RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: PST-W06

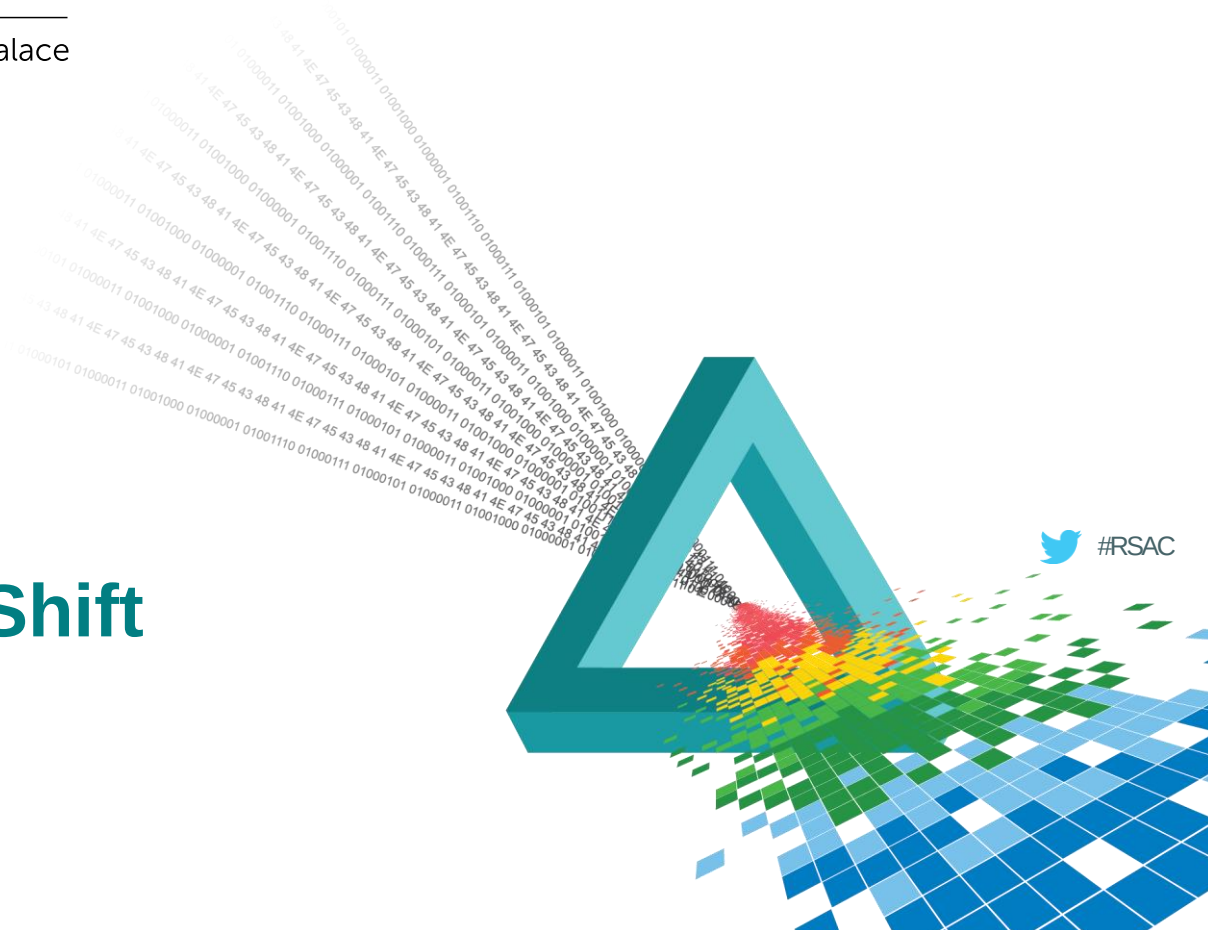
The Components of National and International Cyberspace Governance

Patrick MacGloin
ME Cyber Security Leader
PwC

Mohamed Al Jneibi
National Strategy & Policy
National Electronic Security Authority (NESA)

