

Defining Offensive Cyber Capabilities

Tom Uren

@tomatospy

tomuren@aspi.org.au



Offensive cyber operations

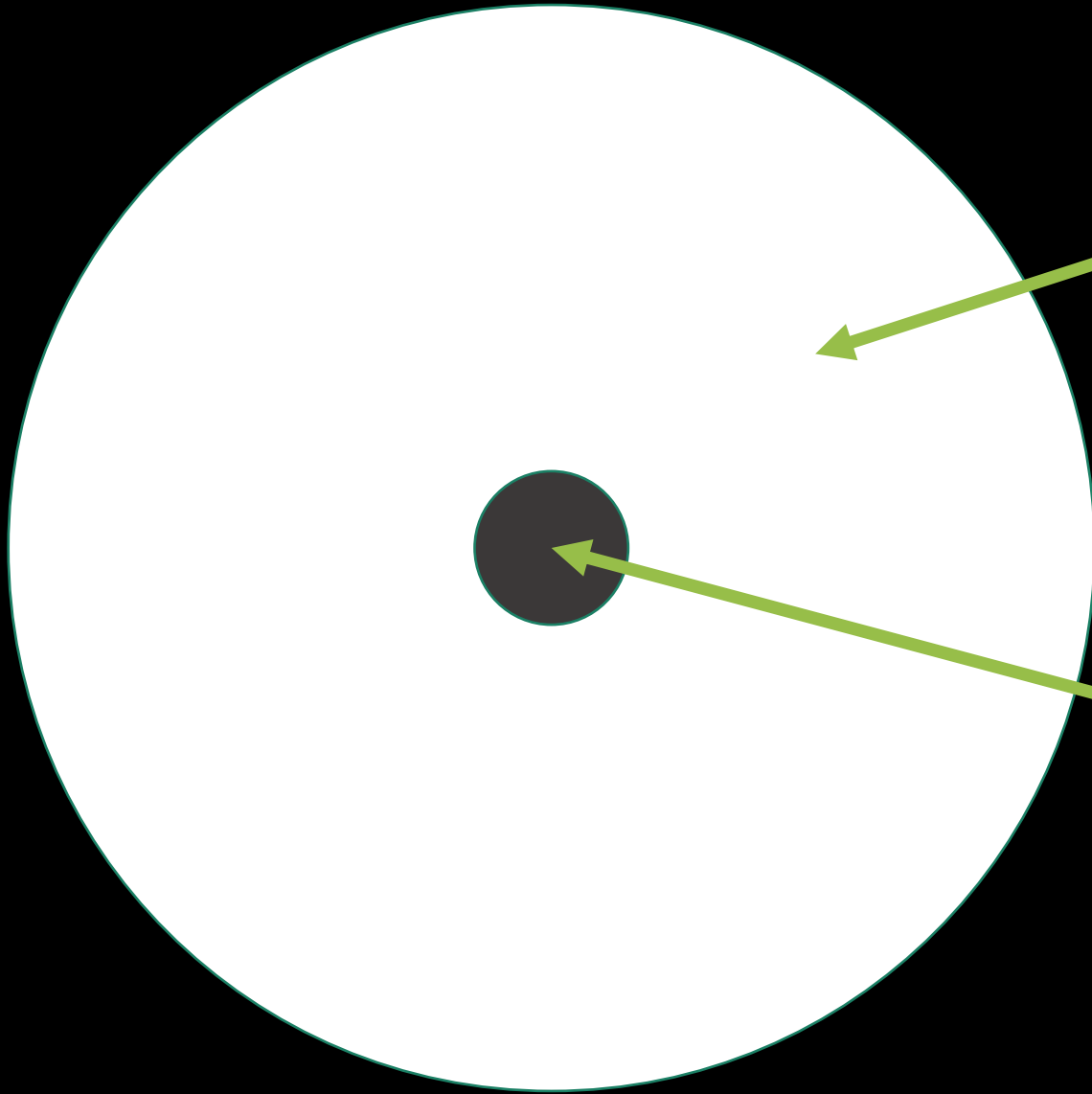
operations to

**manipulate, deny, disrupt,
degrade, or destroy**

**targeted computers, information systems
or networks.**

Cyber weapons: a narrow definition

software and IT systems that,
through ICT networks,
cause destructive effects
and have no other possible uses



