Cyber Security: What is it and why should I care?

Presentation to the
Executive Program on Tax and Digital Transformation

Craig Gillies
Director, Cyber Cooperation
Australian Department of Foreign Affairs and Trade

- The world has never been more connected.

- The ability of ensuring a safe, secure and trusted cyberspace is built on a strong partnerships – government, businesses and the community.

- The threats are real, and security needs to be baked into any digital process, not bolted on.

"Education has always been a profit-enabler for individuals and the corporation. Education, both conception and delivery, must evolve quickly and radically to keep pace with digital transition. Education is a part of the digital equation."
— Stephane Nappo, CISO *Société Générale*

The Internet – Problems and Promises

- The internet was posited to promote the democratization and pacification of the world.

- The internet has revolutionized our way of life – economy, communication etc

- The internet has also brought challenges
  - Conflict associated with control and regulation
  - Emergence of new threats
  - Debates about privacy, protection, and freedom of expression

- What can you do to influence, or control the ecosystem that surrounds you – to maximise the promises, but minimize the problems?

"What makes the internet work?"

Write your responses in the chat functionality

The Internet is like an onion – it has layers

Physical Layer – submarine and land-based cables, radio relays, computers etc.
- Can be built, altered, destroyed, or connected/disconnected from the network.

Logical Layer – services that facilitate transmission
- Can be intercepted, interrupted, or compromised.

Application Layer – the user friendly programs that allow you to use the internet (email, social media, Google)
- Can be exploited, capture data or manipulated.

Cognitive Layer – You! (users)
- Can be tricked, controlled, manipulated, addicted, exploited etc.

"What does C.I.A stand for?"

Write your responses in the chat functionality

"If security were all that mattered, computers would never be turned on, let alone hooked into a network with literally millions of potential intruders".

— Dan Farmer

Why should I care about cyber security?

- You are a **user of the internet**. You can be tricked, controlled, manipulated, addicted, exploited etc.

- You are an **expander of the internet**. You add or manipulate components of the networks of networks – increasing the attack surface.

