Finding our path through the CBM forest

Finding our path through the CBM forest

How can CBMs be operationalized in our region?

Examples drawn from:

- The UNGGE
- ARF Work Plan on Security of and In The Use Of ICTs
- ASPI's regional work.

Challenges:

- Region is diverse and has differing priorities
- Some countries with too little capacity
- Some countries with too much capacity - organizational confusion.

Before Identifying and Implementing CBMs

- What capacity exists?
- Can these CBMs be achieved?
- Where capacity is lacking, help build skills.
    - Lays ground work for future CBMs & is a CBM itself.

Capacity Building to enable better operationalization of CBMs

- Bilateral & Multilateral
- Multistakeholder initiatives
  - Global Centre for Cyber Expertise
- CERT Community - APCERT
- Policing training
- Numbers Community - APNIC
- Private sector

What CBMs are a good fit for our region?

UNGGE

- 16 (a) *The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts.*
  - Australia's ARF Cyber Points of Contact Proposal.
- 16 (d) *The voluntary provision by states of their national views of categories of infrastructure that they consider critical and national efforts to protect them etc.*
  - Lays groundwork for norm that countries should not target critical infrastructure that provides services to the public
- 16 (f) (h) *The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.*
  - How are issues escalated and classified within domestic set-ups?
  - Reduces misunderstandings, creates clarity.
  - Enables easier sharing of threat information.
- 17 (a) *...the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions.*
  - Matchmaking between potential secondees and host organisations.
  - Exchanges involving both government and non-government cyber experts and institutions.
  - Deepens understanding.

ARF Work Plan

- 2 (i.) *The voluntary sharing of information on national laws, policies, best practices and strategies (etc).*
  - Production of white papers
  - Creation of a 'glossary of terms'
- 2 (vii.) *Raising awareness for non-technical personnel and policy makers on threats in the use of ICTs and methods for countering such threats.*
  - Seminars for technical training of policy experts
  - 'Train the trainers'
  - Tailored programs in local languages
- *Conduct of surveys on lessons learnt in dealing with threats to the security of and in the use of ICTs (...) taking into account the work already done in the commercial computer security sector.*
  - Private sector, large capacity & expertise
  - Stake in ensuring stability of online environment

UNGGE

- *16 (a) The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts.*
  - Australia's ARF Cyber Points of Contact Proposal.

- *16 (d) The voluntary provision by states of their national views of categories of infrastructure that they consider critical and national efforts to protect them etc.*
  - Lays groundwork for norm that countries should not target critical infrastructure that provides services to the public

- *16 (d) (iv) The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.*
  - How are issues escalated and classified within domestic set-ups?
  - Reduces misunderstandings, creates clarity.
  - Enables easier sharing of threat information.

- *17 (a) ..the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions.*
  - Matchmaking between potential secondees and host organisations.
  - Exchanges involving both government and non-government cyber experts and institutions.
  - Deepens understanding.

- *16 (a) The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts.*
    - Australia's ARF Cyber Points of Contact Proposal.

- *16 (d) (iv) The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.*

  - How are issues escalated and classified within domestic set-ups?
  - Reduces misunderstandings, creates clarity.
  - Enables easier sharing of threat information.

- *16 (d) The voluntary provision by states of their national views of categories of infrastructure that they consider critical and national efforts to protect them etc.*

    - Lays groundwork for norm that countries should not target critical infrastructure that provides services to the public

- *17 (a) ..the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions.*

    - Matchmaking between potential secondees and host organisations.
    - Exchanges involving both government and non-government cyber experts and institutions.
    - Deepens understanding.

ARF Work Plan

- *2 (i.) The voluntary sharing of information on national laws, policies, best practices and strategies (etc).*
  - Production of white papers
  - Creation of a 'glossary of terms'

- *2 (vii.) Raising awareness for non-technical personnel and policy makers on threats in the use of ICTs and methods for countering such threats.*
  - Seminars for technical training of policy experts
  - 'Train the trainers'
  - Tailored programs in local languages

- *Conduct of surveys on lessons learnt in dealing with threats to the security of and in the use of ICTs (…) taking into account the work already done in the commercial computer security sector.*
  - Private sector, large capacity & expertise
  - Stake in ensuring stability of online environment

