COLLABORATIVE CYBERSECURITY

The Mauritius example

Anri van der Spuy
Dr Krishna Oolun

RESEARCH ICT AFRICA

Cybersecurity and the digital divide paradox

- with increasing connectivity comes more cyber threats
- challenges of IG also apply to cybersecurity: fast response rates, legitimacy, practicality, expertise, flexibility, resources, etc.
- African context: few cybersecurity strategies in place, digital (il)literacy, institutional (in)capacity, etc.

-> the digital divide paradox

Whose responsibility is it?

The scale, scope + pace of cyber threats = it's difficult to deal with cyber threats alone…

- **governments**: focal points, legitimacy
- **private sector**: more resources, expertise, freedom/flexibility, avoiding diplomatic fallout (e.g. Sony/North Korea)
- civil society? technical community? users?

Public-private collaborations

= collaborative relationships in the interest of promoting safety + security; towards common or mutual goals

+

- leverage joint resources
- capitalise on diverse competences/strength
- based on trust, fairness, honesty, reciprocity

–

- poorly understood/defined
- dissonant rationales (commercial vs public interest)
- competition for power, withholding information, trust

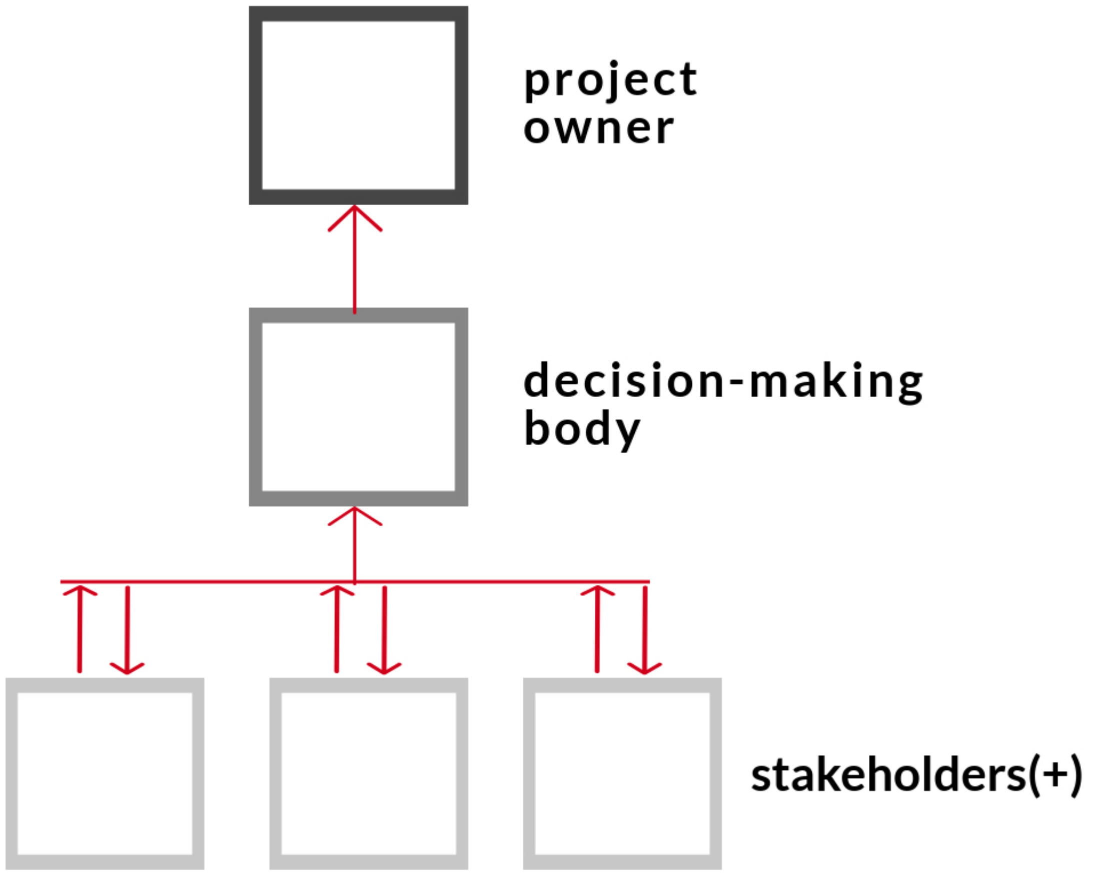
Mauritius

- Rated top African country ITU’s *Global Cybersecurity Index 2017*
- Regional hub (COMESA/SADC)
- National Broadband Policy 2012 + National Cybersecurity Strategy 2014-2019
- Strategy Goal 3: ‘to develop an efficient collaborative model between the authorities and the business communities’

RESEARCH ICT AFRiCA

The Mauritius case

PHASE I: PPP

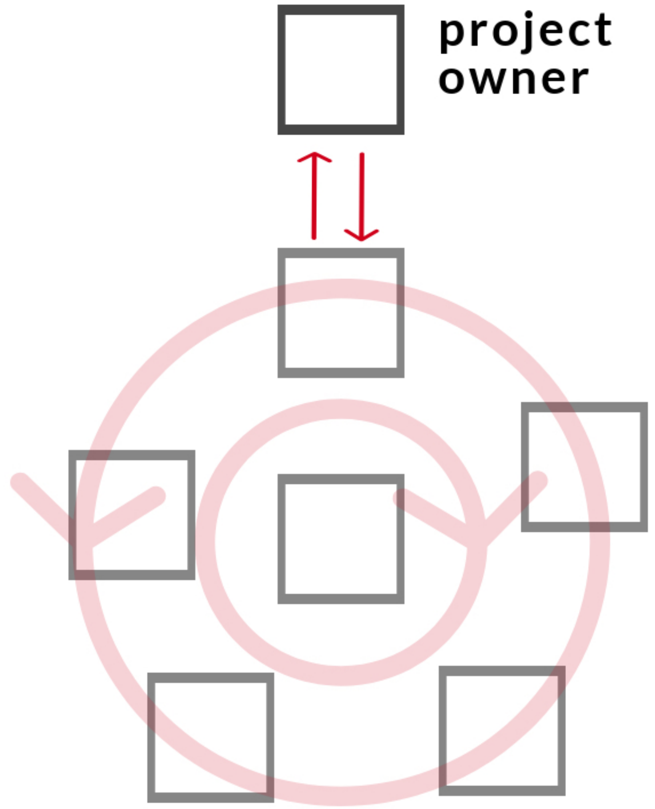


project owner

decision-making body

stakeholders(+)

PHASE II: PPI



project owner

Phase I

- predefined roles
- hierarchical dependency
- prescriptive (lack of flexibility)
- some partners more powerful
- closed

Phase II

- interactions rather than hierarchical reporting lines
- descriptive (more flexible)
- robust information-sharing measures
- more stakeholder buy-in
- open

RESEARCH ICT AFRiCA

Some findings

- ‘more vivid’ stakeholder participation = a step in the right direction, but…
- evolving risks (e.g. third party providers, information sharing, cloud computing, data protection requirements)
- perpetual risk of dominating parties, still need broader participation of stakeholders as digital economy becomes more central to economy

Policy recommendations

- flexibility, transparency + information-sharing among participants are important
- both vertical + horizontal collaboration needed
- descriptive rather than prescriptive
- broader selection of stakeholders valuable
- special effort to involve stakeholders who find it difficult to participate/ are vulnerable to cyber harm

Thank you

RESEARCH
ICT AFRiCA