AGENDA

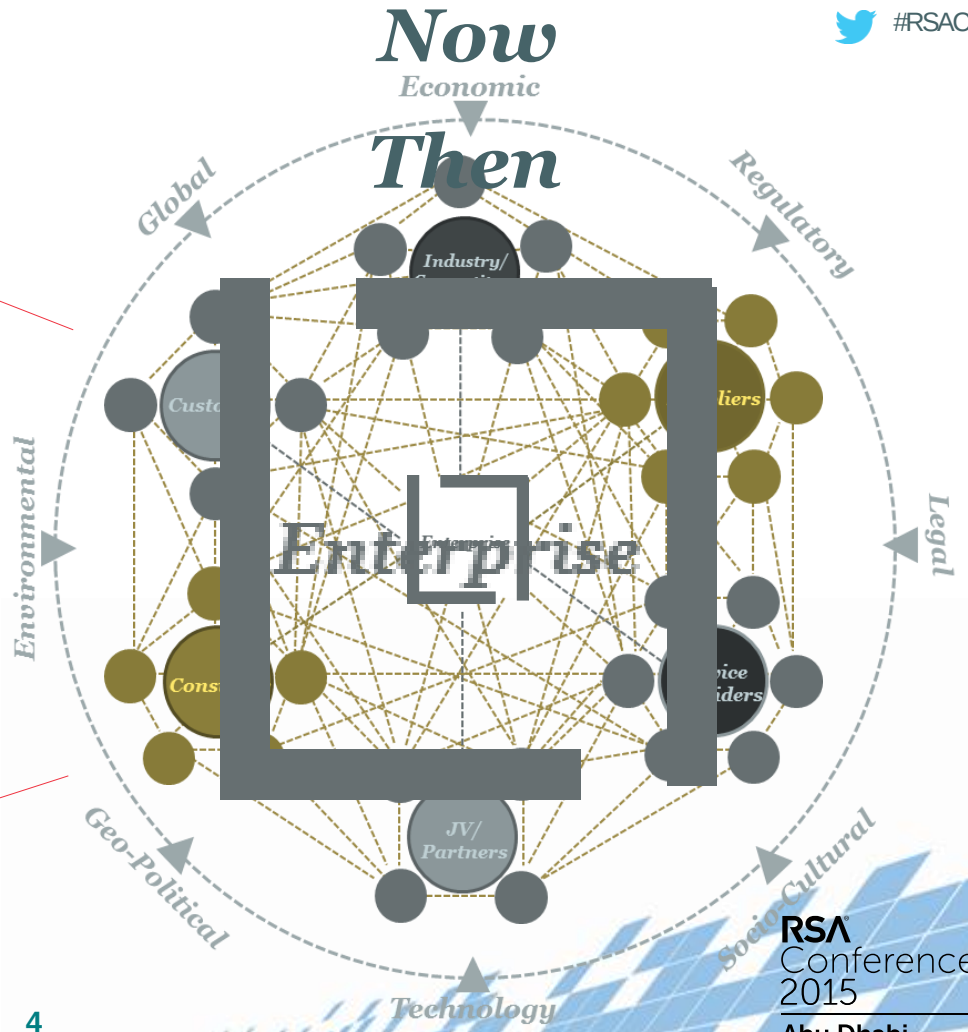
1. The Paradigm Shift
2. The Special Case of the UAE
3. The UAE Model



1. The Paradigm Shift

What is cyberspace?

- More data
- More actors
- Greater connectivity
- Porous perimeters
- External drivers



Levels of analysis

Operational:

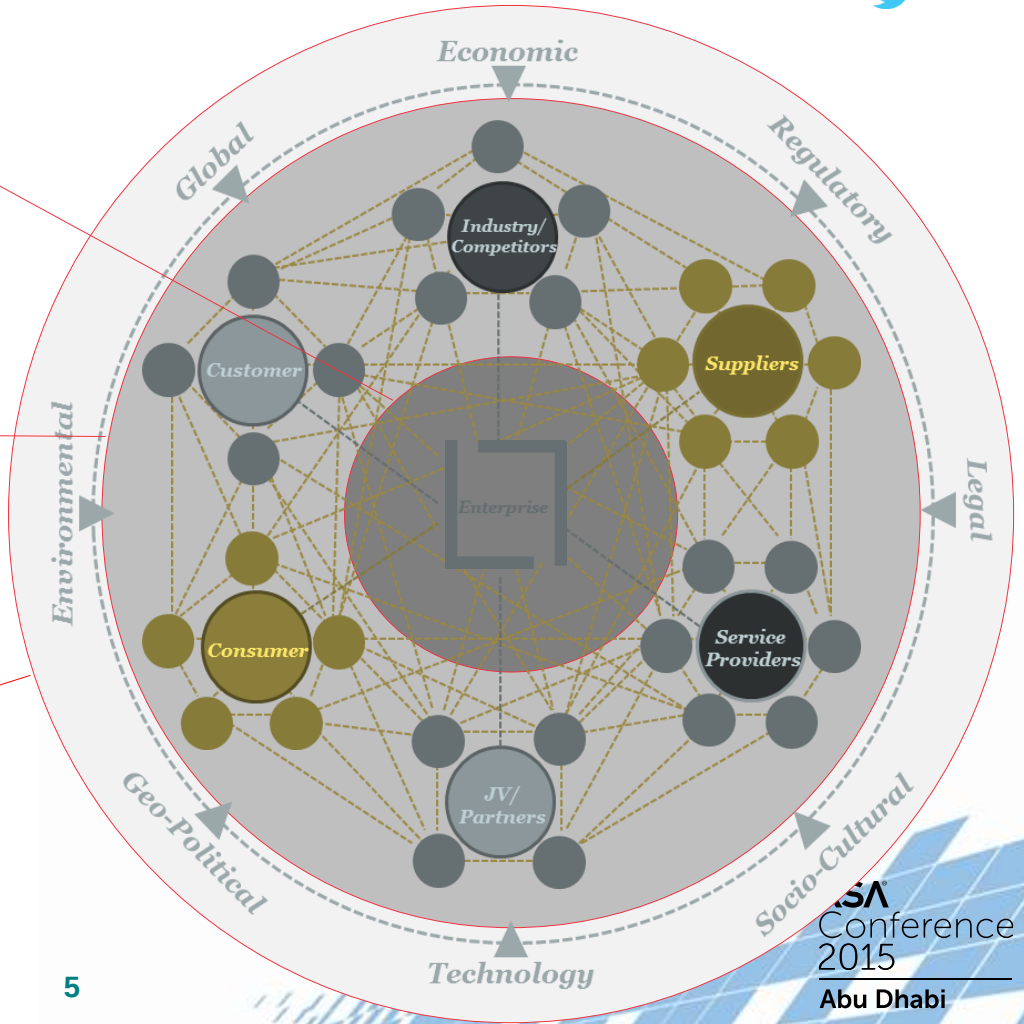
- Operational security
- Asset protection
- Awareness & culture

Tactical:

- Third parties
- Data sovereignty
- Reputation

Strategic:

- Regulatory agendas
- Geo-political conditions
- Technology & demography



International models

Based on Drake & Wilson, 2008 and Choucri, 2012

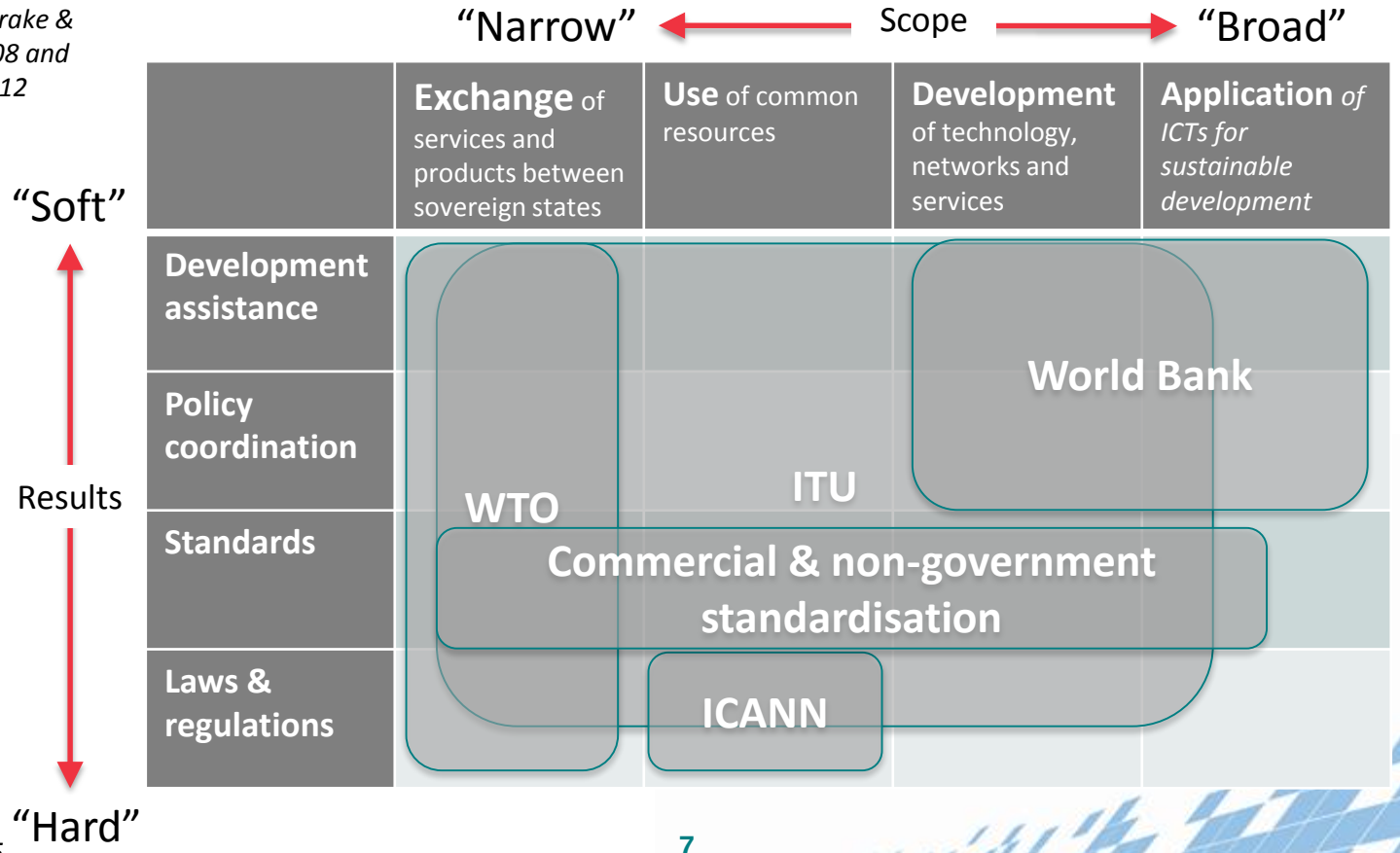
"Narrow" ← Scope → "Broad"

