The DST-funded Information Security Centre of Competence

Dr Barend Taute

ISSA 2009

6 July 2009

our future through science

Outline of the presentation

- Threats and vulnerabilities in Cyberspace

- The Information Security Centre of Competence Concept
- Three broad Market Opportunities defined
- Outcomes and governance

- *Invitation to participate*

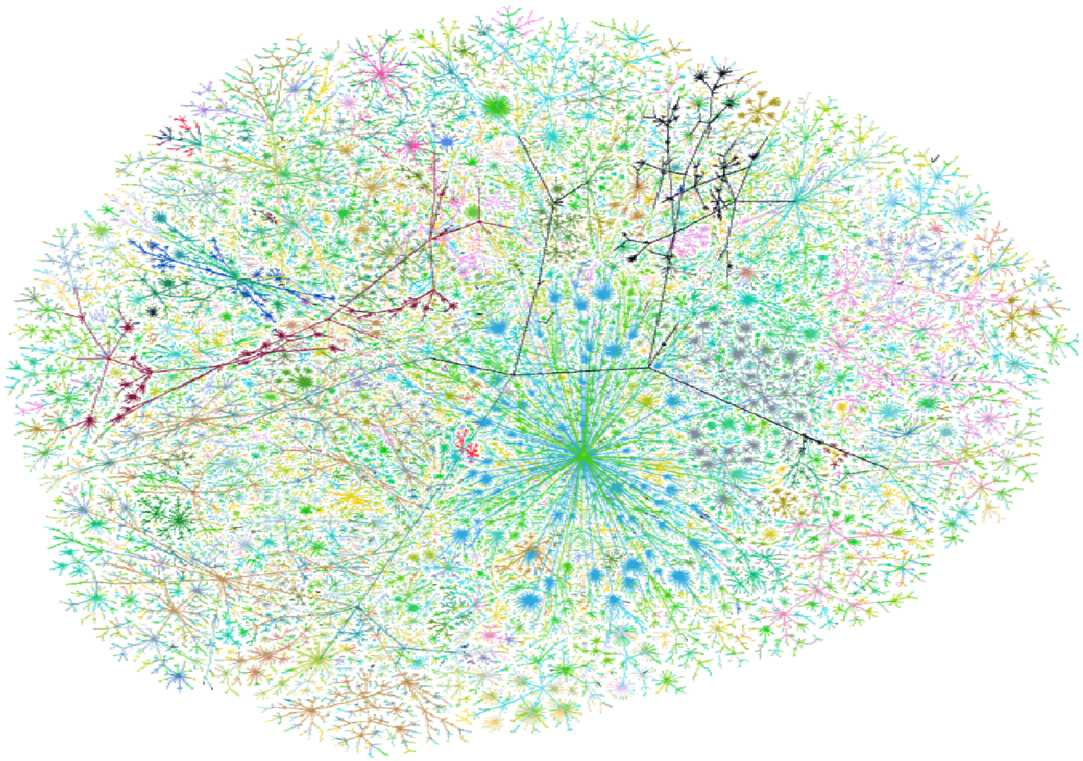
Cyber Threats – to all spheres of life

- **National Security**
- **Industry**
- **e-Government**
- **Personal**

our future through science

Reliance in a world of assumed trust

The Internet:



We need:
- *Availability*
- *Integrity*
- *Confidentiality*

Because we want
- *Computing*
- *Speed*
- *Simplicity*
- *Gadgets*
- *Convenience*
- *Information*
- *Low cost*

– now a network of networks linking more than 300 million computers worldwide – was designed in a spirit of trust

CSIR
our future through science

Cyberspace vulnerabilities and threats

- *"The worldwide information infrastructure is today increasingly under attack by cyber criminals and terrorists — and the number, cost, and sophistication of the attacks are increasing at alarming rates.*

- *With annual damage around the world now measured in billions of US dollars, these attacks threaten the substantial and ever-growing reliance of commerce, governments, and the public upon the new technology to conduct business, carry messages, and process information."*

  - [From a book titled The Transnational Dimension of Cyber Crime and Terrorism edited by Sofaer and Goodman].

CSIR
our future through science

Examples of Cyber Attacks

- Estonia “Web War ONE”
  - Apparent political motives
  - Distributed Denial of Service on electronic infrastructure
  - Only coordinated international efforts could stop it

- Gary McKinnon (2001-2002)
  - Infiltrated multiple US government computers searching for proof that aliens exist
  - Shut down the entire US Army's Military District of Washington network

- Vitek Boden (2000)
  - Attacked sewage flow control systems
  - Raw sewage overflows on Sunshine coast (Brisbane)

- Palestinian Supporters Hack NATO and U.S. Army Sites (2009)
  - Joint Force Headquarters
  - National Capital Region
  - Northern Command

Threats and challenges in cyberspace

Cyberspace encompasses all forms of networked, digital activities.

- ***Cyber Vulnerabilities***
  - = viruses, worms, trojans, phishing, denial of service, interception, intellectual property, spam, information destruction, private info, credit card skimming, …
- ***Cyber Crime***
  - = committed in cyberspace or with cyber tools, theft, fraud
- ***Cyber Terrorism***
  - = Malicious acts for ideological reasons
- ***Information warfare***
  - = Offensive or defensive cyber attacks

our future through science

ICT Related Risks span all levels

- National Security
  - Secrets, military operations, critical infrastructure
- Government
  - eServices, communications, corruption
- Industry
  - Sabotage, espionage, fraud, theft, embarrassment
- Society
  - Banking fraud and theft, identity management, scams, extortion

ICT risks to:

- **Privacy**
  - Balance between security and privacy of identity; "social engineering" is often the weakest point
- **Trust**
  - Trust is at the heart of remote transactions - whether E-commerce retail transactions or state-society relations in an e-democracy
- **Interdependence**
  - The complex, interconnected socio-technical systems that are emerging as a result of networking and computerisation.

Information security

is an all encompassing term that refers to the security of the information systems that are used and the data that is processed.

