Collaborative cybersecurity in Africa

Promoting cybersecurity through better collaboration: the Mauritius example

Anri van der Spuy, manager, Research ICT Africa Digital Policy Project
Dr Krishna Oolun, RIA associate/advisory board

Approach

- **objective**: gaining a more realistic understanding of cybersecurity collaborations in Africa (including the nature and forms thereof)
- **method**: exploratory literature review; qualitative case study in Mauritius (interviews with key stakeholders, policies, documents analysis)
- **scope**: rationale for collaboration, nature of it, challenges, factors that impact success/failure
- **sources**: primary + secondary data

Cybersecurity as a ‘unique’ governance challenge

- with increasing connectivity comes increasing cyber threats
- nature of the cyber environment = difficulty of dealing with cyber threats/harms
- other factors specific to African context: few strategies, digital (il)literacy, general lack of awareness, institutional (in)capacity, etc. > digital divide paradox

= need for fast response rates, legitimacy, expertise, capacity to innovate, flexibility, resources…

Whose responsibility is it anyway?

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

- **governments**: focal points, legitimacy
- **private sector**: more resources, expertise, freedom flexibility, avoiding of 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

-

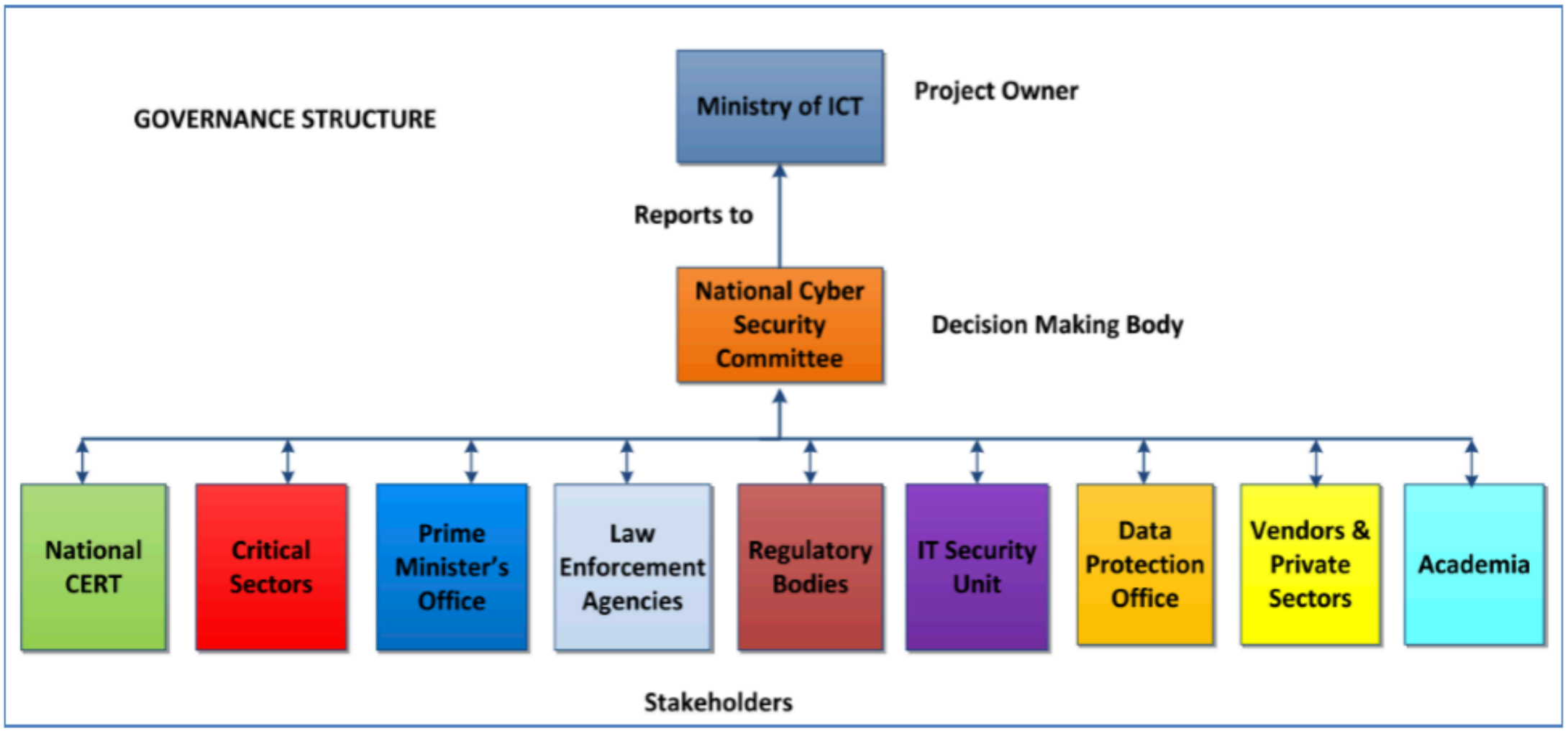
- poorly understood/defined
- dissonant rationales (commercial vs public interest)
- competition for power, tensions, withholding information, mistrust

