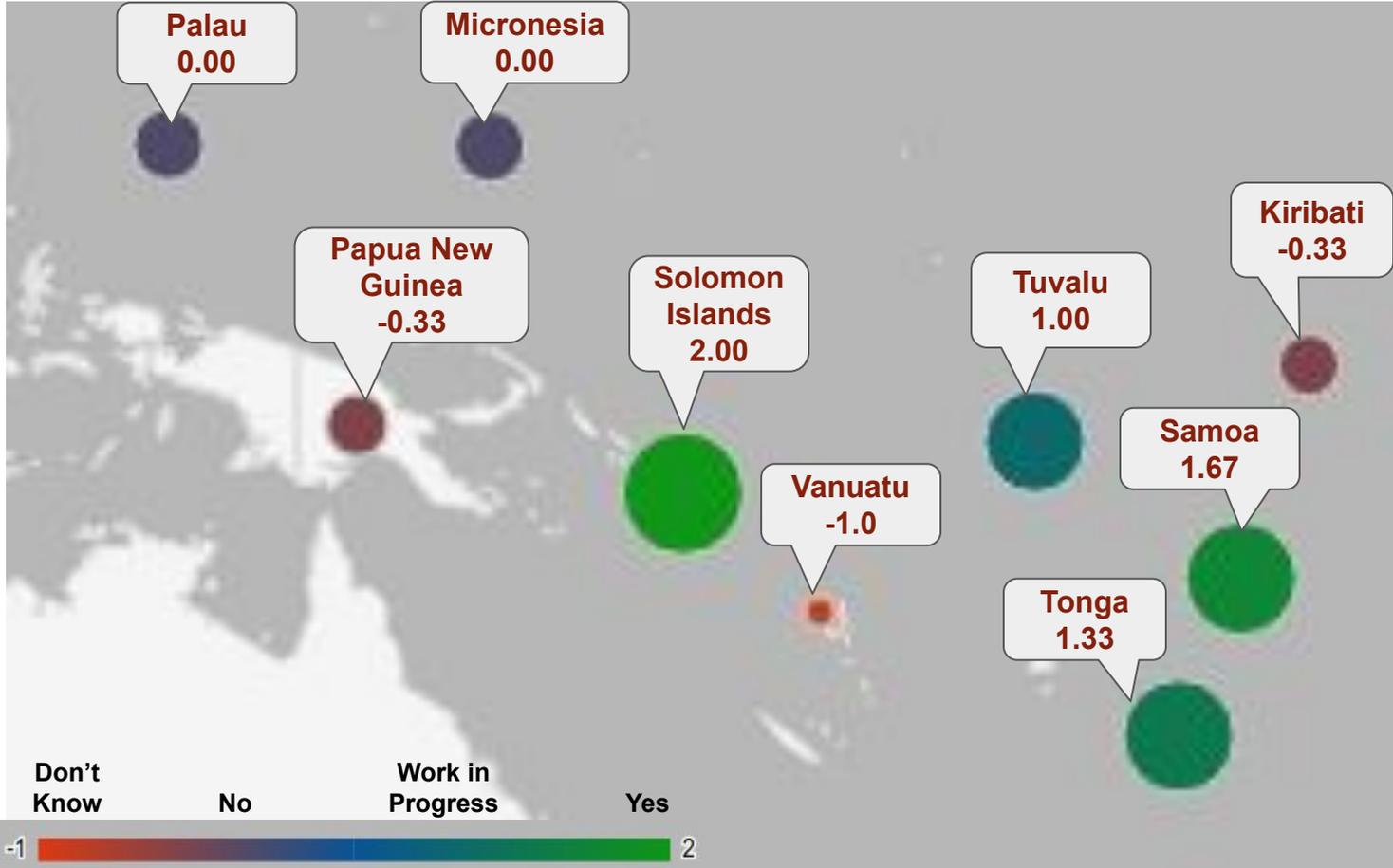
Have you assigned a time to recovery?

Are carriers, vendors, & dependents identified?

Legal & contractual constraints identified?

