MALAYSIA'S NATIONAL CYBER SECURITY POLICY
Towards an Integrated Approach for Cyber Security and Critical Information Infrastructure Protection (CIIP)

MOHD SHAMIR HASHIM
Cyber Media Research & Policy Division
CyberSecurity Malaysia

shamir@cybersecurity.my

24 SEPTEMBER 2009

CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

THE BRAND LAUREATE
CyberSecurity Malaysia
Best in Corporate Branding
Internet Security

Securing Our Cyberspace

CYBER THREATS
- Malaysia

CyberSecurity MALAYSIA

Technology Related Threats

Hack Threat

Intrusion

Fraud

Harassment

Malicious Code

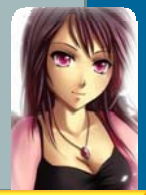
Denial of Service Attack

Cyber Content Related Threats

Threats to National Security

Sedition / Defamation

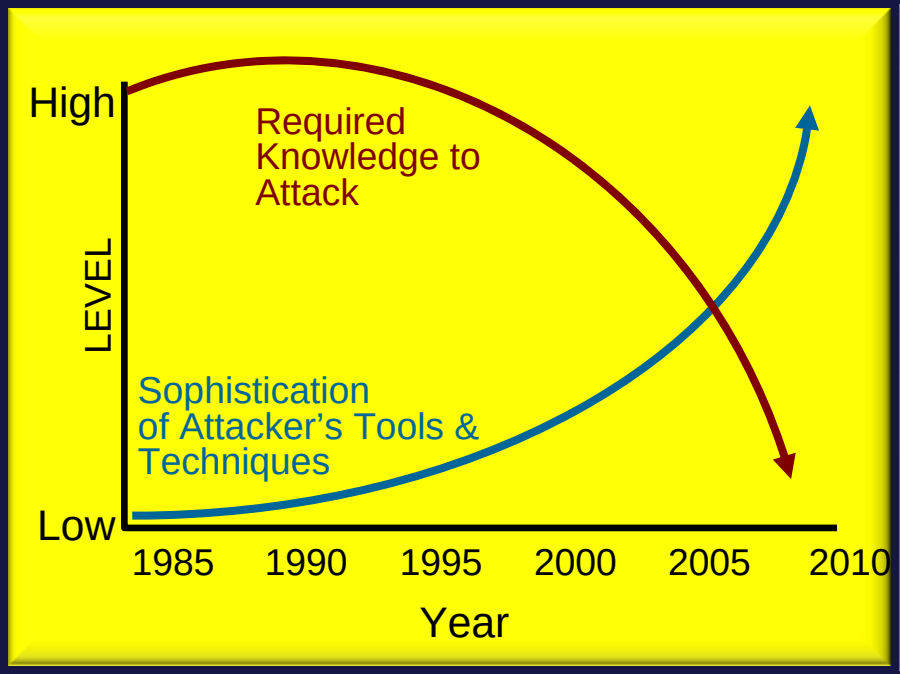
Online Porn



Hate Speech

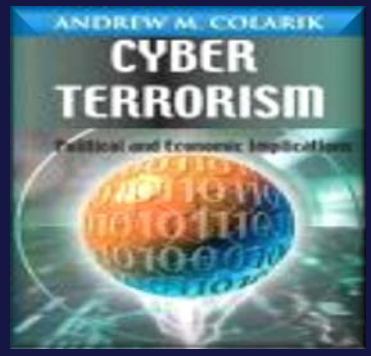
Securing Our Cyberspace

CYBER THREATS
CyberSecurity Malaysia's Analysis



- **Emerging Threats:**
  - large scale, sophisticated and damaging
  - high connectivity creates opportunities to attackers
  - network has everything i.e. financial gain, power, reputation, national secrets
  - conflicts in physical world may lead to conflicts in cyber world