The three main objectives are:

- **Confidentiality**
  - to keep information away from unauthorized people or systems
- **Integrity**
  - that data cannot be changed or modified without authorization
- **Availability**
  - to prevent losing data or systems so that it will be available when needed

South Africa has a track record of Infosec innovations

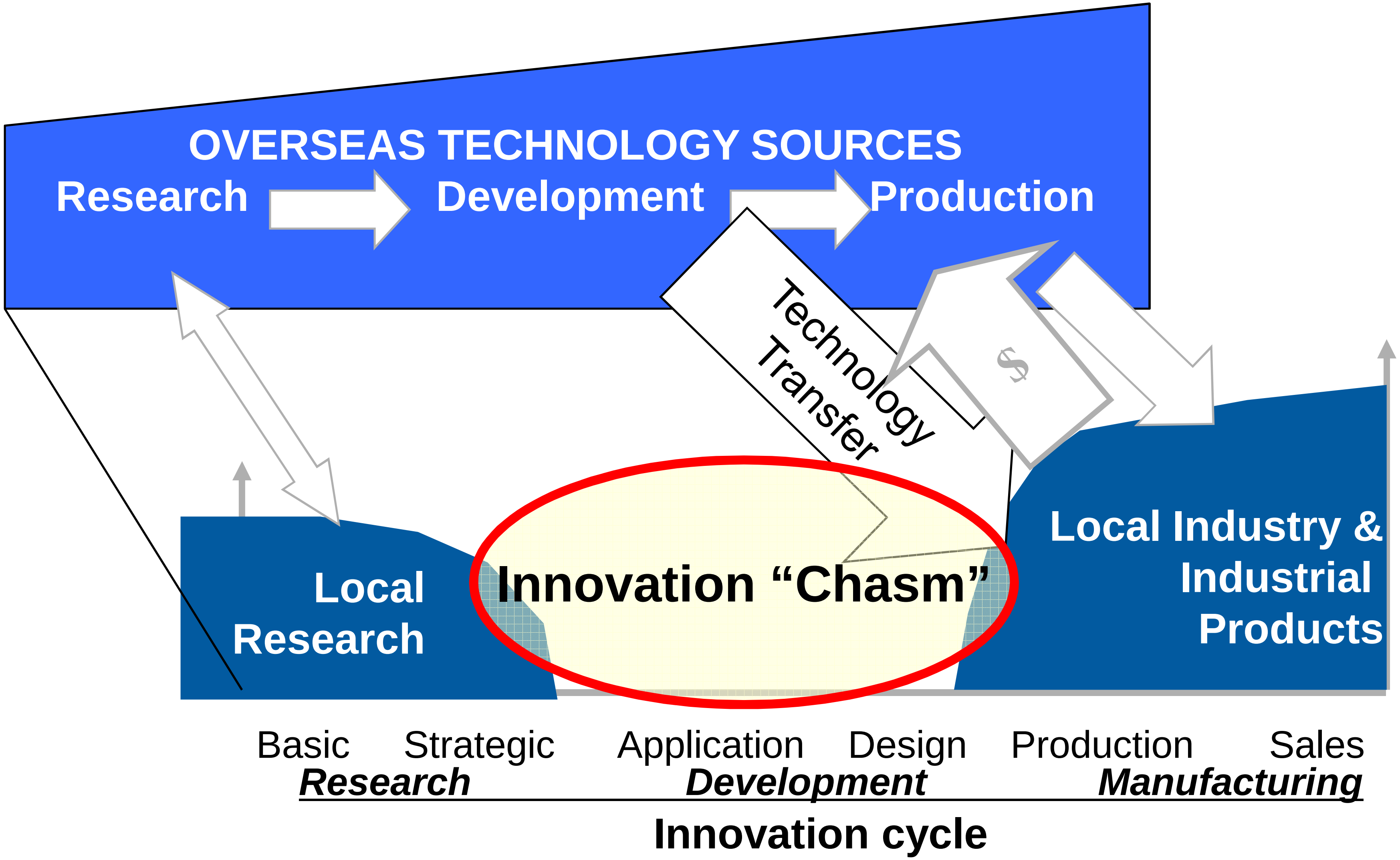
- Cryptography solutions
- Network security systems
- DSTV/Multi-choice pay-TV system
- Thawte consulting (Shuttleworth) – PKI certificate system for internet
- Prepaid electricity
- Cellphone banking
- RFID solutions
- Etc ….

The Technology Innovation Agency ACT (Dept of Science & Technology)

The TIA Act

"The object of the Agency is to support the State in <u>stimulating and intensifying technological innovation</u> in order to improve economic growth and the quality of life of all South Africans <u>by developing and exploiting technological innovations</u>"

Why TIA?



OVERSEAS TECHNOLOGY SOURCES

Research → Development → Production

Technology Transfer

$

Local Research

Innovation “Chasm”

Local Industry & Industrial Products

Basic Strategic Application Design Production Sales

Research *Development* *Manufacturing*

Innovation cycle

CoEs vs. CoCs

- **A Centre of Excellence** *comprises a consortium of HEIs with a clear research agenda in pursuit of knowledge generation and its possible application in response to a societal challenge*
  - Outcomes includes among others: New Knowledge, PhD's, Post Doctoral, Publications, Patents etc.