Have all readiness components been identified?

# Comprehensive Contingency Plans



Are communication services prioritized?

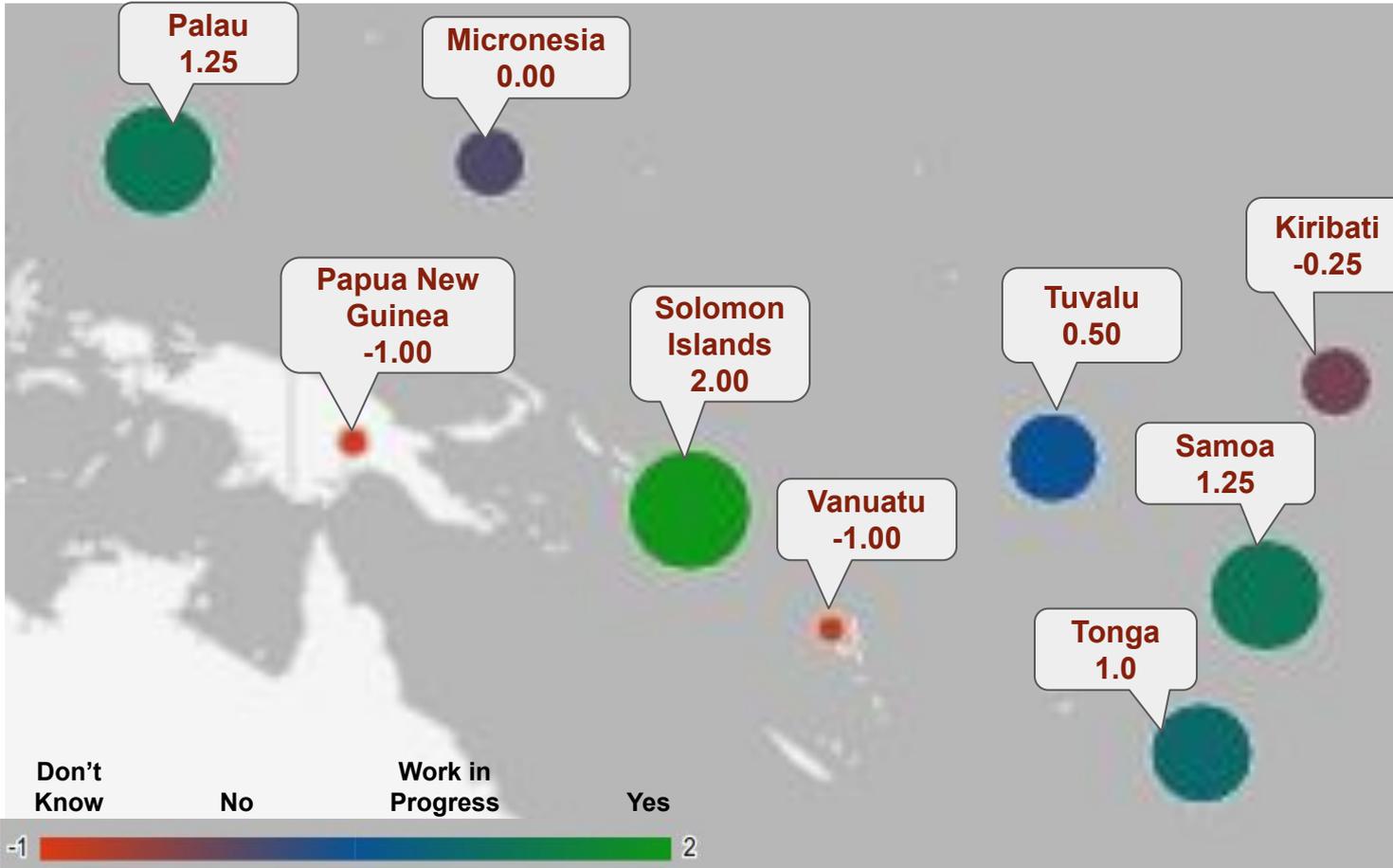
Have you assigned a time to recovery?