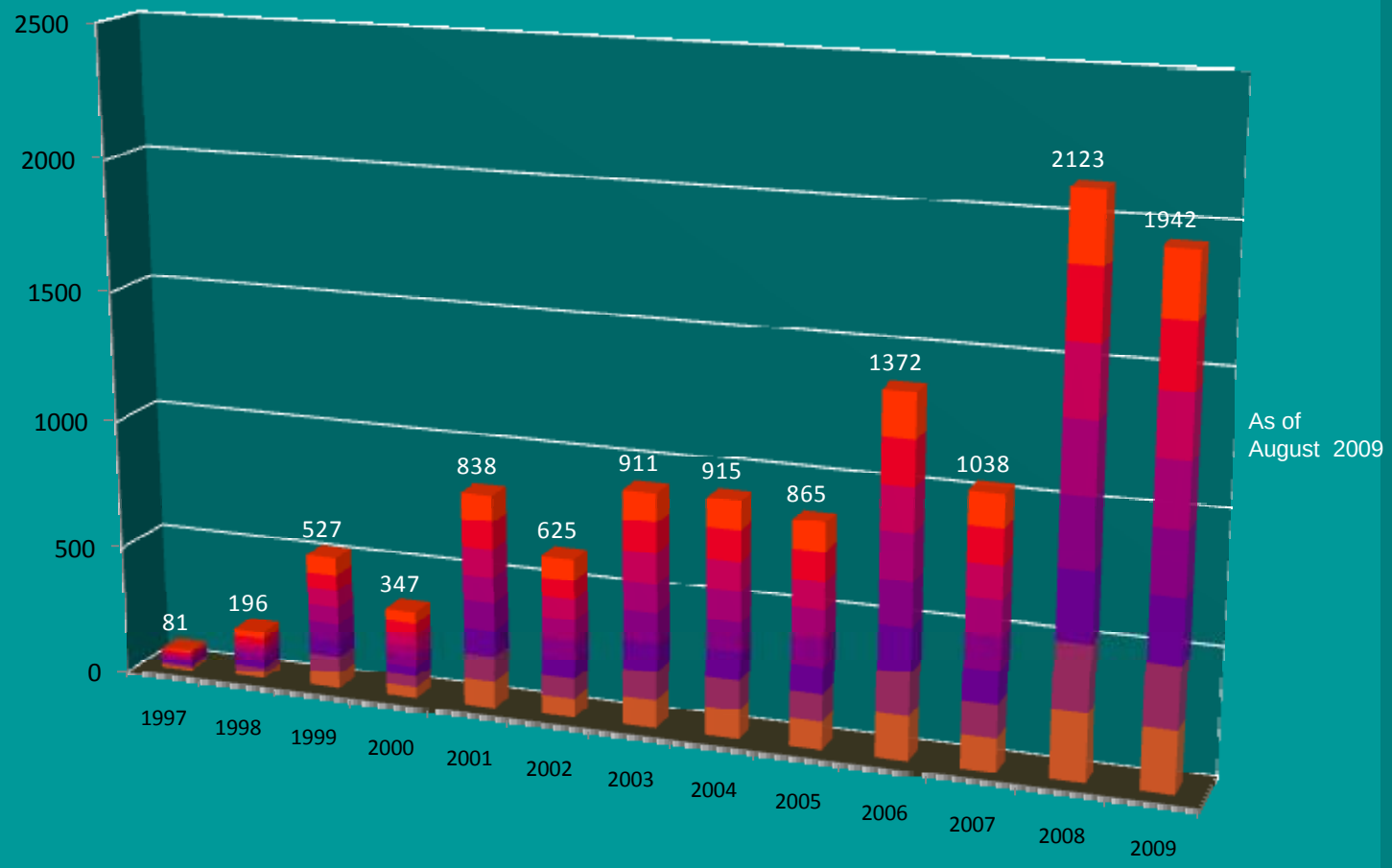
- Opportunities and capabilities can trigger cyber conflicts
- Cyber Terrorism / Cyber Warfare most likely to become a future threat
- Critical National Information Infrastructures (CNII) may become attractive targets



