Cybersecurity: Policy Development and Challenges for Vanuatu

Lloyd M. Fikiasi

3 December 2013,

Kuala Lumpur,

Malaysia

The Government of The Republic of Vanuatu

TRR

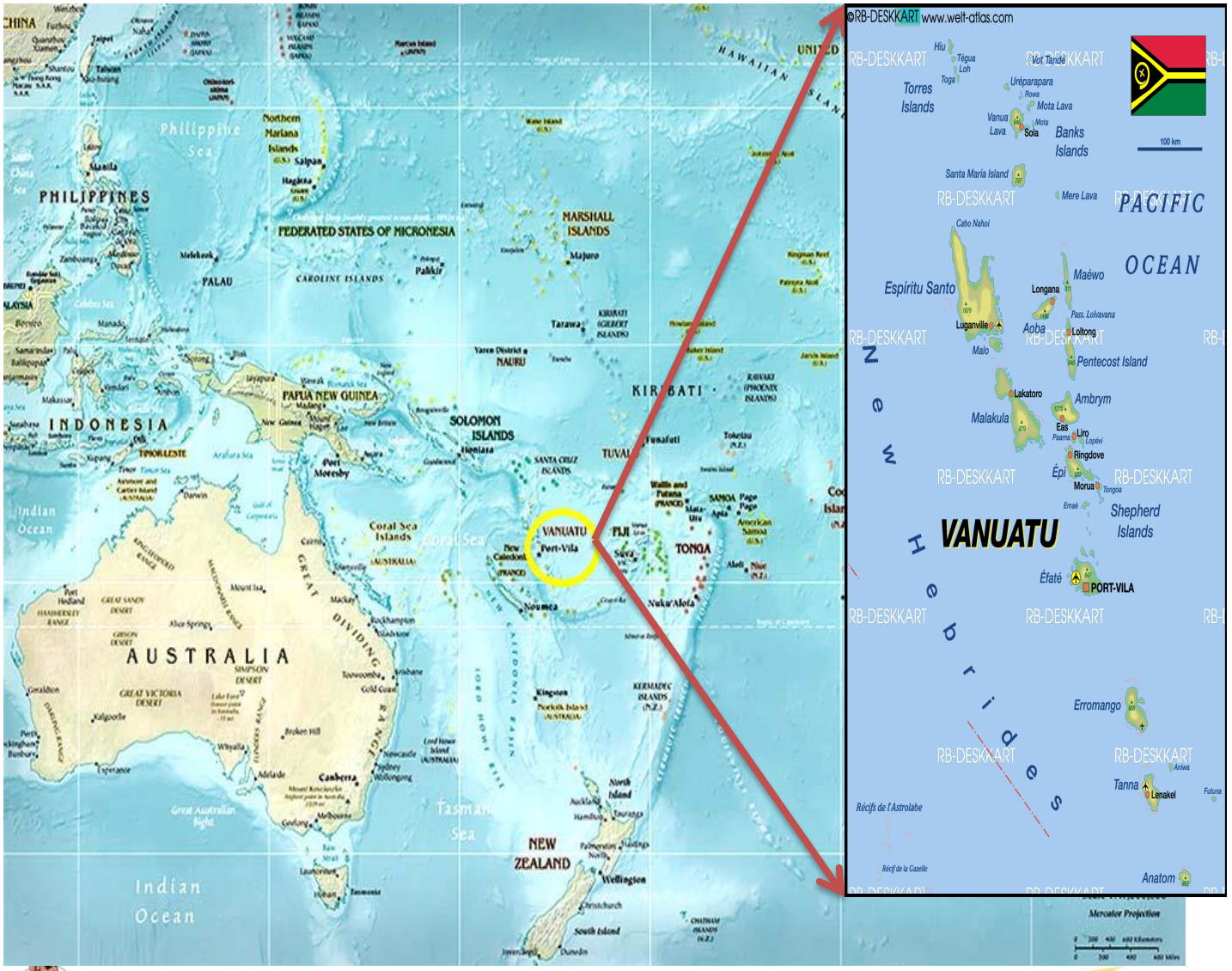
Telecommunications & Radiocommunications Regulator