Software that
could be
used to
destroy

Software that
can only
destroy

Recommendation 1

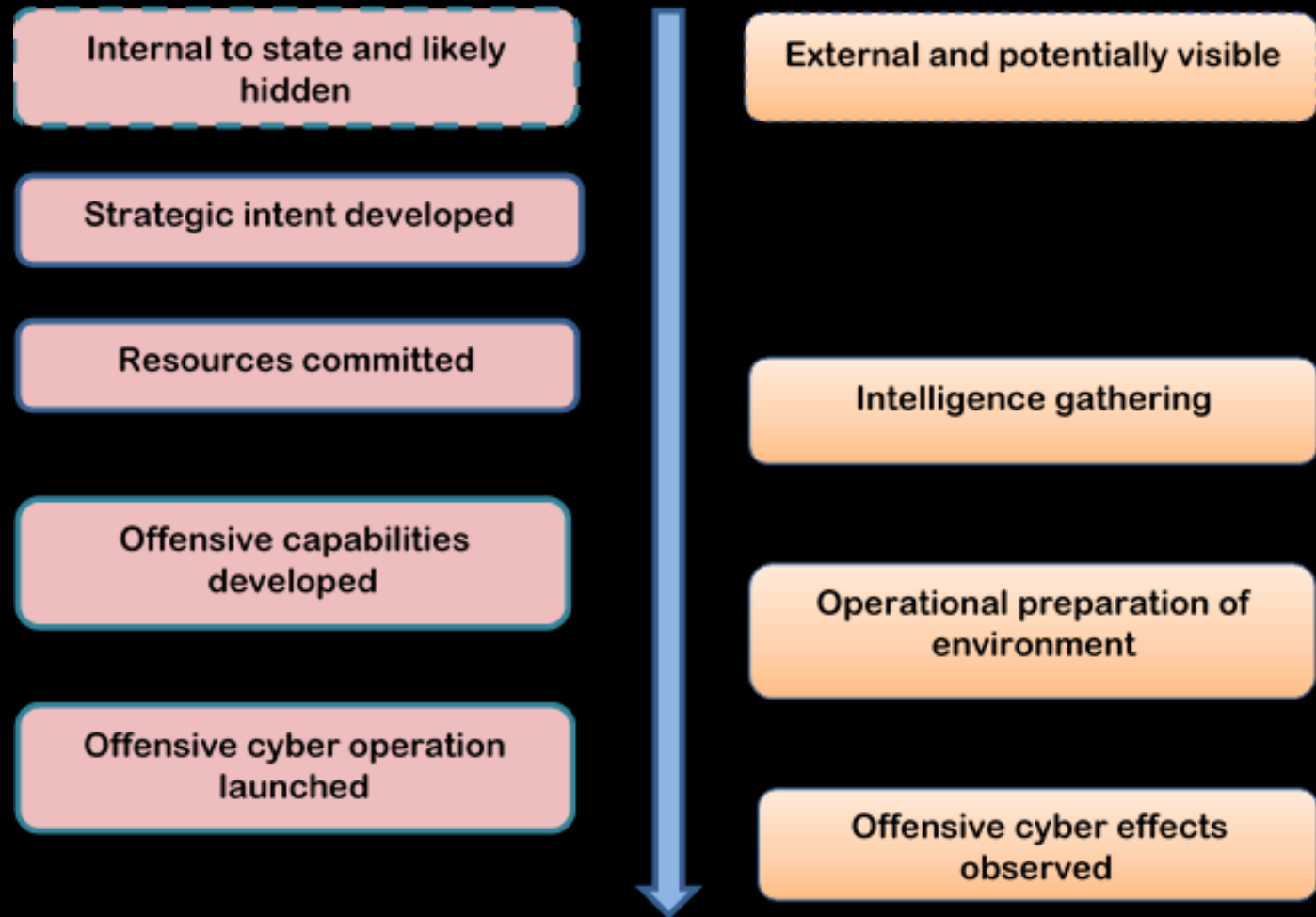
- Affect vulnerability and exploit markets
 - Vulnerability Equities Process
 - Encourage patching

Recommendation 2

- Promote focussed operations
 - Eg Stuxnet, Sony Pictures, Islamic State
 - Due diligence in containing effects
- Measure damage
 - Mostly based on public companies
 - Enables and justifies proportionate responses, encourages specific operations

Recommendation 3

- Invest in transparency and confidence building



Summary

Offensive cyber operations

**manipulate, deny, disrupt, degrade, or
destroy**

Talking about cyber weapons is pointless

Affect the offensive cyber environment