CYBER SECURITY INCIDENTS - MyCERT

- A total of 11,780 security incidents were referred since 1997 (excluding spam)

Type of incidents:
- **Drones Report**
- **Denial of Service**
- **Fraud & Forgery**
- **Vulnerability Probing**
- **Harassment**
- **Indecent Content**
- **Malicious code**
- **System Intrusion**

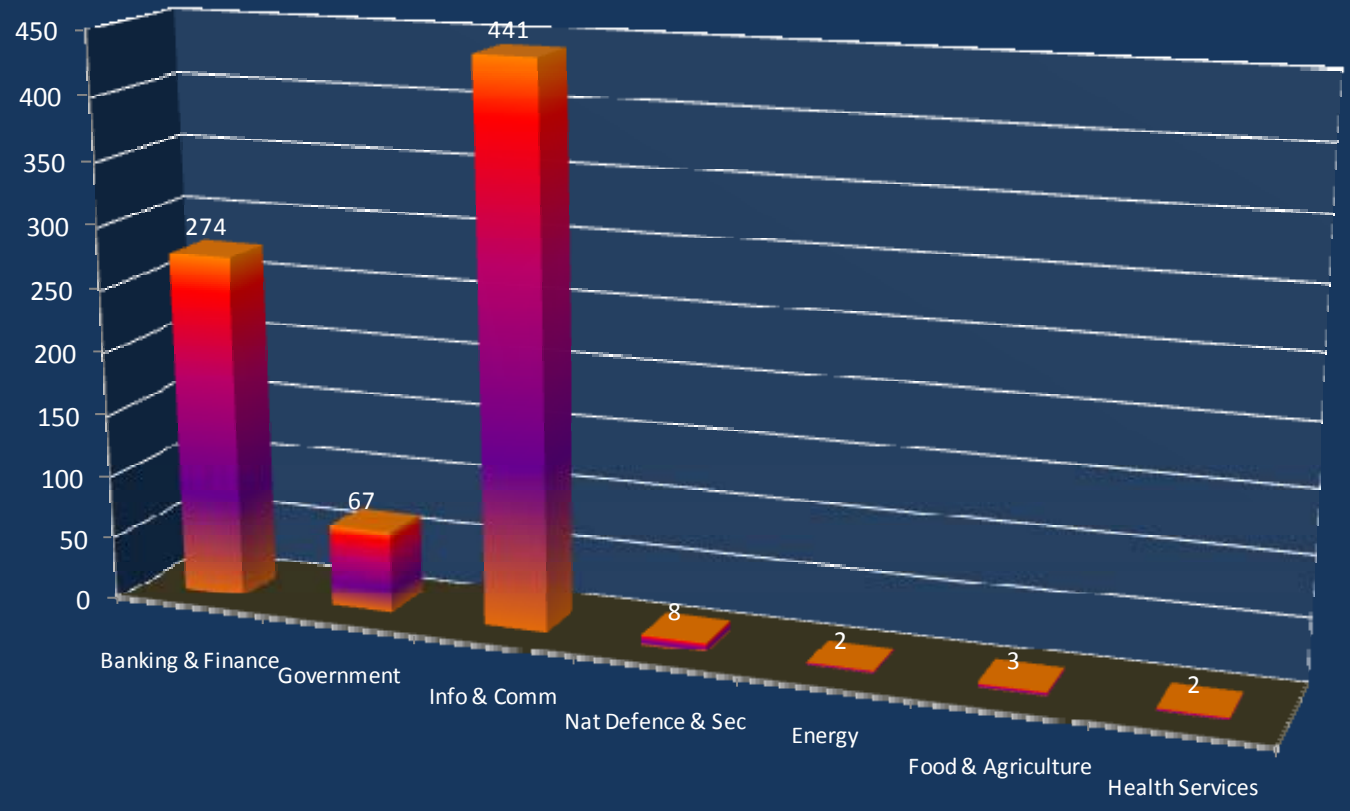


Securing Our Cyberspace

CYBER SECURITY INCIDENTS
- MyCERT : CNII MALAYSIA

- A total of 797 security incidents were referred from Jan-August 2009

Type of incidents:
- **Spam**
- **Drones Report**
- **Denial of Service**
- **Fraud & Forgery**
- **Vulnerability Probing**
- **Harassment**
- **Indecent Content**
- **Malicious code**
- **System Intrusion**