Are carriers, vendors, & dependents identified?

Legal & contractual constraints identified?

Have all readiness components been identified?

# Tested Emergency Recovery Procedures



Are emergency recovery procedures in place?

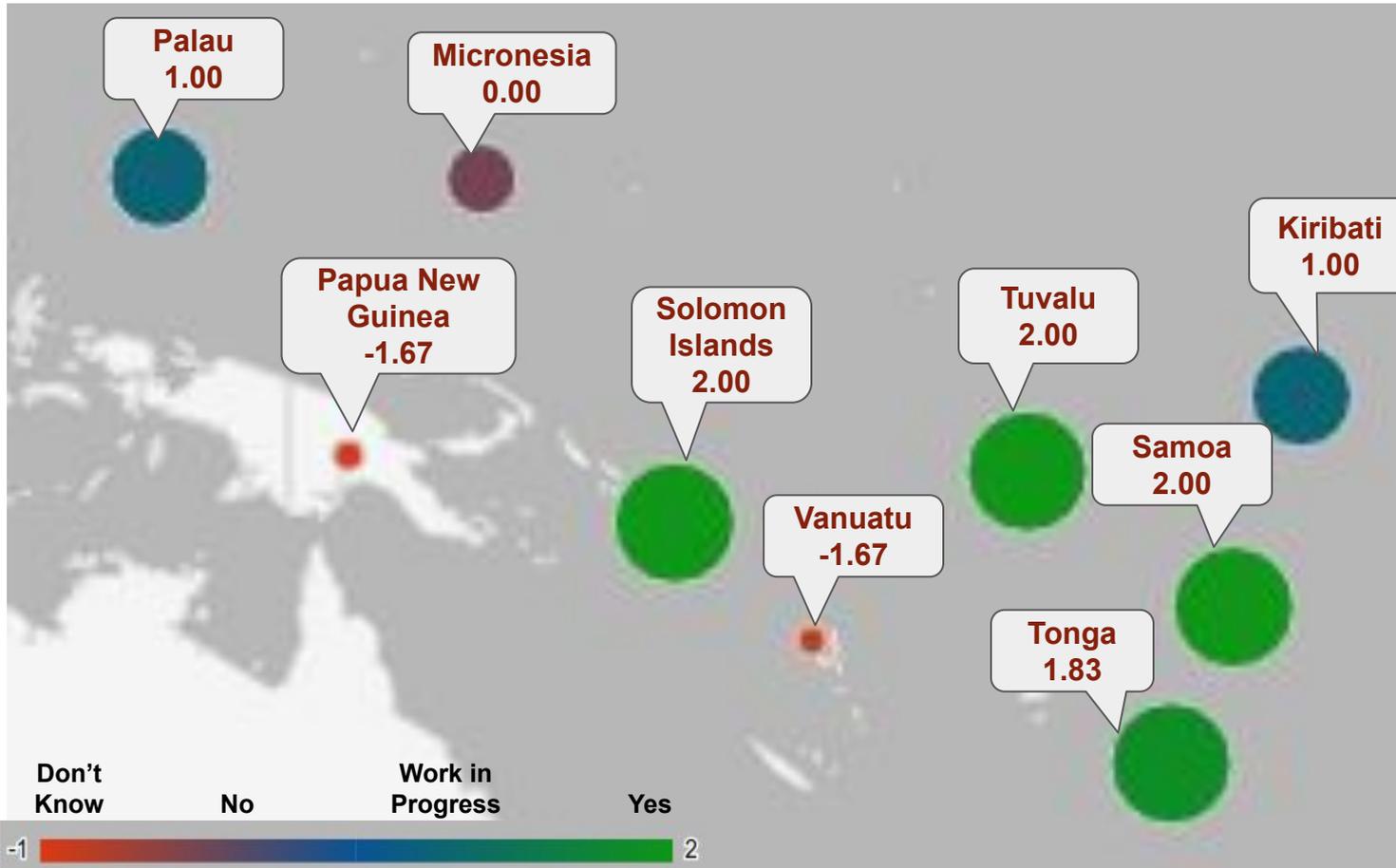
Are minimal recovery times and downtimes defined?