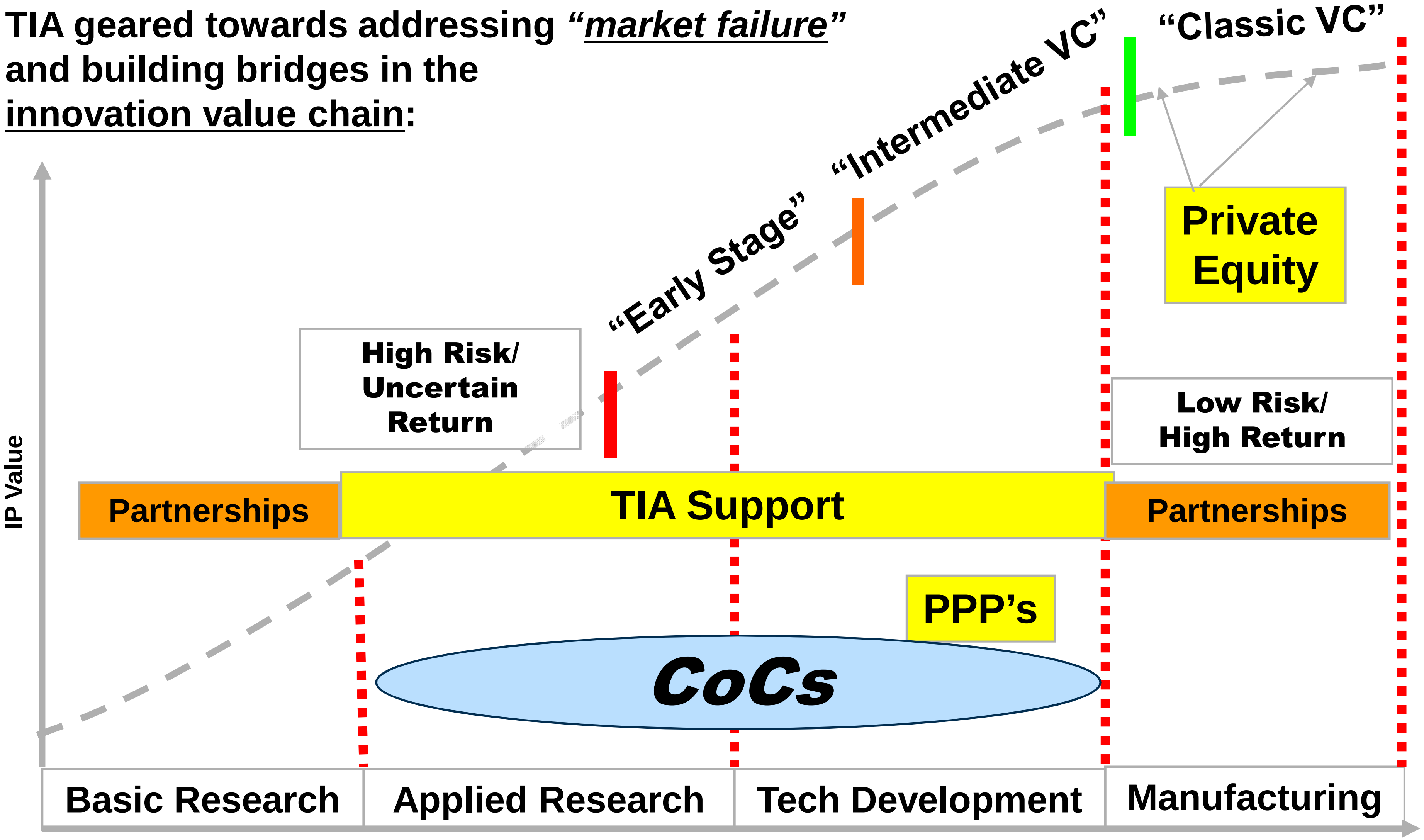
- **Centre of Competence** : *A form of university, industry, and research institutions alliance that do mainly applied research and development that ultimately produce new innovations.*
  - *Outcomes includes among others: new technology based products and services, innovations, Intellectual Property (which maybe further developed and or licensed), new technology based enterprises*

Centre of Competence Principles

- The CoC relies on harnessing the resources, capabilities and synergies of all, with clear market focus and innovation research objectives in pursuit of <u>products and services</u>
  - Must have commercial or public-good potential
  - Must respond to market opportunity/failure and/or socio-economic challenges

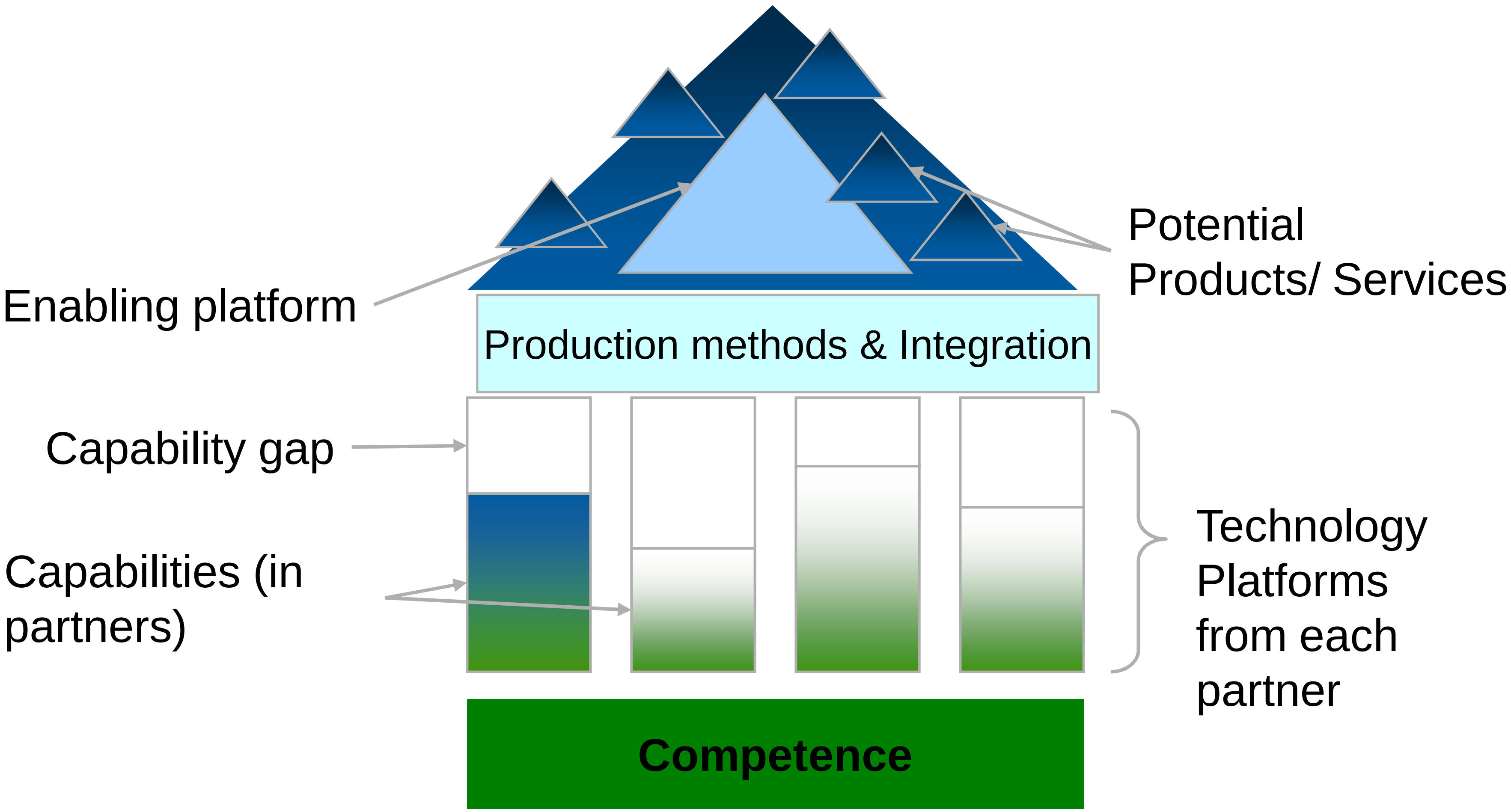
- Guided by national priorities across government