THE NATIONAL CYBER SECURITY POLICY - Objective

2005 The National Cyber Security Policy formulated by MOSTI

2006 NCSP Adoption and Implementation

The policy recognises the critical and highly interdependent nature of the CNII and aims to develop and establish a comprehensive programme and a series of frameworks that will ensure the effectiveness of cyber security controls over vital assets

Objectives:

- Address The Risks To The Critical National Information Infrastructure
- To Ensure That Critical Infrastructure Are Protected To A Level That Is Commensurate With The Risks
- To Develop And Establish A Comprehensive Program And A Series Of Frameworks

Securing Our Cyberspace

THE NATIONAL CYBER SECURITY POLICY
- Vision & CNII Sectors

VISION

'Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well being and wealth creation'

DEFENCE & SECURITY

- Ministry of Defense, Military
- Ministry of Home Affairs, Police

TRANSPORTATION

- Ministry of Transport

BANKING & FINANCE

- Ministry of Finance
- Central Bank
- Securities Commission

HEALTH SERVICES

- Ministry of Health

EMERGENCY SERVICES

Ministry of Housing & Local Municipality

CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Assets (real & virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on

- *National economic strength*
- *National image*
- *National defense & security*
- *Government capability to function*
- *Public health & safety*

ENERGY

- Energy Commission
- Electricity Co., Petroleum Company

INFORMATION & COMMUNICATIONS

- Ministry of Information, Communications & Culture
- Malaysia Communication & Multimedia Commission

GOVERNMENT

- Malaysia Administrative, Modernisation and Management Planning Unit

FOOD & AGRICULTURE

- Ministry of Agriculture

WATER

- National Water Service Commission

Securing Our Cyberspace

THE NATIONAL CYBER SECURITY POLICY
- Implementation Approach

(0 – 1 YEAR) ADDRESSING IMMEDIATE CONCERNS

- Stop-gap measures to address fundamental vulnerabilities to the information security of the CNII.
- Creating a centralised security platform.