- You are **reliant on the internet**. To make business grow and innovate, to create wealth (that can be collected/invested), to improve the lives of our citizens.
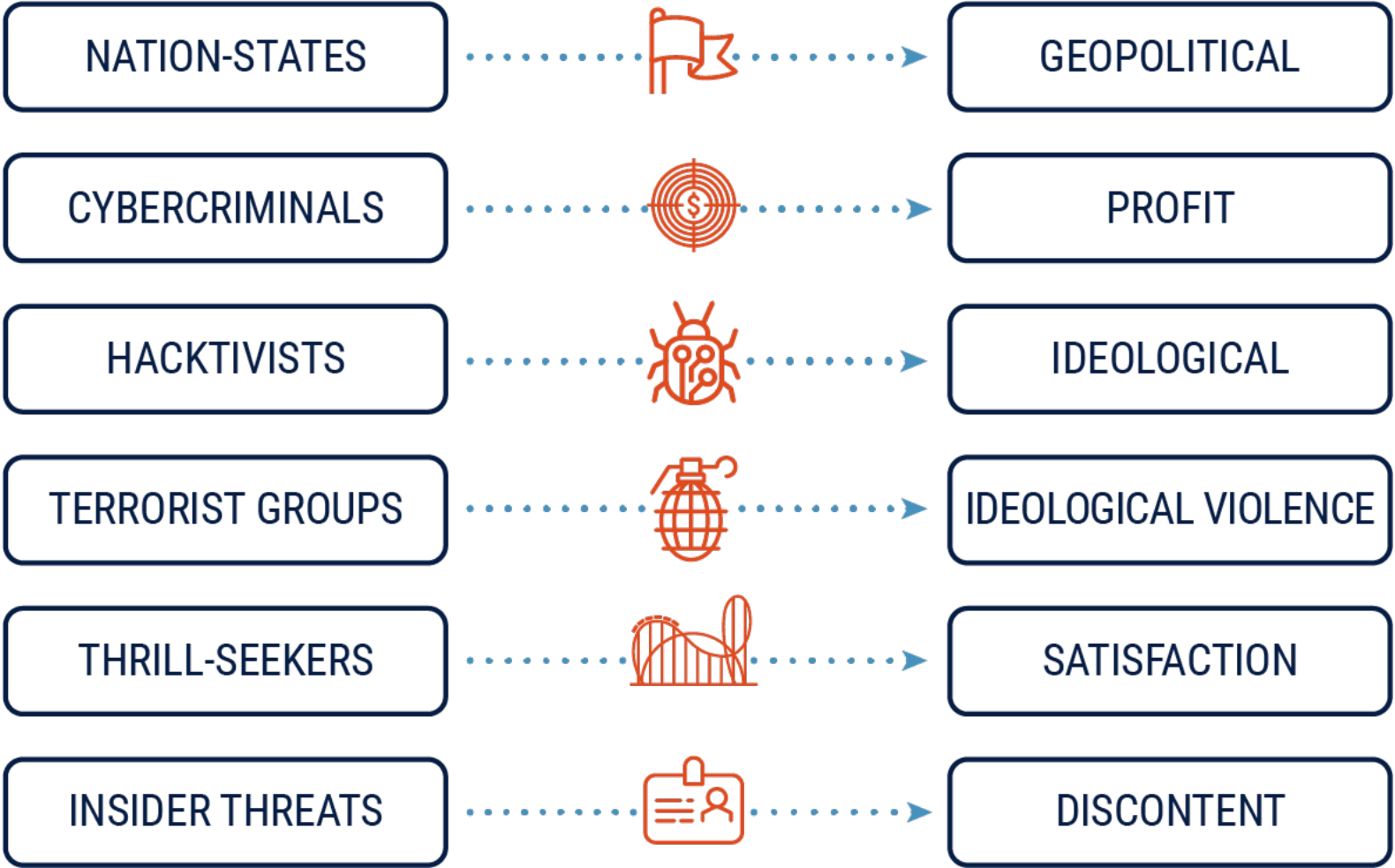
"Who are the main threat actors in cyberspace, and what are their motivations?"
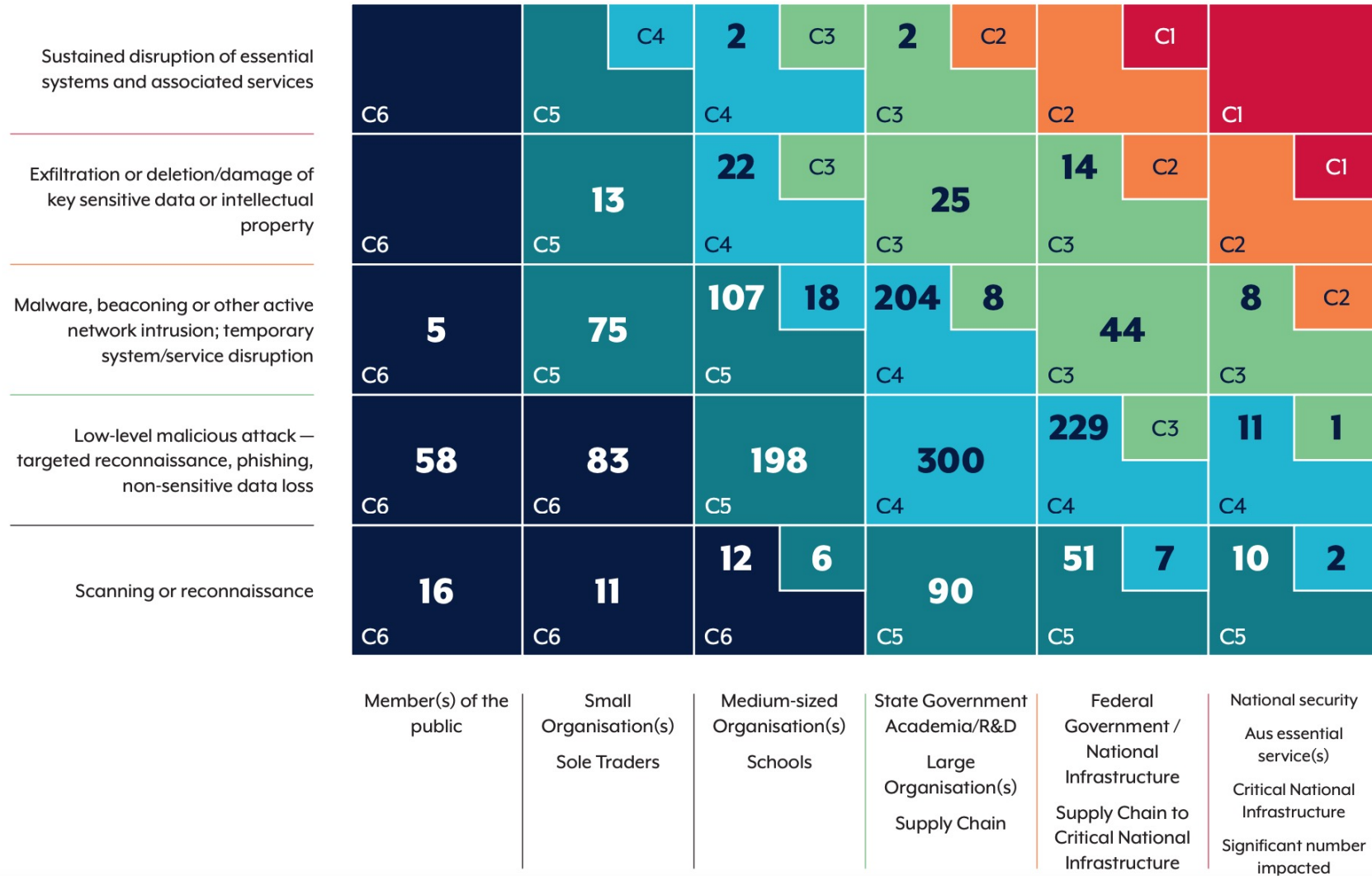
Write your responses in the chat functionality