Content

1. Brief background
2. Drivers for Policy Development
3. Policy Approach
4. Challenges
5. Way forward
6. Conclusion

1. BRIEF BACKGROUND

Vanuatu

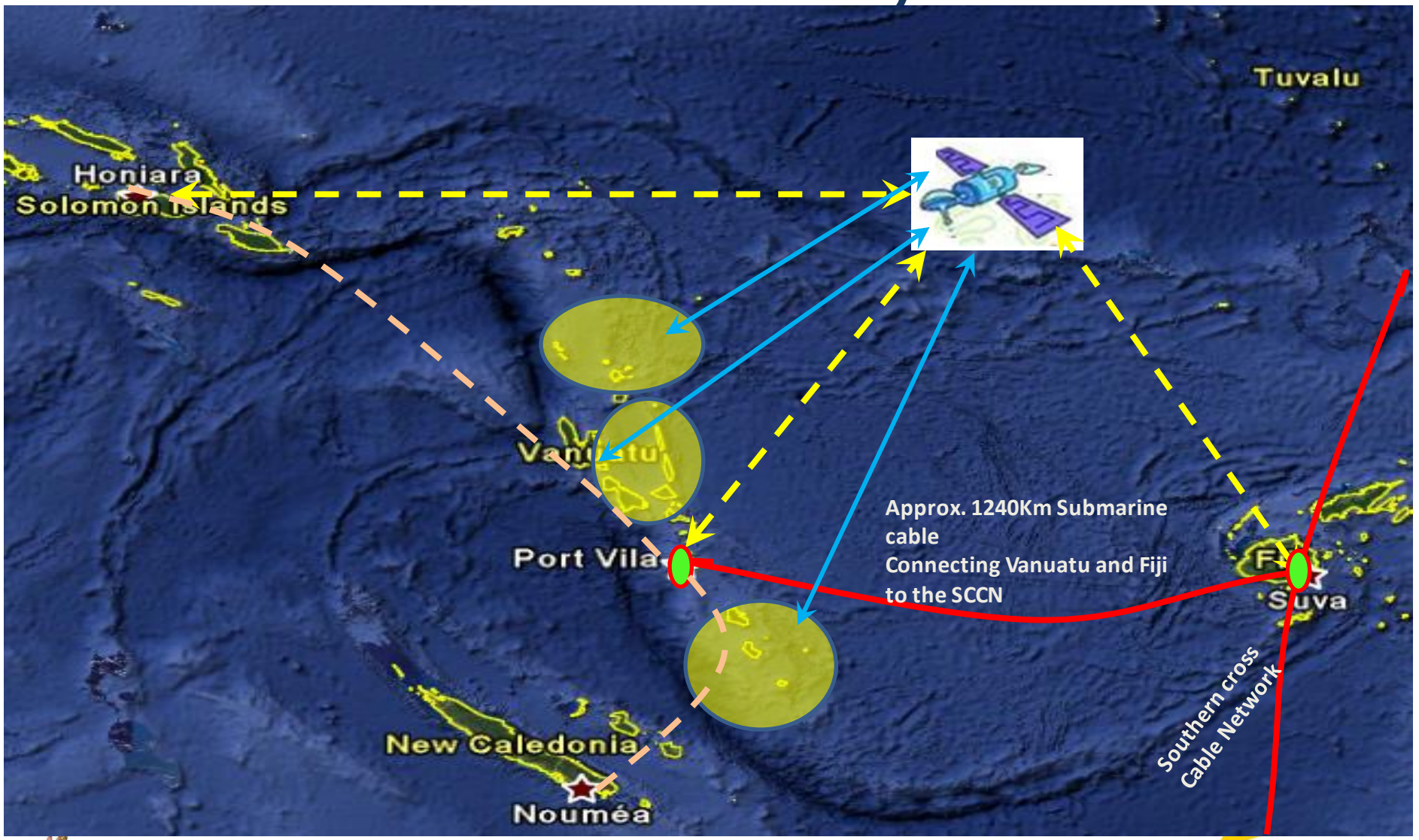


- **Population: approx. 266, 244**
  - **80% rural**
  - **20% urban**
- **Total land area:** 5,000 sq.KM
- **Sea area** 12,000 Sq. Km.
- **More than 80 Islands**
- **Official Language:** French, English and Bislama (approx. 183 indigenous ethnic tribal languages)
- **Government:** Westministerial System
- **Sources of Revenue:** Agricultural products (copra, Kava) cattle and tourism