Mauritius

- Rated top in ITU's *Global Cybersecurity Index 2017*
- 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'

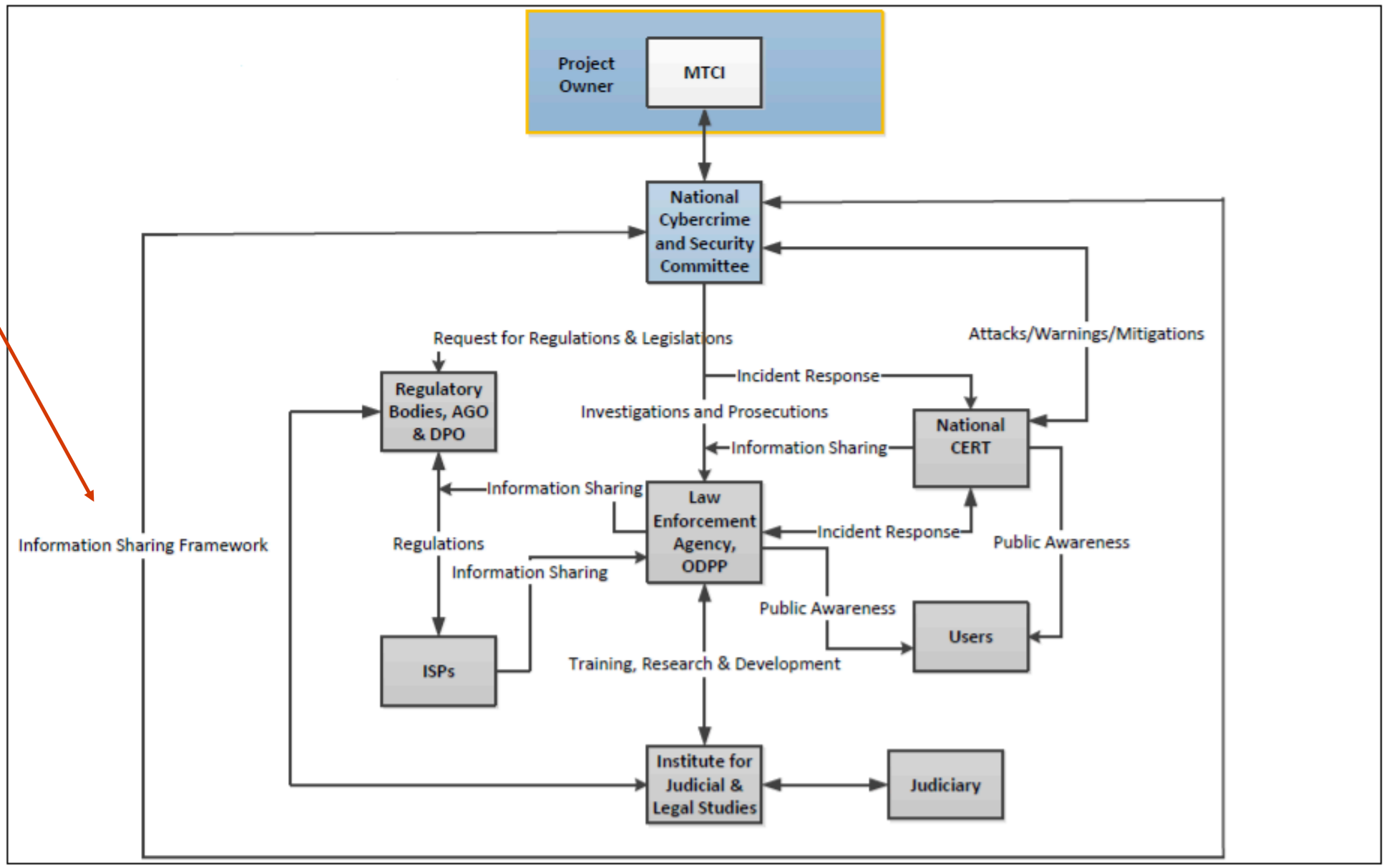
The Mauritius case: phase I

2014-16: PPP (defined roles + methods)



The Mauritius case: phase II

2016-current: PPI



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

The Mauritius case: 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

1. Flexible, broad approaches are preferable to hierarchical, rigid arrangements
2. Collaborations must have clear goals/objectives
3. Need for more African governments to adopt collaborative arrangements based on 1+2
4. Indicators (perceptions) could be useful to assess and improve cybersecurity collaborations in Africa

Next steps

- More comparative examples of collaborations in Africa needed (and compared to Mauritian case) - possible South Africa case as next step
- Better understanding of collaborative arrangements would be useful - e.g. PPPs, PPIs + multistakeholder collaborations
- Collaborative examples from other sectors (e.g. environmental protection) could provide useful lessons

Thank you