"Soft" ↑ Results ↓ "Hard"

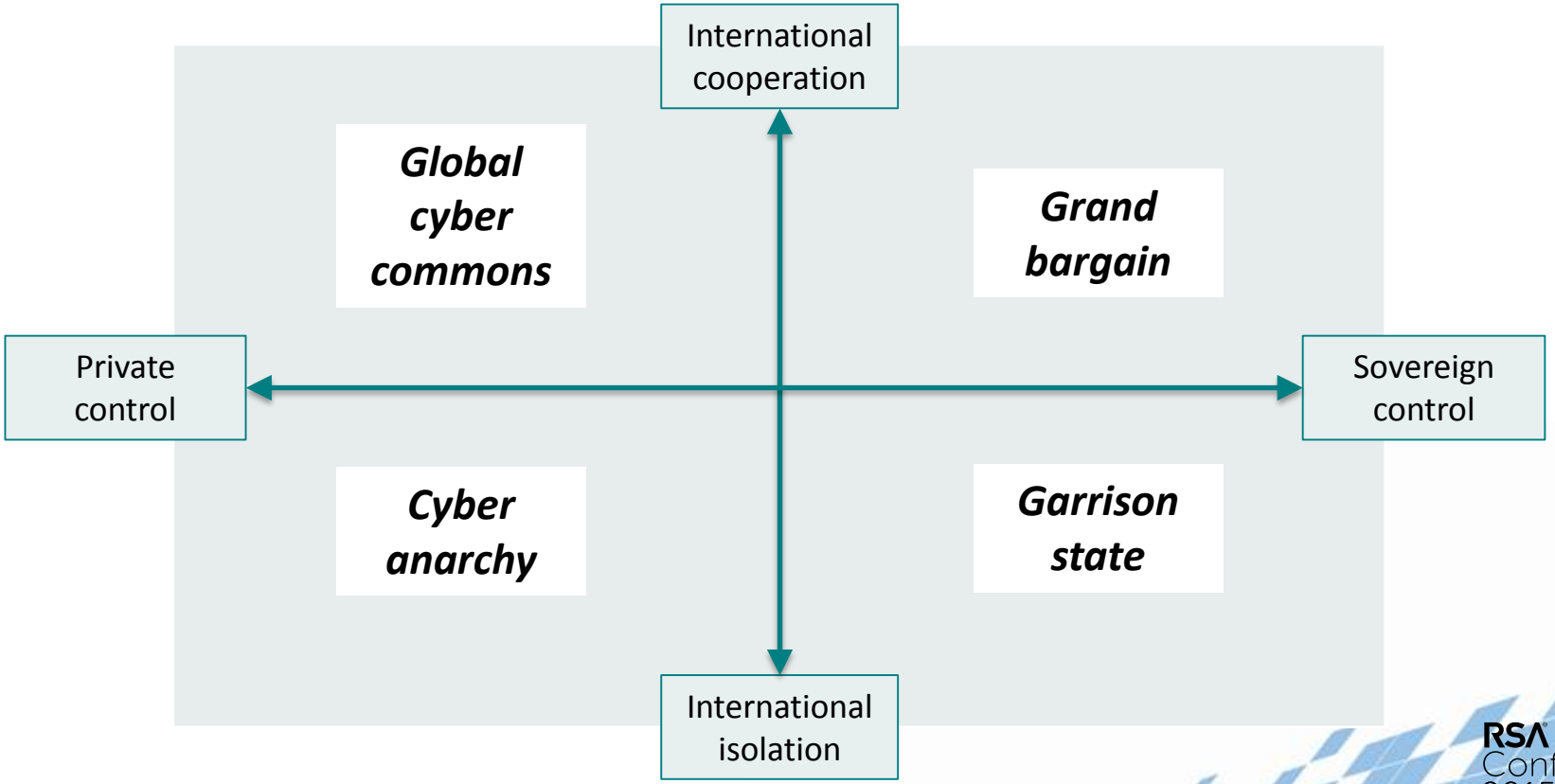
	Exchange of services and products between sovereign states	**Use** of common resources	**Development** of technology, networks and services	**Application** *of ICTs for sustainable development*
Development assistance				
Policy coordination				
Standards				
Laws & regulations				