Technology overview

- Open market access
- 2 Mobile operators & 5 ISPs
- Satellite Technology
- Submarine Cable (Landed and currently install)
- 3G Network in Urban, 2.5G in rural areas

International Gateway

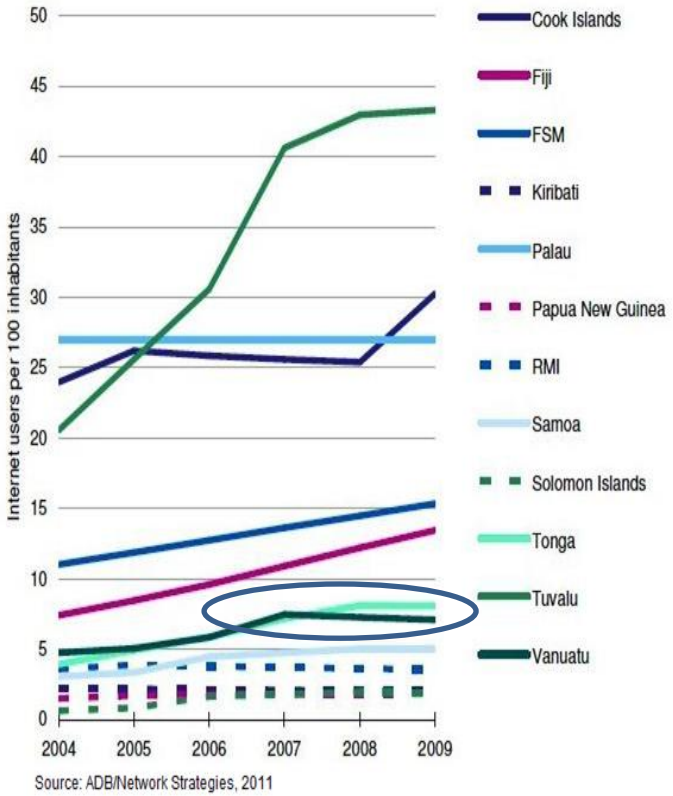


Statistic

- Mobile coverage (92% mobile coverage)

  3G plus internet (urban areas and 2.5G in rural) basic internet through smart phones using 3G and 2.5G.

- Internet usage – still under 15% usage (ADB Network Strategy Report 2011).



TRR
Telecommunication & Radiocommunication Regulator

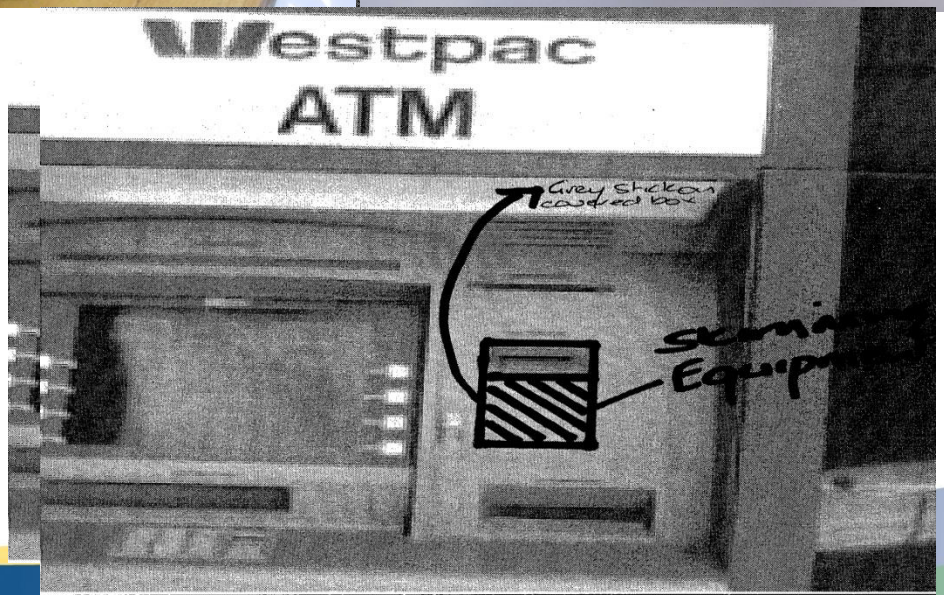
Incidents:

Less internet penetration does not mean Vanuatu did not experience cybersecurity issues:

- In 2012, the former Prime Minister's email was hacked;
- Phishing e.g. commercial banks website;
- SPAM: lottery winning (private and Government emails)
- Cyber-bullying increase;
- Connecting to the cloud with high speed internet access-infrastructure (means more vulnerable to threat).

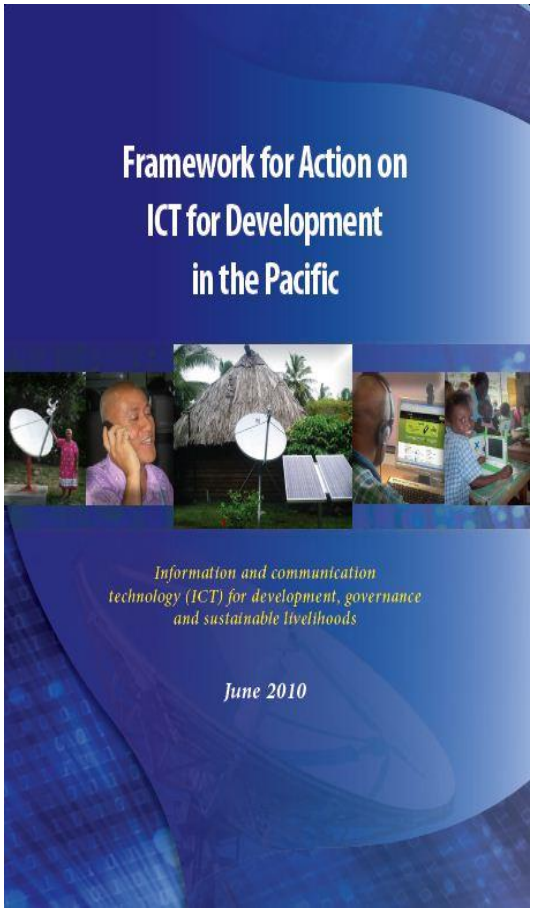
Westpac ATM Fraud – Skimming

Card Scanning Device



2. Drivers for Policy Development

- Pacific region approach: establishment of Framework for Action: Policy & Legislation in place before 2015:
- Increase of cyber activities: online, social medias, financial inclusion, e-banking/wallet, part of the digital era;
- Advance technology introduced (Broadband, submarine cable-means usage will increase-expose users to cyberspace;
- Cyber incidents slowly increase;
- Lack of and outdated laws relating to cybersecurity and cybercrime;



TRR
Telecommunication & Radiocommunication Regulator

For example:

- **can we prosecute someone**:
  - who copied files from your computer or flash drive without your permission?
  - who gained unauthorized access into your comp r?
  - Who ga ed un thori d a cess to your comp ter fr m a oth country?
  - Who crashed your network or bank system?
  - Who gained through online scam (Nigeria, ‘Lost my Wallet’)?

NO!