TIA geared towards addressing *"market failure"* and building bridges in the innovation value chain:



The TIA will focus its financial and non-financial offerings along the *innovation chasm,* and will operate with the required flexibility across the innovation value chain through partnerships

CoC Option 4 – Enabler



Potential Products/ Services
Enabling platform
Production methods & Integration
Capability gap
Capabilities (in partners)
Technology Platforms from each partner
Competence

Motivation for an Information Security CoC

- Increased need for Information Security
  - Rate of new ICT technologies
  - Increasing dependence on ICT
  - Growing understanding **opportunities/threats**

- No coordinated capacity to respond effectively to national-scale incidents and attacks
  - Affecting government, industry, citizens, critical infrastructure
  - such as the large scale attacks aimed at the critical electronic infrastructure of Estonia during April/May 2007.

- Innovation rates and knowledge flows from research to industrial and economic activities have slowed down
  - The full potential of South African expertise is not being realised.
  - Innovation chasm to be overcome
  - ICT is too valuable to depend on overseas solutions
  - We can do it!

The Information Security Centre of Competence Concept

our future through science

The Department of Science and Technology approved the establishment of an

Information Security Centre of Competence

with the coordinating hub at the Meraka Institute (CSIR ICT unit) and

direct supervision and management by the soon to be established **Technology Innovation Agency (TIA)**

The main purpose of ISCOC:

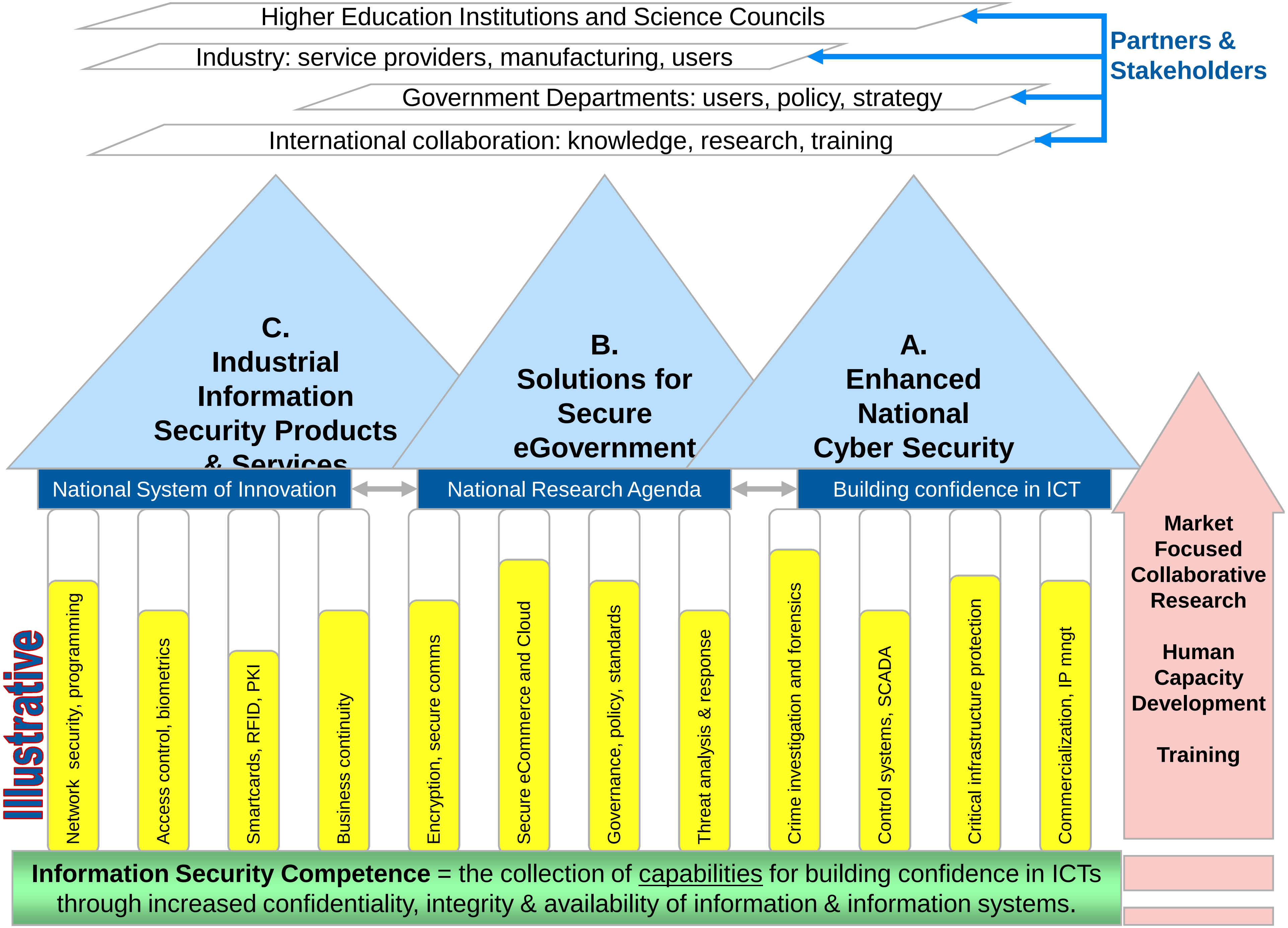
collaborative development of

technological competencies

and R&D

leading to commercialisation and transfer of R&D outputs

in Information Security.



Higher Education Institutions and Science Councils

Industry: service providers, manufacturing, users

Government Departments: users, policy, strategy

International collaboration: knowledge, research, training

Partners & Stakeholders

C. Industrial Information Security Products & Services

B. Solutions for Secure eGovernment

A. Enhanced National Cyber Security

National System of Innovation

National Research Agenda

Building confidence in ICT

Illustrative

- Network security, programming
- Access control, biometrics
- Smartcards, RFID, PKI
- Business continuity
- Encryption, secure comms
- Secure eCommerce and Cloud
- Governance, policy, standards
- Threat analysis & response
- Crime investigation and forensics
- Control systems, SCADA
- Critical infrastructure protection
- Commercialization, IP mngt

Market Focused Collaborative Research

Human Capacity Development

Training

Information Security Competence = the collection of capabilities for building confidence in ICTs through increased confidentiality, integrity & availability of information & information systems.

Information Security Research, Development and Innovation Coordinating HUB

- Strategy, business plan, Steering Committee
- **Audit** of the National System of Innovation
  - Tertiary education, science councils, government
- **Local networking** and conferences
- **Market sector** potential, trends, role players, partnerships
- National **Infosec Research Agenda**
  - Stakeholder needs, market needs, technology trends
- **International** networking, learning, collaboration
- **Human Capacity Development** – degrees, courses, research
- **Performance indicators**
  - Innovation capacity, market impact, economic impact
- Leading the **innovation process**
  - Integrated innovation platforms, phases, funding, IP rights, transfer
- Support to **Standards**

CSIR
our future through science

The National System of Innovation in Infosec

- Tertiary Education Institutions (informatics, elec eng, comp sc)
  - Rhodes, UP, UJ, NMMU, UFH, Unisa, UKZN, TUT, UCT, ..
  - Challenges: staff, students, focus and funding
- Science councils
  - CSIR: Meraka Institute, Defence Peace Safety & Security, Modelling & Digital Science
- Government
  - DST, DComms, NIA, NCC, COMSEC, DPSA & SITA, SAPO, SANDF, ..
  - SARS, DHA, DTpt, DHealth, SABS, DoJ&CD, SIU, E-CAC, …
- Industry
  - Vendors, Innovators
  - Integrators, Services
  - ISG Africa, …
- International
  - CERT-FI, FIRST, TERENA, ENISA, Royal Holloway UK
  - IST Africa, George Mason Univ, ….

Strategy for HCD at Tertiary Institutions

- Agree on focus areas within existing and required strengths
- Funding per Master's degree or PhD with sufficient funds for staff research and conference attendance
- Grow towards clearer research objectives as the National Research Agenda is refined