International models

Based on Drake & Wilson, 2008 and Choucri, 2012



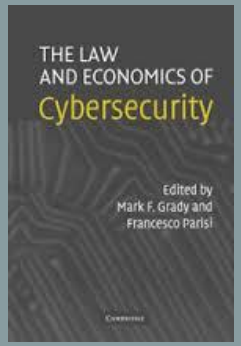
The national balancing act



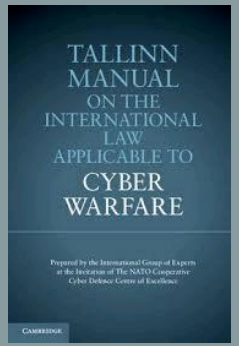
National governance models

Several international (supra-national) frameworks for cyber security governance, across academic to applied levels of adoption.

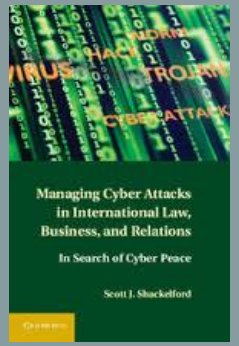
Declaration of cyber independence



Domain specific



Doctrine



Polycentric models

International governance models

National governance frameworks

OECD guidelines for cyber resilience

Guidelines

Key components	Outline
National strategy	Coordination and contextualisation of cyber related issues within context of the broader national security agenda
Legal foundations	The legal mechanisms that clearly identify responsibilities, minimum levels of resilience expected from critical providers, and definitions
Identified authorities	Clear definitions of national entities and their spheres of responsibility
National incident response	National level monitoring, response and coordination of events
Industry/ government partnerships	Acknowledgement that cyber security and resilience cannot be delivered by government alone: sector and national level collaboration
Information exchange mechanisms	Sharing of threat intelligence at international, national, sector and commercial level

National governance frameworks

OECD guidelines for cyber resilience

Guidelines	Key components	Examples
	**National strategy**	Distributed: eg Canada, UK Sector specific: eg USA
	Legal foundations	Mandated requirements: most OECD Voluntary guidelines/emerging regulation: eg EU GDPR
	Identified authorities	Coordination Leadership
	National incident response	Federal CNIP
	Industry/ government partnerships	Sector level National level
	Information exchange mechanisms	Sector National and international

2. The special case of the UAE

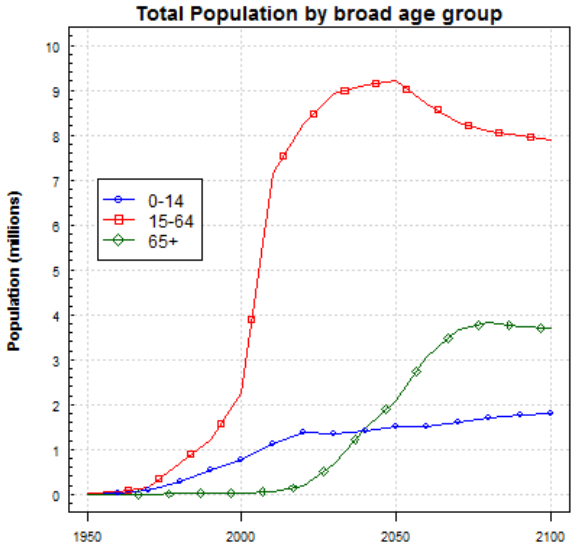
Key factors in the UAE

- Demography
- Technology adoption
- Governmental adoption

Key factors in the UAE

- Demography
- Technology adoption
- Governmental adoption

UN population forecast for UAE
2014



UN Department of Economic and Social Affairs, 2015

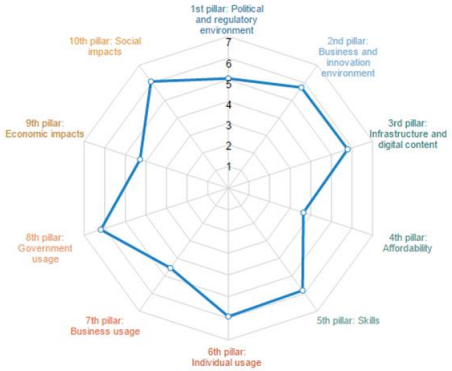
Key factors

- ***Growing young population***
- ***Increased familiarity with technology***
- ***Generational and cultural considerations***