Cyber Threat Actors

CYBER THREAT ACTOR

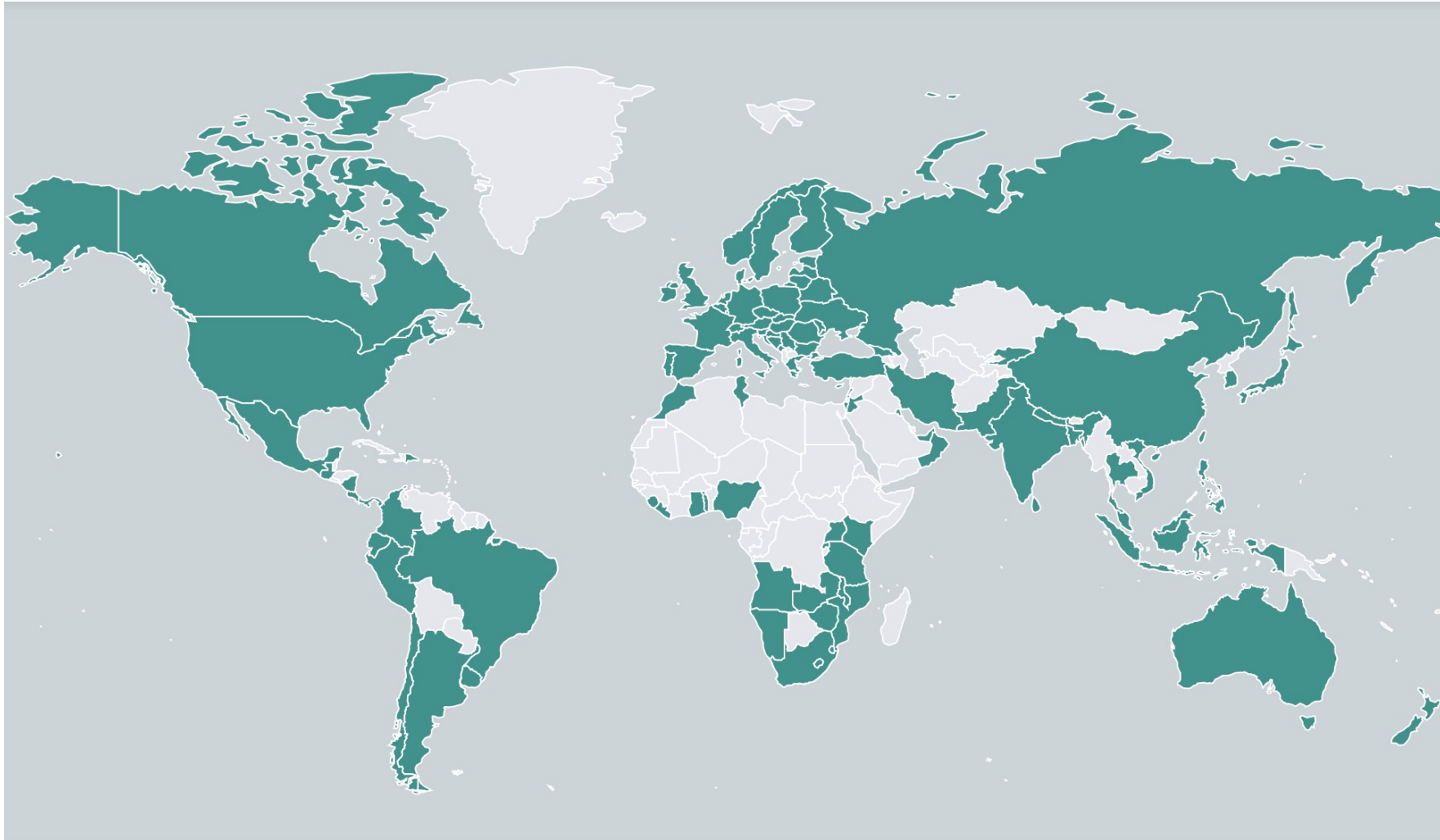|	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

The scale of the problem – view from Australia

Source: Australian Cyber Security Centre (ACSC)

The scale of the problem – Global

Source: Carnegie Endowment for International Peace

- **Scams** – Fake or scam emails and messages - called phishing - is still the number one way that cyber criminals are able to cause havoc .

- **Ransomware** – vicious form of malware, holds data and systems hostage unless a ransom is paid, often in bitcoin

- **Business Email Compromise (BEC)** - when criminals use email, instant message, SMS and social media to fraudulently access money or goods.

- **Targeting of Managed Service Providers (MSPs) and supply chains** - due to the nature of the services they provide and privileged access to customer networks

Key Takeaways

- **The internet is everywhere** – maximise its benefits and mitigate the risks. We are part of the ecosystem, protect what we have to protect others.

- **Cyber Security is a foreseeable business risk** – Know what your risk is. What systems have I got, who would want access to my system or my data, how could they gain access, what would the impact be?

- **Cyber Security baked in, not bolted on -** Expect that you will be a victim, and bake security into your digital transformation.

- **Prepare for the worst** – What will you do if you become a victim?

Questions?