Cyber defence tools: Operational to the strategic

A NATO CCDCOE perspective

Comdt Frank Hickey (OF-3) Irl

Researcher, Operations Branch

Dr Claire Kwan (LUX)

Researcher, Strategy Branch

30 October 2024

CCDCOE

Agenda

1. Cyber Defence tools – an operational perspective
2. Cyber Defence tools – a strategic and policy perspective

Cyberspace - Terms and definitions

ENISA Cyberspace Definition:

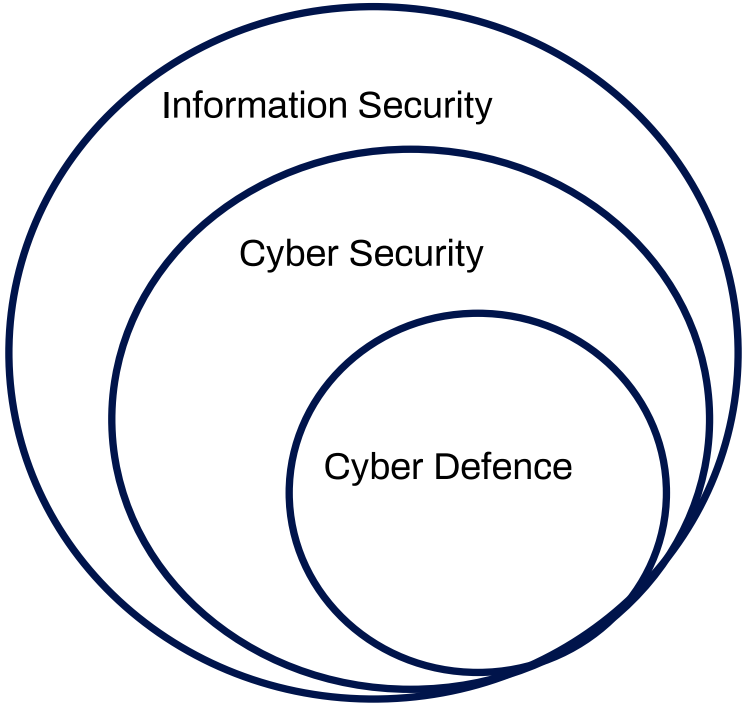
Cyber space is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information.

Cyber Security

Threat Agnostic

Cyber Defence

Threat Specific



Information Security

Cyber Security

Cyber Defence

Cyberspace – Understanding the Operational Environment

Cyber Defence: Cyberspace terrain Analysis.