Key factors in the UAE

- Demography
- Technology adoption
- Governmental adoption

23rd globally in 2015
24th in 2014



Key strengths

2nd ***Business & innovation environment***
2nd globally

2nd ***Government usage***

2nd ***Social impacts***

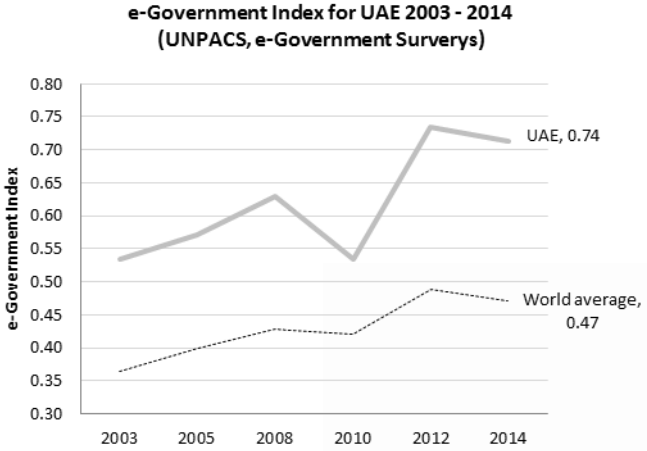
WEF, Network Readiness Index, 2015

Key factors in the UAE

- Demography
- Technology adoption
- Governmental adoption

ITU, United Nations Public Administration and Development Management, 2015

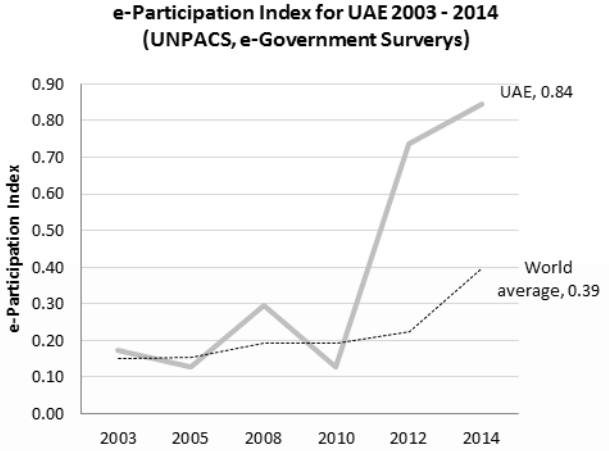
UN eGovernment Index



Online services & telecom infrastructure

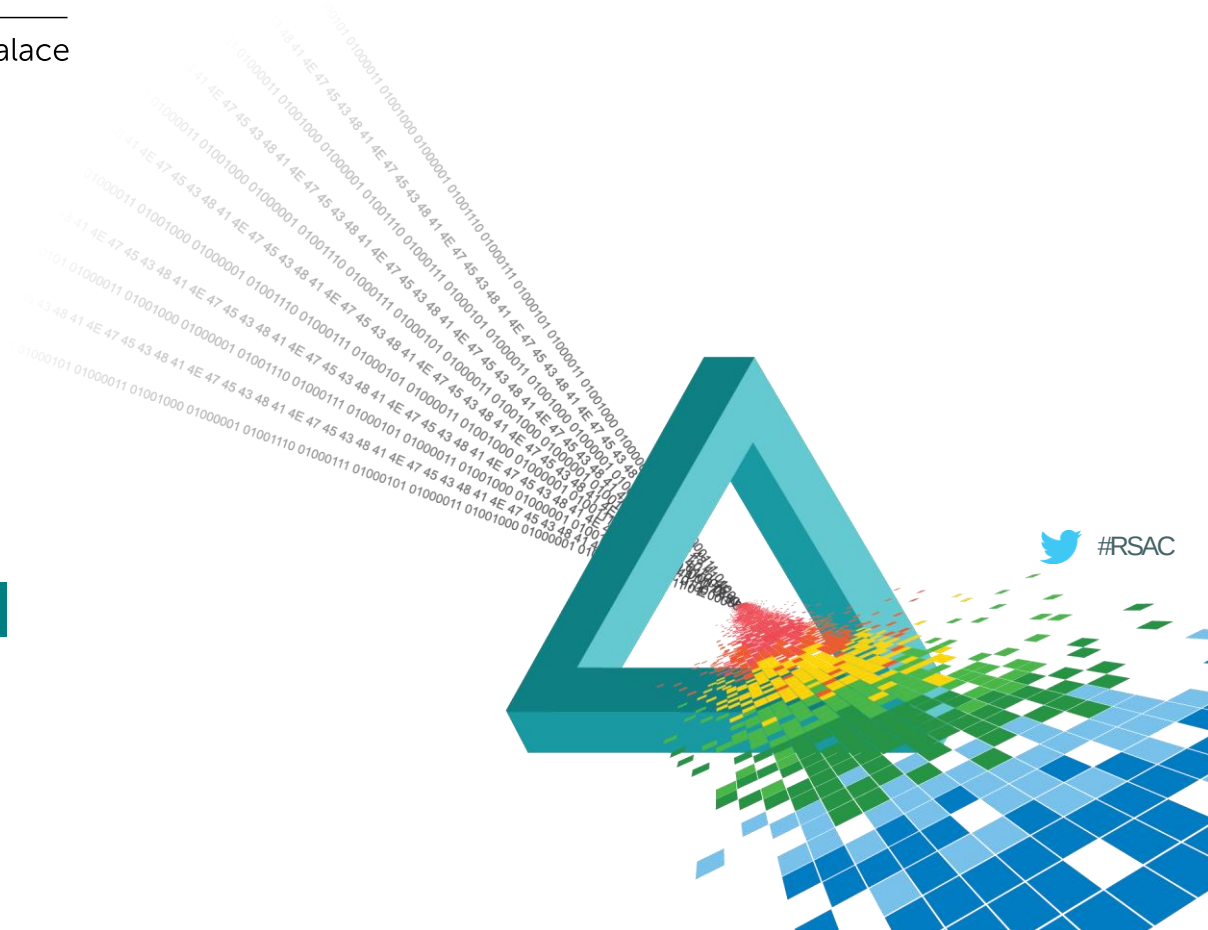
Human capital

UN eParticipation Index



UAE is a top performers

3. The UAE Model



NESA Mandates

DEFEND & RESPOND

PROTECT CRITICAL INFRASTRUCTURE

IMPROVE THREAT AWARENESS

DEVELOP HUMAN CAPITAL