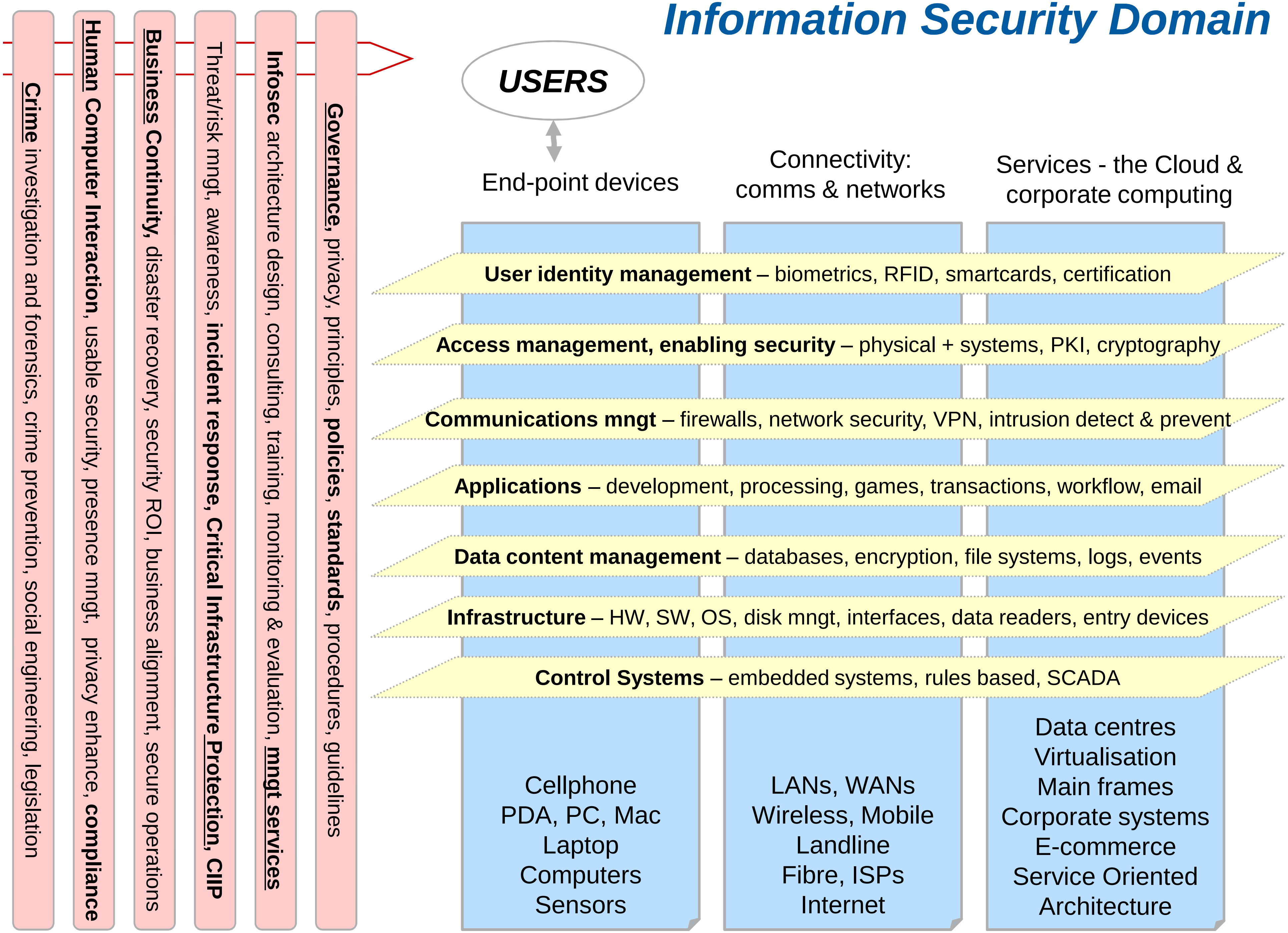
our future through science

SA IT Security Market Sizing and Forecast 2006 – 2011, BMI, Jan 2008

- From 2005 – 2006 the ICT market grew by 11% while the ICT security grew by 23%
  - Growth expected to continue
- Compliance as key driver – integration of IT security
- Ongoing growth in threats, risks, attacks, business impact
- Viruses, internal staff and spyware as major threats
- Collaboration and bundling of security solutions
- Growth in identity and access management, due mobile devices
- Growing complexity of IT and risks require variety of security solutions, managed security solutions
- Cost and lack of skills

- FOLLOW-UP: threats, trends, innovators, needs

Information Security Domain



Crime investigation and forensics, crime prevention, social engineering, legislation

Human Computer Interaction, usable security, presence mngt, privacy enhance, **compliance**

Business Continuity, disaster recovery, security ROI, business alignment, secure operations

Threat/risk mngt, awareness, **incident response, Critical Infrastructure Protection, CIIP**

Infosec architecture design, consulting, training, monitoring & evaluation, **mngt services**

Governance, privacy, principles, **policies**, **standards**, procedures, guidelines

USERS

End-point devices

Connectivity: comms & networks

Services - the Cloud & corporate computing

User identity management – biometrics, RFID, smartcards, certification

Access management, enabling security – physical + systems, PKI, cryptography

Communications mngt – firewalls, network security, VPN, intrusion detect & prevent

Applications – development, processing, games, transactions, workflow, email

Data content management – databases, encryption, file systems, logs, events

Infrastructure – HW, SW, OS, disk mngt, interfaces, data readers, entry devices

Control Systems – embedded systems, rules based, SCADA

Cellphone
PDA, PC, Mac
Laptop
Computers
Sensors

LANs, WANs
Wireless, Mobile
Landline
Fibre, ISPs
Internet

Data centres
Virtualisation
Main frames
Corporate systems
E-commerce
Service Oriented
Architecture

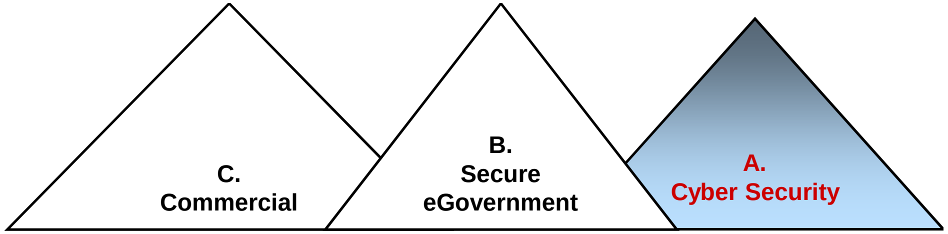
The issue is …

- We can’t do it all and thus have to focus on areas of
  - ***Market failure***
    - no take up due to lack of skills or
    - High entry barrier
    - Or national interest with potentially low commercial return
  - Where local capacity can develop solutions
  - Creating opportunities to buy local
  - And be globally competitive
- **This is a DST mechanism to focus on relevant INNOVATION in Information Security**

our future through science

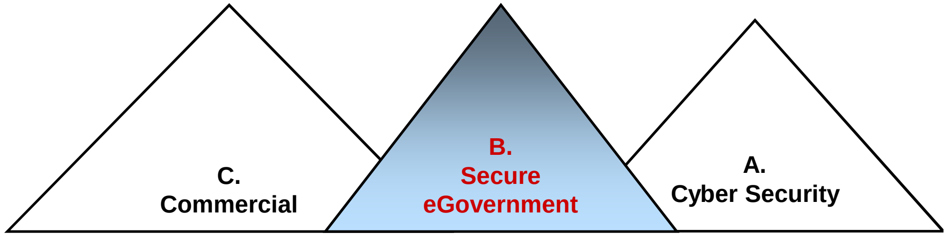
Three broad Market Opportunities defined

our future through science



Market Opportunity A:
Innovative Products and Services that contribute to enhanced National Cyber Security

- Threat and risk assessment
- Awareness and computer security incident response
- Critical infrastructure protection (CIP)
- Critical Information Infrastructure Protection (CIIP)
- Cyber crime investigation, prevention, forensics
- ECT Act is a key driver



Market Opportunity B:
Innovative Solutions that will enable Government to provide Secure eGovernment products and services