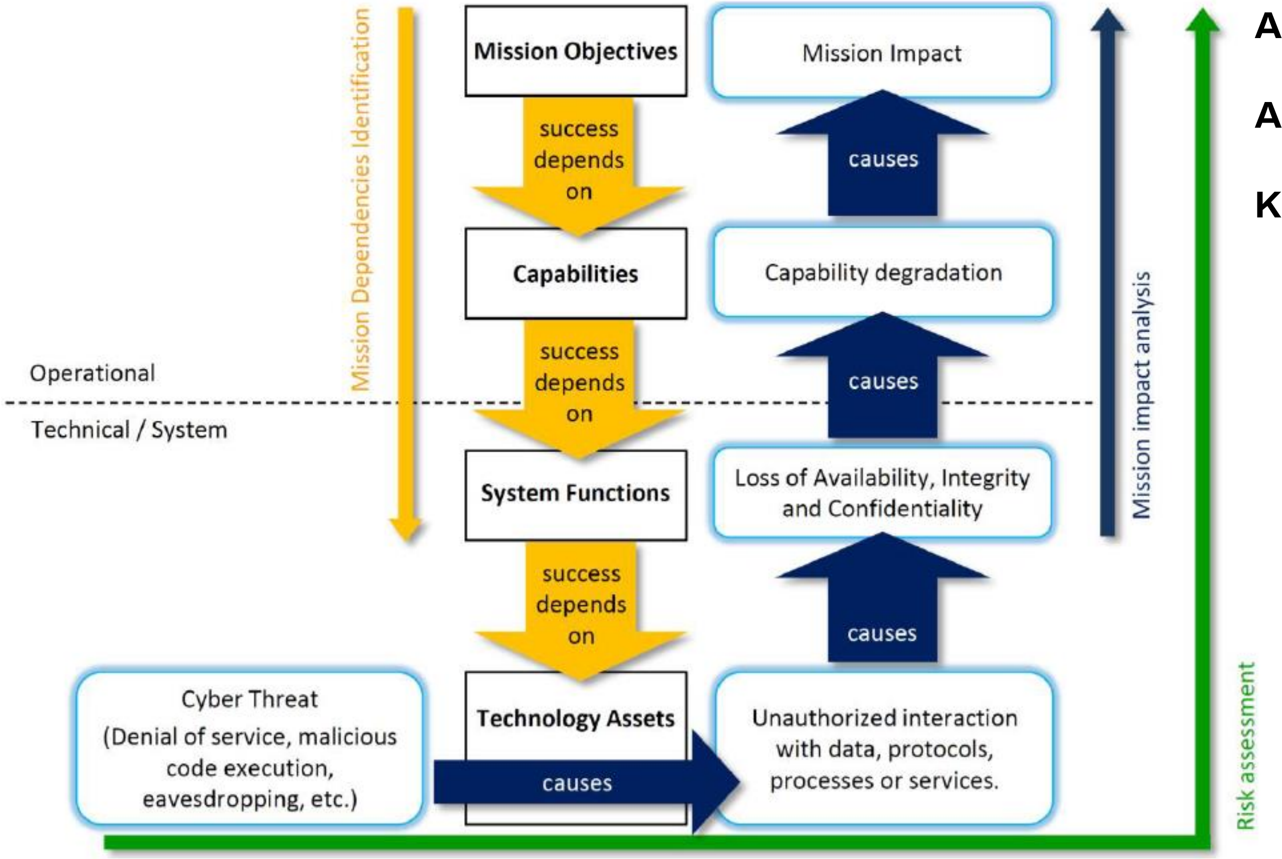


Figure 1: Cyber Mission Assurance model.

Area of Interest: Where should we be looking

Avenues of Approach: Ingress and egress points

Key Terrain In Cyberspace: Most important assets

TOOLS

- Network Mapping
- Network Traffic Analysis
- Vulnerability Scanning
- Cloud Asset Management tools

Cyberspace – Understanding the Operational Environment

Cyber Defence: Threat Actor Analysis

- A small number which specifically focus on our industry / successfully attacked
- Identify most likely Threat actors to target us for what reason and how

BACKGROUND
MOTIVATION
VICTIMS
TTPs

- **Background:** STATE – NON STATE actors in our Geographical area and industry
- **Motivation:** Geopolitical / Financial
- **Victims:** Cyber attacks in our Industry
- **TTPs:** How