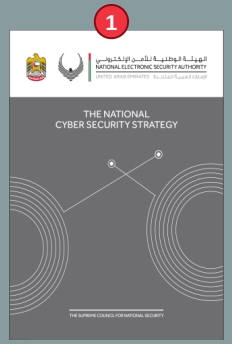
DEVELOP TECHNICAL CAPABILITIES

COOPERATE WITH PARTNERS

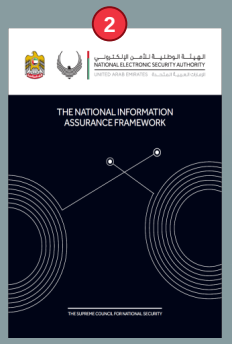
Foundational [Capstone] Policies

As part of its initial efforts, NESA developed and issued the National Cyber Security Strategy, key National Policies, as well as the UAE Information Assurance Standards

Official Policies and standards

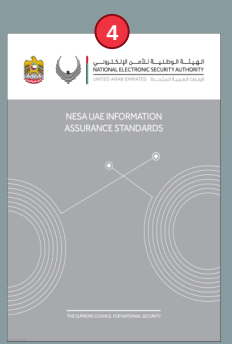


National Cyber Security Strategy



National Information Assurance Framework

Critical Information Infrastructure Protection Policy

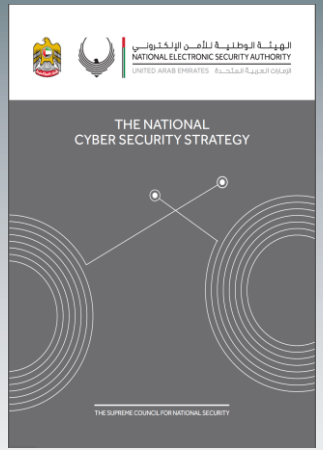


UAE Information Assurance Standards

The UAE's National Cyber Security Strategy

National Cyber Security Strategy | National Information Assurance Framework | Critical Information Infrastructure Protection Policy | UAE Information Assurance Standards