Our Target:

Vanuatu

- Cybercrime draft Policy to be passed by mid 2013;

- Draft Cybercrime Legislation passed before end of December 2014;

which is still in-line with targets set in the Framework for Action for ICT in Pacific

CWG ensure this to happen.

Policy Development:

- In December 2012, Government established a working Group tasked to support the drafting of cybersecurity Policy and Cybercrime legislation to address cybersecurity and cybercrime issues in Vanuatu.
- Multi-stakeholder members.
- Work close with ITU- through ICB4PAC Project 2011 – ITU Project for Pacific countries.
- Develop a draft cybersecurity policy and cybercrime legislation in 2012.
- Our Draft skeleton legislation in place-contain specific provision for child online pornography

- Consultation on Policy: wide public consultation
- Government and private sector including operators;
- Feedbacks received- NGO's, individuals and other member of public;
- Submitted before DCO and to Council of Ministers early-Mid 2013;
- Policy finalized and endorsed by COM early November 2013;
- Passing of the Policy achieved;

3. Policy Approach

Policy structure

National Vision

“Citizens of Vanuatu, tourists, businesses and government to enjoy the full benefits of a safe, secure and resilient cyber space enabling them to get access to knowledge and share information while understanding and addressing the risks, to reduce the benefits to criminals”.

TRR
Telecommunication & Radiocommunication Regulator

Introduction

National Vision

Goal 1
Develop the necessary organizational structure

8 Objectives

1. Establish of a Multi-stakeholder Committee
2. Identify all Ministry and Dept.
3. Identify rural champions-private partnership
4. Establish a National CERT
5. Create Child Online Protection Group
6. Create strategy to encourage Incidents report
7. Develop Unit within Police for cybersecurity
8. To carry out survey to report on incidents

Goal 2
Standardization and Services

7 Objectives

1. Work close with Operators protect infrastructure
2. Standards for operators to protect infrastructure from threats
3. work close with CERT
4. CERT to provide service to citizens and business-cybersecurity needs
5. Enable ISPs to block unwanted internet contents
6. Enable mobile operators to block SIM accessing unwanted services
7. Empower CERT to carry out services

Goal 3
Strengthening the legal framework

2 Objectives

1. Review current legislations/framework
2. Draft cybercrime legislations

Goal 4
Capacity building

4 Objectives

1. Curriculum for school
2. Create partnership locally and internationally
3. Develop programs for law enforcements
4. Law enforcment create crime prevention program-cybercrime

Goal 5
International Cooperation

3 Objectives

1. Ensure legal framework inline with international framework
2. Partnership with international groups e.g. InterPol
3. Identify international program to benefit Vanuatu

4. Challenges

Challenges:

- Identifying Champions;
- Capacity building- law enforcements, judiciary and general users;
- Lack of financial and skilled human resources
- Supporting schools curriculum- cost implications and change of structure;
- Technology keep on changes, which may require change to policy approach.

5. Way Forward

Way forward

- Regulator continue to support Government on policy implementation;
- CWG draw down strategic plans for implementing each goals of the policy;
- Regulator through its consumer awareness and IG programes will continue to raise cybersecurity awareness to public;
- Maintain the support from experts: international bodies such as APT, ITU-IMPACT and similar for capacity building and technical advises (esp. law enforcements and judiciary);
- Collaborate with national key stakeholder including Government for implementation;
- Share experiences with regional counterparts;
- Take multiple stakeholder approach to implement the policy;
- Encourage champions in rural and within all governmental departments.

6. Conclusion

- Safe use of ICTs and internet is a goal of Vanuatu Government;
- Protect users in cyberspace and the use of ICTs in Vanuatu;
- Having such policy is a big milestone for Vanuatu;
- Vanuatu will continue to advocate for “safe use of internet and ICT”;
- Champions and multiple stakeholder approach is Key for implementing the Policy.

- Is having a cybersecurity Policy for Vanuatu the answer to cybersecurity issues?

THANK YOU!

Lloyd Fikiasi
Office of the Regulator-Vanuatu
lloydfikiasi@trr.vu
www.trr.vu

END-