Are team responsibilities and procedures defined?

Have communications and telecom links been established?

Are hardware, software, and link performance frequently tested?

# Event Detection & Notification Practices



Is there a specific procedure for being notified of escalating events or threats?

Is there a specific procedure for notifying disaster management and recovery teams?

Has a minimal time defined for notifying recovery teams?

# What can we, unofficially, infer from the results?

1. Samoa and Solomon Islands claim to have well established all BCP
  - a. requirements with trained personnel, institutionalized procedures
  - b. identified all communication priorities and systems
2. All other participating member state institutions have management procedures;
  - a. but fall short in implementing the necessary elements for making their communication resilient.
3. Only Solomon Islands has fully tested telecom emergency recovery procedures
4. Solomon Islands, Tonga, and Tuvalu have established mechanisms to be vigilant of threats and inform response teams
  - a. Ability to relay those to the response teams for activating any kind of response procedures.
  - b. The others either have partial or no mechanism to alert of events or threats.

# RASTER Methodology

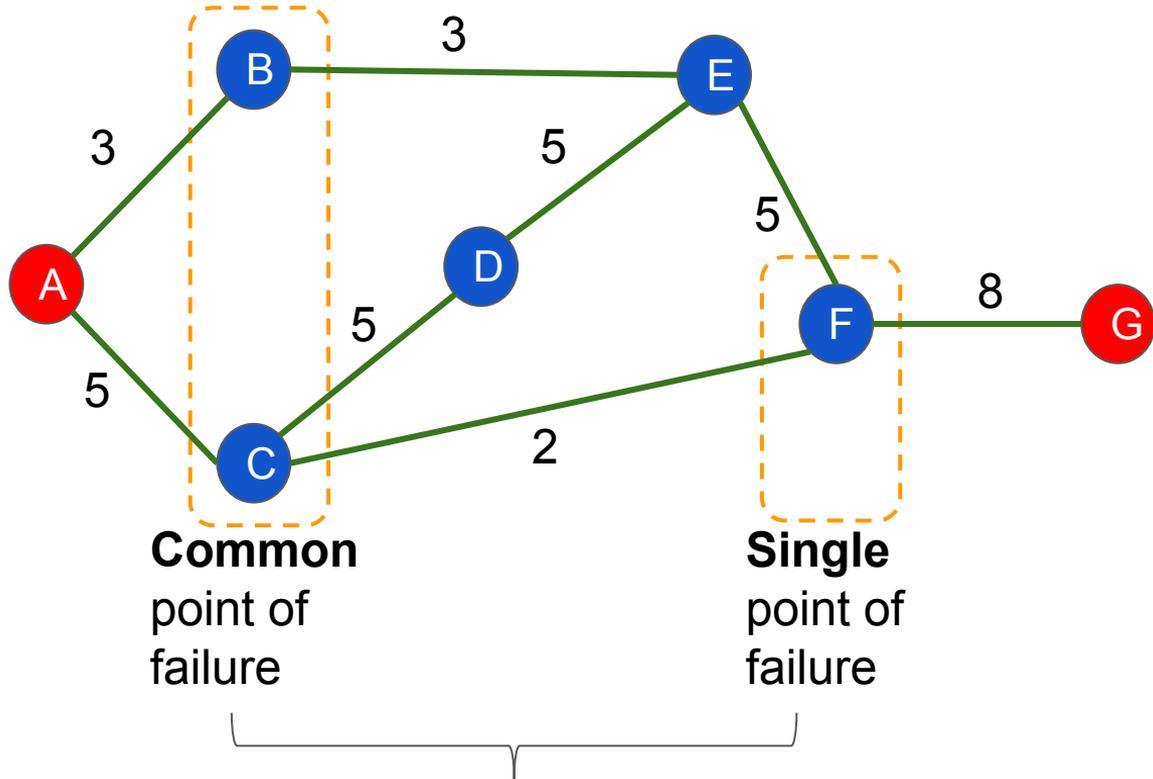
Risk Assessment and Step-wise Refinement

**GOAL** of Raster is to make the organisations becomes less vulnerable to telecom failures by first understand what can go wrong with each telecom service they use.