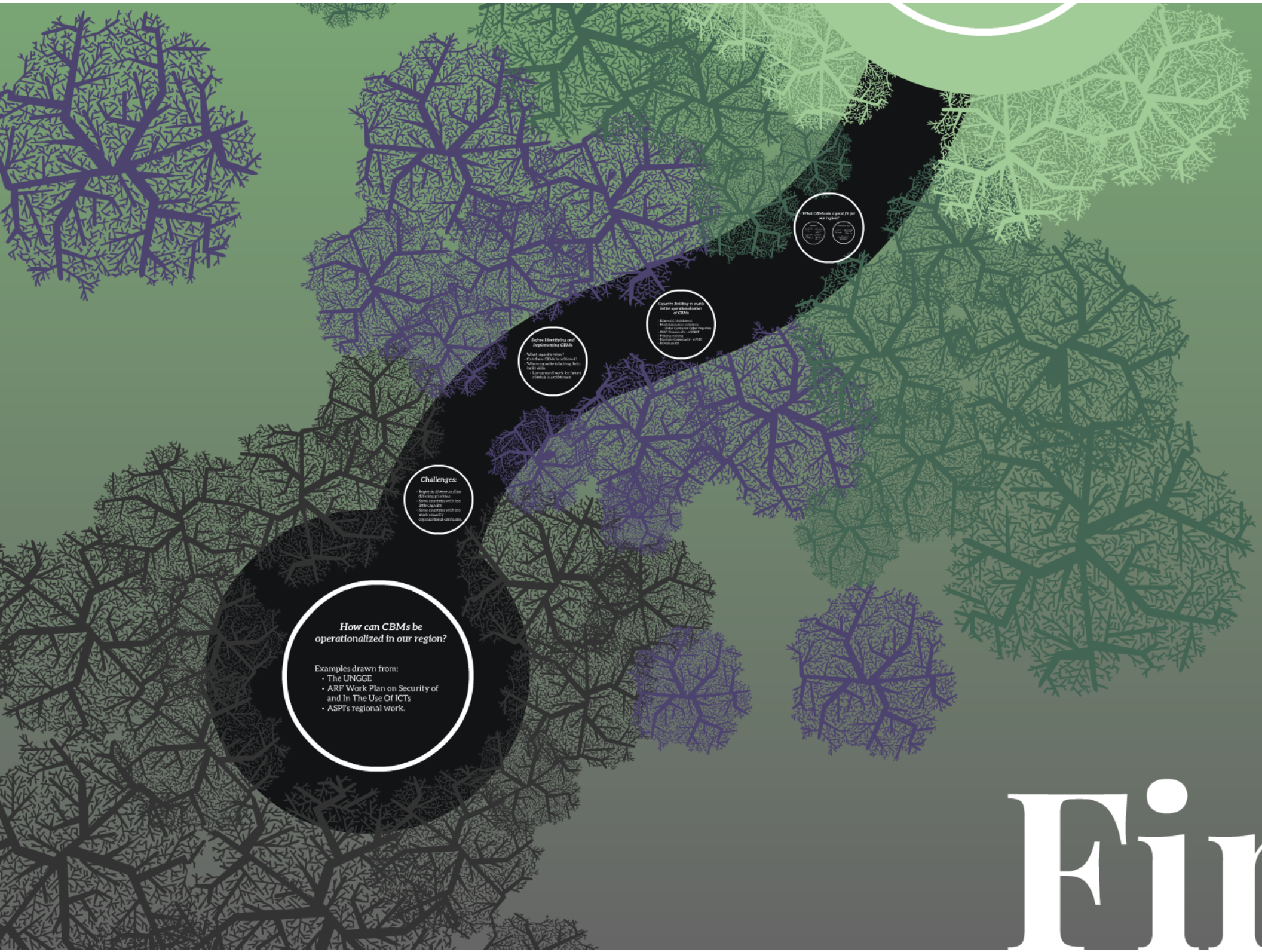
- *2 (i.) The voluntary sharing of information on national laws, policies, best practices and strategies (etc).*
    - Production of white papers
    - Creation of a ‘glossary of terms’

- *2 (vii.) Raising awareness for non-technical personnel and policy makers on threats in the use of ICTs and methods for countering such threats.*

    - Seminars for technical training of policy experts
    - 'Train the trainers'
    - Tailored programs in local languages

- *Conduct of surveys on lessons learnt in dealing with threats to the security of and in the use of ICTs (…) taking into account the work already done in the commercial computer security sector.*

    - Private sector, large capacity & expertise
    - Stake in ensuring stability of online environment


What CBMs are a good fit for our region?
Capacity Building to enable better operationalisation of CBMs
Before Identifying and Implementing CBMs
Challenges:
How can CBMs be operationalized in our region?
Examples drawn from:
• The UNGGE
• ARF Work Plan on Security of and In The Use Of ICTs
• ASPI's regional work.

Conclusion

- What existing capacity do we have in the region?
- How can we strategically develop capacity in support of operationalizing CBMs?
- There are numerous useful CBMs that can be effectively implemented now.

THANK YOU!

Jessica Woodall
International Cyber Policy Centre
The Australian Strategic Policy Institute
Contact: jessicawoodall@aspi.org.au

Finding our path through the CBM forest