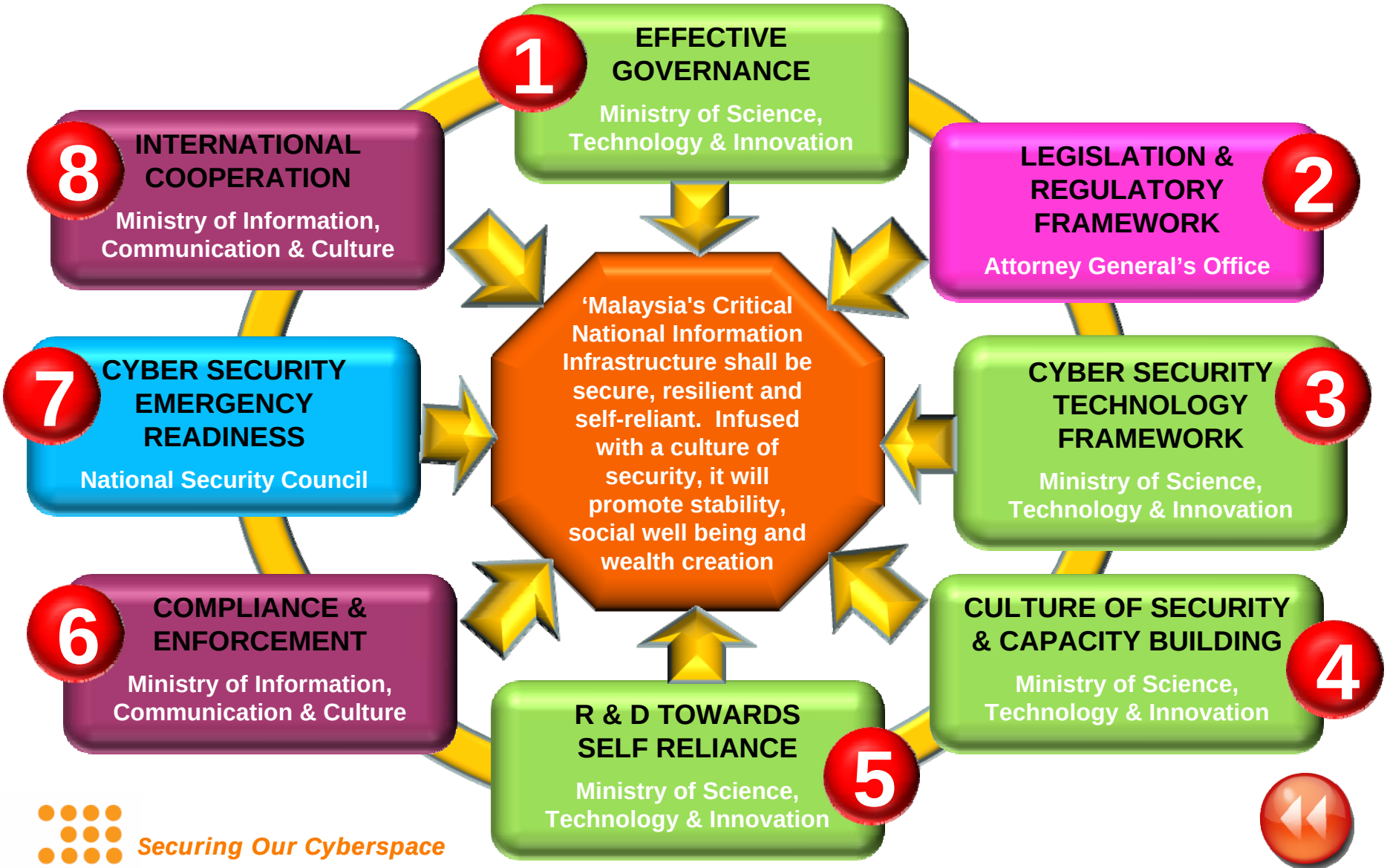
(0 – 3 YEARS) BUILDING INFRASTRUCTURE & HUMAN CAPACITY

- Setting-up the necessary systems, processes, standards and institutional arrangements (mechanisms) .
- Building capacity amongst researchers and info security professionals.

(0 – 5 YEARS & BEYOND) DEVELOPING SELF-RELIANCE

- Developing self-reliance in terms of technology as well as professionals.
- Monitoring the mechanisms for compliance.
- Evaluating and improving the mechanisms .
- Creating the culture of Info Security.