TOOLS

Cyber Threat Intelligence Platforms: Which Focus on Threat Actors and Motivation

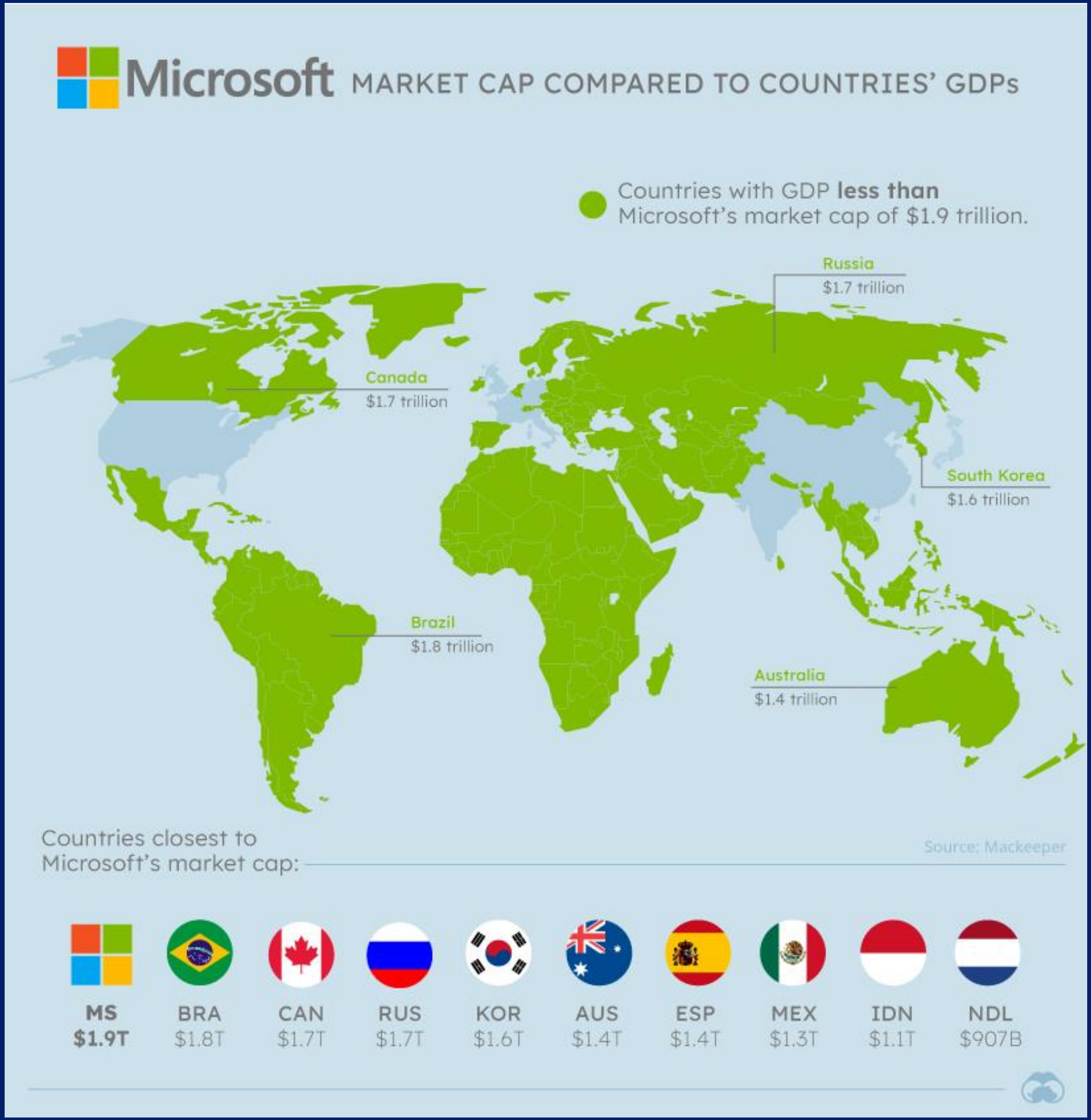
Reports which on Threat Actors motivation and intent

Cyber Defence: Strategy and policy considerations for the banking sector

1. Characteristics of cyberspace
2. Strategic considerations
3. Courses of action: A practical example
4. Takeaways

CCDCOE

Cyberspace characteristics



Countries closest to Microsoft's market cap:

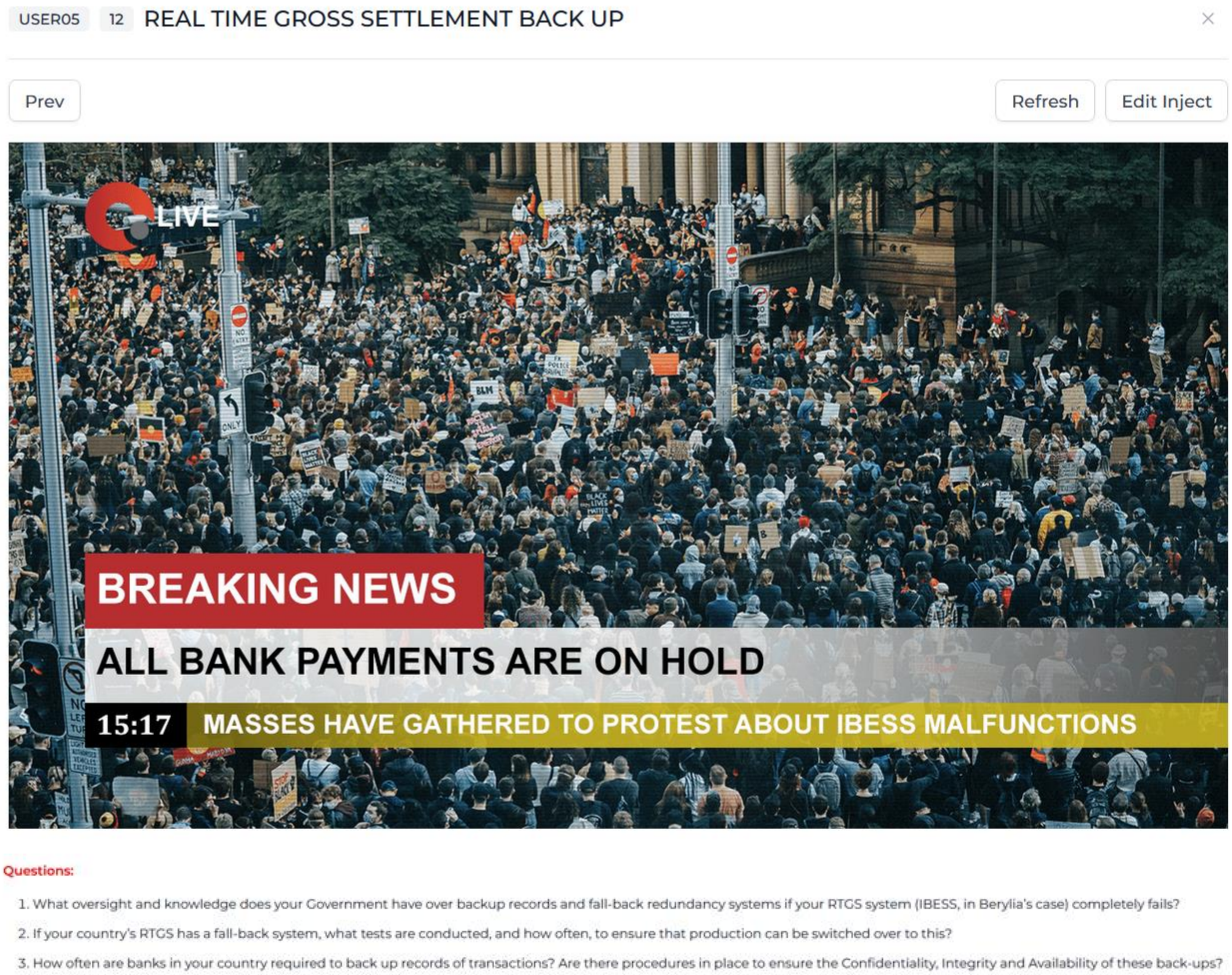
MS	BRA	CAN	RUS	KOR	AUS	ESP	MEX	IDN	NDL
$1.9T	$1.8T	$1.7T	$1.7T	$1.6T	$1.4T	$1.4T	$1.3T	$1.1T	$907B

CCDCOE

Strategic considerations

- → Cyberspace has no borders
- → No peace in cyberspace
- → Whole of society approach to defence

Exercising


USER05
12
×
Prev
Refresh
Edit Inject
LIVE
BREAKING NEWS
ALL BANK PAYMENTS ARE ON HOLD
15:17
MASSES HAVE GATHERED TO PROTEST ABOUT IBESS MALFUNCTIONS

REAL TIME GROSS SETTLEMENT BACK UP

Questions:

1. What oversight and knowledge does your Government have over backup records and fall-back redundancy systems if your RTGS system (IBESS, in Berylia's case) completely fails?
2. If your country's RTGS has a fall-back system, what tests are conducted, and how often, to ensure that production can be switched over to this?
3. How often are banks in your country required to back up records of transactions? Are there procedures in place to ensure the Confidentiality, Integrity and Availability of these back-ups?

Takeaways

→ Cyberspace cuts through everything

→ Your choices matter

→ Iterative exercising and mapping is a lifelong process

CCDCOE

NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Cmdt Frank Hickey frank.hickey@ccdcoe.org

Dr Claire Kwan claire.kwan@ccdcoe.org