Raster facilitates the:

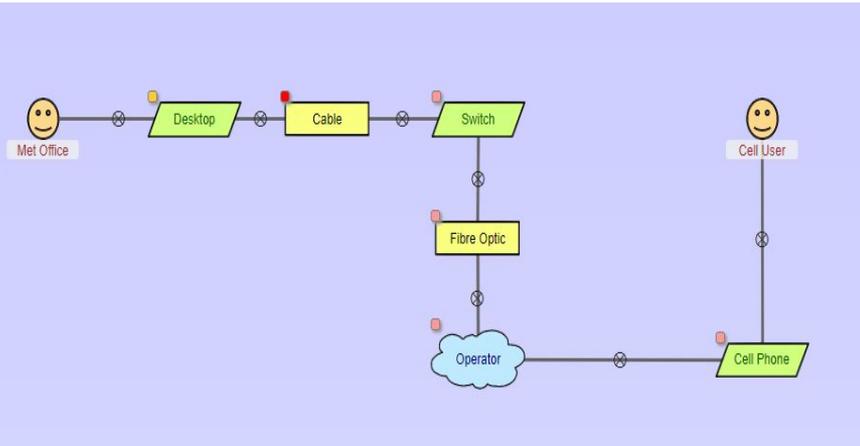
- Uncovering of “black swans”
  - Risk with low probability and high impact (or effects)
  - Basically, rare catastrophic events that bring your comms down to their knees.
- Preparation of recommendation using a tested methodical analysis:
  - based on the technical aspects of failure of telecoms services
  - also takes account of the societal impact of failures, and
  - risk perceptions of external stakeholders

# Points of Failure and Impact



- Common point of failure - single event that affects a collection of nodes
  - E.g. power outage
- Single point of failure - single event effects one nodes
  - E.g. physical damage
- Impact is the minimum cut that affects the maximum flow
  - E.g. removing node E forces to use a lower cost edge CE

# Example evaluation and outcomes from a group exercise



Significant SINGLE POINTS of failures:

- No Power
- Faulty Transmitter
- Availability of staff

Significant COMMON POINTS of failure:

- Broadcasting Transmission tower infrastructure damaged
- Antenna damaged

Single failures

	Configuration	Malfunction	Physical damage	Power	Congestion	Interference	Jamming	Signal weakening	Break	Cable aging	Congestion	Overall
Cable									U	L		H
Cell Phone	U	L	H	H								H
Fibre Optic								H	L	M		H
Operator	L	M	H	H	H	M	H	H	L	L		H
Switch	M	H	L	H								H
Desktop	L	M	M	M								M

Common cause failures

	Configuration	Malfunction	Physical damage	Power	Congestion	Interference	Jamming	Signal weakening	Break	Cable aging	Congestion	Overall
Break									H			H
Congestion											H	H
Physical damage			H									H
Power				H								H
Configuration	M											M
Malfunction		M										M
Cable aging								L				L

Remediation (Treatment) strategy

- Getting broadcast streaming operational
- Have backup power supply within 30mins of reporting failure
- Have alternate redundancy broadcasting equipment available at all times

# Conclusion

1. E-Resilience is a system property but understood almost exclusively in terms of continuity and recovery; the “**bounce forward**” adaptive role of E-Resilience remains uninvestigated
2. E-Resilience, in its current practices, hasn't Included the fundamental enablers of E-Resilience, which are **robustness, self-organization, and learning**
3. RASTER and BCP readiness methods have proven to serve as a catalyst for implementing a true E-Resilience **diagnose** and **remediate** program to bounce forward

# Thank You

Nuwan Waidyanatha

Senior Research Fellow

[nuwan@lirneasia.net](mailto:nuwan@lirneasia.net)



LIRNEasia

*Pro-poor. Pro-market.*