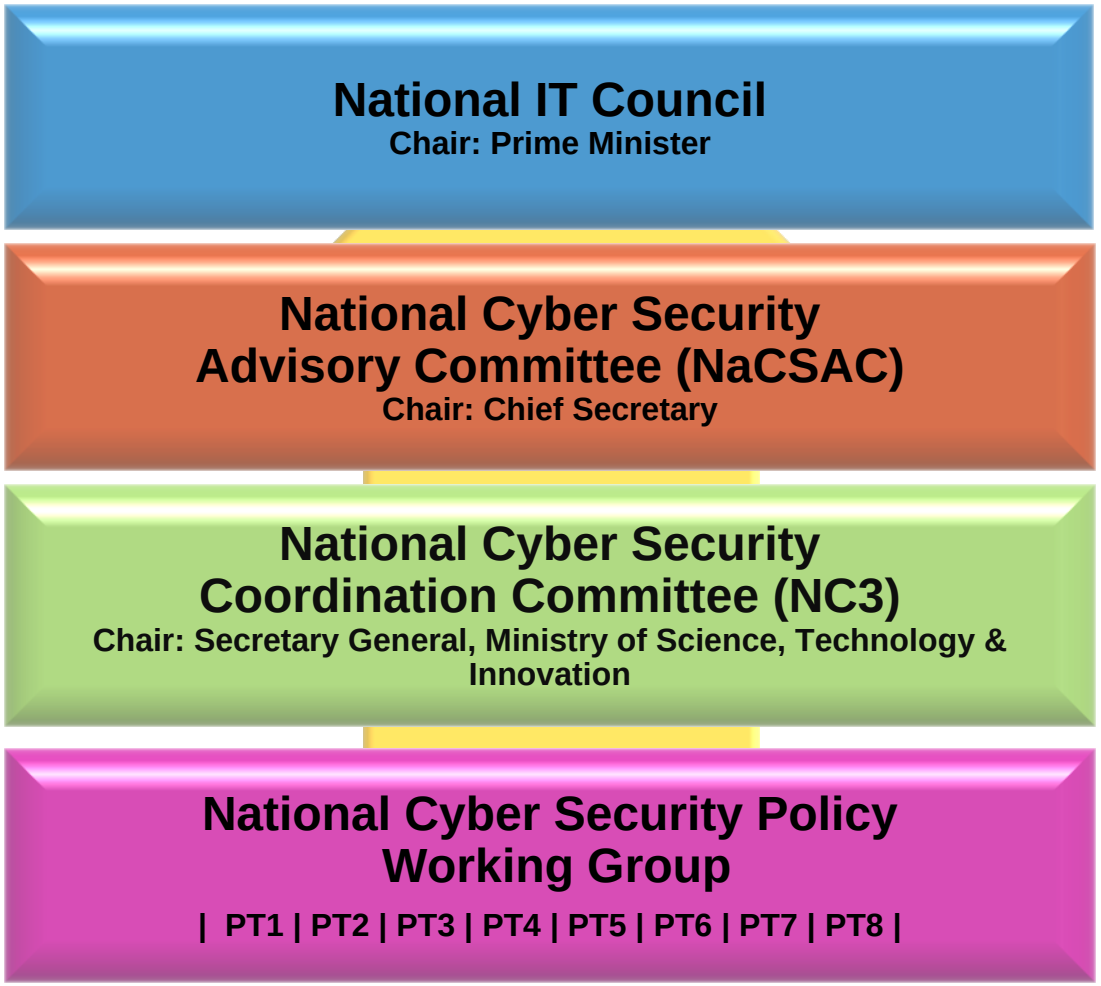
THE NATIONAL CYBER SECURITY POLICY
- Policy Thrust



Securing Our Cyberspace

PT 1: EFFECTIVE GOVERNANCE
- Structure

Establishment of a national info security coordination center



PT 1: EFFECTIVE GOVERNANCE
- Members

1. Malaysian Administrative, Modernisation and Management Planning Unit, Prime Minister's Dept
2. National Security Council, Prime Minister's Dept
3. Attorney General's Office. Prime Minister's Dept
4. Chief Government Security Officer's Office, Prime Minister's Dept
5. Ministry of Science, Technology & Innovation
6. Ministry of Defence
7. Ministry of Foreign Affairs
8. Ministry of Energy, Green Technology & Water
9. Ministry of Finance
10. Ministry of Information, Communication & Culture
11. Ministry of Transportation
12. Ministry of Home Affairs
13. Central Bank of Malaysia
14. National Water Services Commission
15. Malaysian Communication & Multimedia Commission
16. Energy Communication
17. Security Commission Malaysia
18. CyberSecurity Malaysia

A Study on the laws of Malaysia to accommodate legal challenges in the Cyber Environment