Strategy

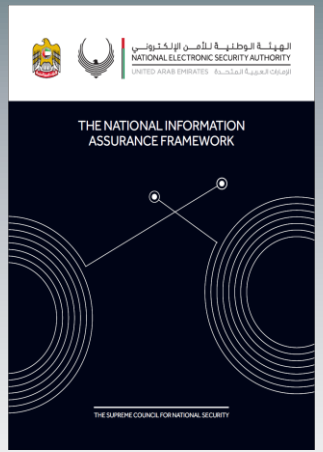


Objectives	Purpose and Main Components
Prepare and Prevent	Strengthen the security of UAE cyber assets and reduce corresponding risk levels
Respond and Recover	Manage incidents to reduce impact on society and the economy
Build National Capability	Cultivate cyber security research and innovation and develop UAE's workforce to meet cyber security needs
Foster Collaboration	Foster collaboration between national and international stakeholders to catalyze cyber security efforts
Provide National Leadership	Provide national leadership to orchestrate local and emirates cyber security initiatives at the national level

The National IA Framework

National Cyber Security Strategy	**National Information Assurance Framework**	Critical Information Infrastructure Protection Policy	UAE Information Assurance Standards

Framework



Objectives	Purpose and Main Components
1. Entity Context	Risk-based approach to identifying and protecting key information assets within an entity
2. Sector / National Context	Value-add components that establish the links from an individual entity to the sector and national context
3. Information Sharing	Primary mechanism for entities to exchange information with external actors
4. National Standards	Common, sector-specific, and product / service-specific standards applicable across all stakeholders
5. National IA Governance	Management elements needed to successfully implement the national IA framework

UAE CIIP Policy

National Cyber Security Strategy	National Information Assurance Framework	Critical Information Infrastructure Protection Policy	UAE Information Assurance Standards

Policy

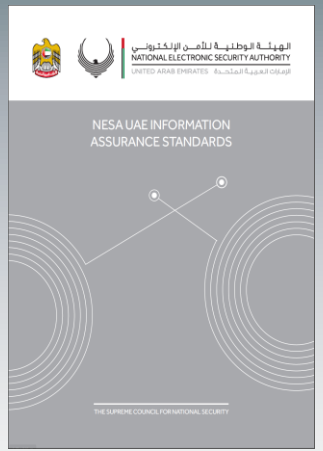
Objectives

- Sets the course for implementing Critical Information Infrastructure Protection in UAE
- Establish a common national approach to identifying CIIs
- Point out to cyber security requirements for CIIs and establish compliance need
- Assigns key roles and responsibilities to the relevant stakeholders
- Establish an approach for fostering engagement and collaboration

UAE IA Standards

National Cyber Security Strategy | National Information Assurance Framework | Critical Information Infrastructure Protection Policy | **UAE Information Assurance Standards**

Strategy



Objectives	Purpose and Main Components
Raise Minimum Security	provide requirements to raise the minimum level of protection of information systems and supporting systems
Prioritize Implementation	Enable a risk-based approach for the implementation of these Standards
Outline Roles and Responsibilities	Outline clear vision of roles and responsibilities of main stakeholders at national, sector and entity levels
Complement Other Standards	Complement entity's existing information security standards implementation
Unified Source of Standards	Provide a unified source of information security standards across all sectors in the UAE

Basis of UAE IA Standards

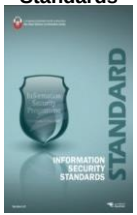
Analyzed IA Standards

ISO 27001

ISO 27002

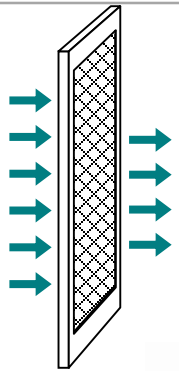
NIST SP 800-53

ADSIC InfoSec Standards



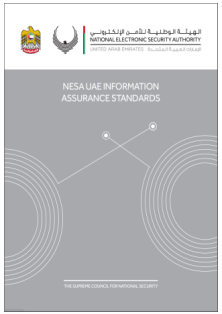
SANS 20

Analyzed Dimensions



1. Breadth of Controls
2. Depth of Controls
3. Ease of Adoption
4. Prioritization for Implementation
5. Recognition and Footprint

Analysis Outcome



A custom UAE IA Standard was developed leveraging strength areas among the analysed standards

Take-Away Points

- A national strategy on cybersecurity should emphasize (or acknowledge) the importance of technology enablement
- Information Assurance should be seen within the context of the participating entities
- In the case of the UAE, Information Assurance initiatives across key sectors is jointly being lead by the relevant sector regulators
- Any successful national program should integrate a collaborative risk based approach towards better adoption of IA practices

Thank You