- Information is a vital public asset – government owns vast amounts
- Applying new ICT to the full range of government functions
  - cost, convenience, access to information and transactions
- **Enabling** enhanced service delivery given trust in ICT:
  - Govt – Govt, Govt – Business, Govt - Citizen
- Balancing Security and Privacy needs, protect against loss
- Thus improving effectiveness of Government

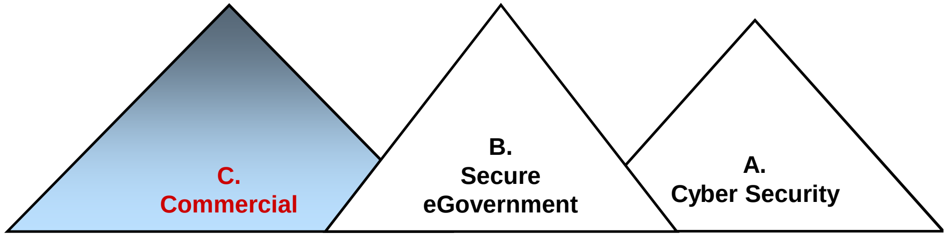
our future through science

Importance of E-government and Information Security research

- E-government as driver of information security research and innovation
  - Government is the largest single procurer of ICT
  - Therefore – government can create demand factors for local research and innovation

- The nature of research
  - it takes long
  - much of it is not terribly useful

- The benefits of information security research for e-government
  - Not all the problems have been solved
  - Research drives innovation
  - Doing research makes you a better buyer
  - You can only have e-government if you have secure e-government
  - Spin-off benefits



Market Opportunity C: *Innovations for niche, high-value, globally competitive, commercial Infosec Products & Services*

- New licensable technology, products and services
- Strong export potential.
- Strong experimental development capacity and broad knowledge
- New completed products, applications and services
  - In NICHE areas where it makes sense
  - In areas of “market failure” where
    - no takers or big entry barrier
    - local R&D can provide solutions
- TIME TO MARKET is critical in ICT

our future through science

Phases for each Market Opportunity (MO)

Phase 0 = MO Consortium for guidance

P1 = Define the MO Mission statement

P2 = MO Needs Analysis

- Stakeholder engagement, threat analysis, market study
- Required vs available, prioritize gaps

P3 = MO Strategy

- R&D and innovation plan, HCD, funding, partnership agreements

P4 = Impact achievement

- HCD, R&D, innovation, IP rights management, knowledge dissemination, technology transfer, commercialisation

Integrated Innovation Platforms
- initial list

Purpose:

- Enable HCD, facilitate collaborative R&D, promote better understanding of needs, close gaps in technology, seek opportunities for innovation OUTPUTS in areas A, B and/or C

Detailed plans:

- Objective, problem, proposed solutions, market/users, impact, collaborators, partners, risks, phases towards impact

1. ***Computer security incident response capabilities***
2. ***Computer crime prevention, investigation and forensics***
3. ***Critical infrastructure protection (CIP) and CIIP***
4. ***Security of open source software***
5. ***Implementation frameworks for PKI***
6. ***Security of mobile and wireless networks***
7. ***Person identification and smart cards***
8. ***Cryptography solutions for secure communications***

Key Performance Indicators

HCD and innovation capacity

- Stronger NSI
- Favourable regulatory environment
- Access to funding
- Increase in PhDs, researchers
- Research chairs
- Maturity in component competencies
- Increased research outputs
- Increased international transfer

Impact on Market Opportunities

- Increase in enterprises
- Increase in IP and patents
- Increase in products & services in market
- Increase regional innovation

Economic impact

- Total IS investment
- Improve technology balance of payments (less imports)
- Increased access to international funding

our future through science

Ways to participate

- Join Work/Steering Groups for Market Opportunities A, B and C
  - Identify opportunities, define R&D agendas,
  - Define integrated innovation platforms
- TEIs and research institutions:
  - funding available for needs-directed academic research and studies towards higher degrees
- Government, industry
  - define infosec needs, market gaps and opportunities, readiness to fund innovation
- Become part of the National System of Innovation in Infosec:
  - from market to mind to market,
  - requiring problem description and business plan,
  - venture co-funding
  - coordinated and joint R&D, sharing skills, facilities
  - commercialisation
  - IP protection and exploitation.

Any Questions??

our future through science

Information Security Research Agenda for South Africa

our future through science

Outline of the National Research Agenda presentation

- The Need for a national Information Security Research Agenda
- SWOT analysis
- Some examples
- Inputs from Panel Members

- Initial list of topics

our future through science

The Need for a National Information Security Research Agenda

- To build trust in the use of ICTs through formulating a prioritised R&D agenda and fostering collaboration in the National System of Innovation
- To give inputs to government decisions on future R&D
- To collate knowledge about global markets, products and research
- To capitalise timely on global market opportunities within the complex global needs

- To perform R&D that will strengthen our strategic independence and skilled human capital in key areas
- To aim for medium and long term sustainability of research platforms

SWOT analysis for South Africa wrt Information Security

Strengths

- Local ICT industry and expertise
- Pockets of excellence in research and education
- Capitalising ICT wave
- Learning from abroad
- Cyber legislation (ECT and others)
- Government agencies
- Innovation track record
- Standards working groups
- Financial services

Weaknesses

- Insufficient Human Resources
- No central cyber incident response
- Insufficient enforcement ability
- Insufficient threat data
- Fragmented research
- Incentives for higher degrees
- Threats under commercial wraps
- Innovation chasm

Opportunities

- Coordinated national effort
- International cooperation
- Open Source SW provides control
- Use our legal framework
- Innovation in RFID, payment systems, mobile applications, digital rights management, financial services, crypto, PKI, ROI potential
- Coordinated incident response

Threats

- Vulnerability +Crime +Terror +Warfare
- Growing ICT dependence => vulnerable
- Need, greed, “malicious need”, ideology
- Speed of new technology & vulnerabilities
- Threats from local / anywhere
- Methods / tools freely available
- Innovative cyber criminals
- Loss of own capabilities

International Information Security challenges

- **Grand Challenges: (SecureIST roadmap - EU)**
  - Countering vulnerabilities and threats within digital urbanization
  - Duality between digital privacy and collective security: digital dignity and sovereignty
  - Objective and automated processes – the Reinforcement of the Science and Technical Foundations of Trust, Security and Dependability (TSD)
  - Beyond the Horizon: a new convergence outside the Digital Universe
- **Hard Problems (INFOSEC Research Council - US)**
  - Global-Scale Identity Management
  - Insider Threat
  - Availability of Time-Critical Systems
  - Building Scalable Secure Systems
  - Situational Understanding and Attack Attribution
  - Information Provenance
  - Security with Privacy
  - Enterprise-Level Security Metrics

Cyber Security Strategy of the United Kingdom

safety, security and resilience in cyber space

June 2009

Vision:

Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space:

working together, at home and overseas,

to understand and address the risks,

to reduce the benefits to criminals and terrorists, and

to seize opportunities in cyber space to enhance the UK’s overall security and resilience.

To address the UK's cyber security challenges, the Government will:

- ***Establish a cross-government programme*** to address priority areas in pursuit of the UK's strategic cyber security objectives, including:
  - –– Providing additional funding for the development of innovative future technologies to protect UK networks;
  - –– Developing and promoting the growth of critical skills;
- ***Work closely with*** the wider public sector, industry, civil liberties groups, the public and with international partners;
- ***Set up an Office of Cyber Security (OCS)*** to provide strategic leadership for and coherence across Government;
- ***Create a Cyber Security Operations Centre (CSOC)*** *to*:
  - –– actively monitor the health of cyber space and co-ordinate incident response;
  - –– enable better understanding of attacks against UK networks and users;
  - –– provide better advice and information about the risks to business and the public.

Deloitte.

Risk Advisory.

Overview of 2009 landscape

Craig Rosewarne

June 2009

Sixteen CIO / Security reports were analysed…

- **Deloitte** 2009 FSI security survey
- CIO priorities for 2009 - **CIO Insight**
- IT-Business Balance issues survey
- Business expectations for IT focus 2009 - **Gartner**
- State CIO Priorities 2009 - **NASCIO**
- Top Network Security Threats in 2009 - **Bank Info Security**
- Top CIO concerns - **FierceCio.com**
- Security trends for 2009 – **Computer Weekly** report
- Profit driven attacks report – **ISF 2009**
- IT Predictions for 2009 - **IDC**
- **Deloitte** 2009 Consumer Business Top Security Initiatives
- Top CIO Challenges - the **CTO Forum**
- 12 Hot IT Management Trends for 2009 - **CIOupdate.com**
- Key Information Security trends for 2009 - **ISSA**
- **Forrester** – 12 Recommendations For Your 2009 Information Security Strategy
- Twenty Most Important Controls Effective Cyber Defense - **SANS.org**

80 key findings summarised down to top 30 areas…

SECURITY / RISK		CIO	
Preventing targeted hacks for financial gain	Technology	Cutting IT costs and Improving ROI	Strategy
Focus on Third Party Provider risk	Process	Align IT strategy to business strategy	Strategy
Compliance management / Legal & Regulatory compliance / Electronic Records Management	Strategy	Benefits of Cloud computing	Technology
Data protection & information leakage	Technology	Benefits + Security requirements around Virtualisation technologies	Technology
Security infrastructure improvement (Network + applications)	Technology	Attracting & retaining IT professionals	People
Web security - Adopting Web 2.0 while guarding privacy and confidentiality + Web development security + (Boundary Defense)	Technology	Managing IT outsourcing / in sourcing effectively / Consolidation: centralizing, consolidating services, Shared Services: business models, sharing resources	Strategy
Security awareness - Malicious Insiders/Careless Employees / Social Engineering	People	Effective corporate & IT governance management	Strategy
Security Strategy (Look for opportunities to make security invisible / Governance for security)	Strategy	Improving enterprise workforce effectiveness (skills & competency assessments)	People
Identity & access management	People	Increasing the use of information/analytics	Review
ISMS (ISO 27002 threat assessment)	Process	Effective Programme delivery / Project risk management	Process
Establish a Forensics response + incident management capability (+Identify & establish an agreement with third party cybercrime-intelligence services)	Process	Creating a green IT culture	Strategy
Managing mobile device security	Technology	Privacy	Process
Assessing business risk with a clear understanding of PCI requirements	Process	Business Continuity	Process
Security Monitoring - Maintenance and Analysis of Complete Security Audit Logs	Review	Balanced scorecards, Dashboards & reporting	Review
Policy, Standards and secure baselines	Process	Talent retention strategies	Review

Initial list of key areas from Tertiary Education Institutions

our future through science

1. Open source security environment
2. Identity management and use of biometrics and digital signatures. Dependable identification.
3. PKI implementation framework for eGovernment (management & implementation)
4. Critical infrastructure protection, includes information, communication & industrial systems.
5. Security in medical informatics
6. Emerging threat analysis including social engineering
7. Culture of awareness, secure coding practice, corporate security, security planned in.
8. Risk management, security incident response, disaster recovery, business continuity, effective content for security awareness for corporates, user awareness.
9. Mobile and wireless system security, WiFi, GSM, WiMax
10. Security of social networks (You-tube etc)
11. Legislation, legal use of IT, ethical use of IT
12. Effect of broad band liberalisation and increased bandwidth (SEACOM cable)
13. Governance – legal requirements, responsibilities, standards, policy
14. Privacy-enhancing technologies and legislation, how enforce
15. Security of RFIDs for tracking, identity management, authentication
16. Role based access control, digital rights management, info/data protection
17. Cryptography – local expertise, quantum cryptography
18. Computer crime investigation and digital forensics
19. Security of E-Commerce, internet banking, insurance, credit cards, mobile banking

Questions and suggestions?

- **Who would like to become part of the IS-RA team?**
- **specific documents and requirements?**

our future through science