Stage 1 Identification of issues and challenges faced in the cyber environment

Stage 2 Assessment of current legislative framework

Stage 3 Recommendation of type of amendments to the law



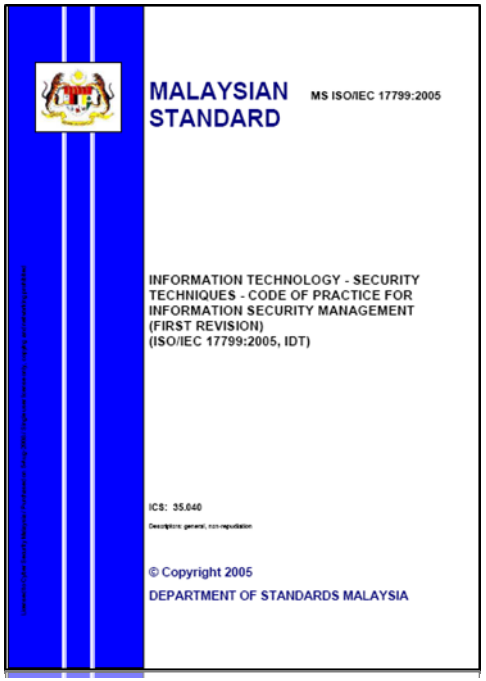
Reduction of & increased in the success in, prosecution in cyber crime

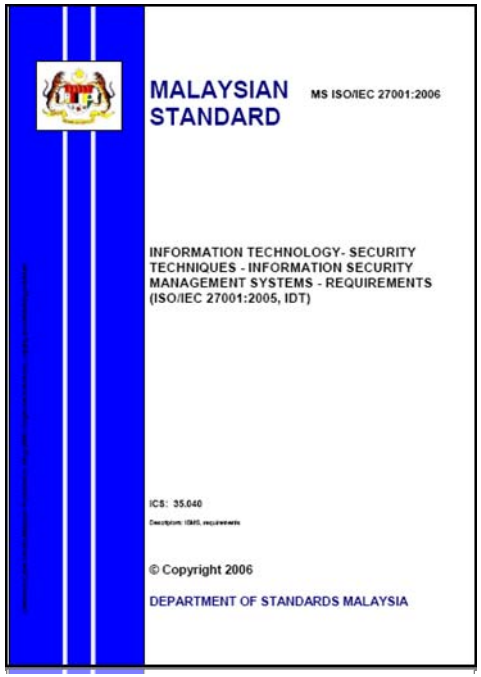
Securing Our Cyberspace

PT 3: CYBER SECURITY TECHNOLOGY FRAMEWORK - Standards

To increase the robustness of the CNII sectors by complying to international standards:

MS ISO/IEC 27001:2006 Information Security Management System (ISMS)





The International Standards

MS ISO/IEC 27001:2006 **MS ISO/IEC 17799:2005**

Adopted as Malaysian Standards

Securing Our Cyberspace

Expansion of national certification scheme for infosec mgmt & assuarance

Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme

Malaysia was accepted as CCRA Certificate Consuming Participant on 28 March 2007

MISSION
"to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products"

Malaysia was accepted as CCRA Certificate Consuming Participant on 28 March 2007

Austria			India
Czech Republic			Turkey
Denmark			Italy
Findand			Malaysia
Greece			Pakistan
Hungary			Singapore

PT 4: CULTURE OF CYBER SECURITY & CAPACITY BUILDING – Capacity Building

CyberSecurity MALAYSIA

DRI the institute for continuity management

- Associate Business Continuity Professional (ABCP)
- Certified Functional Continuity Professional (CFCP)
- Certified Business Continuity Vendor (CBCV)
- Certified Business Continuity Professional (CBCP)

(ISC)²

- Certified Information Systems Security Professional (CISSP)
- Systems Security Certified Practitioner (SSCP)

ISACA Serving IT Governance Professionals Malaysia Chapter

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)

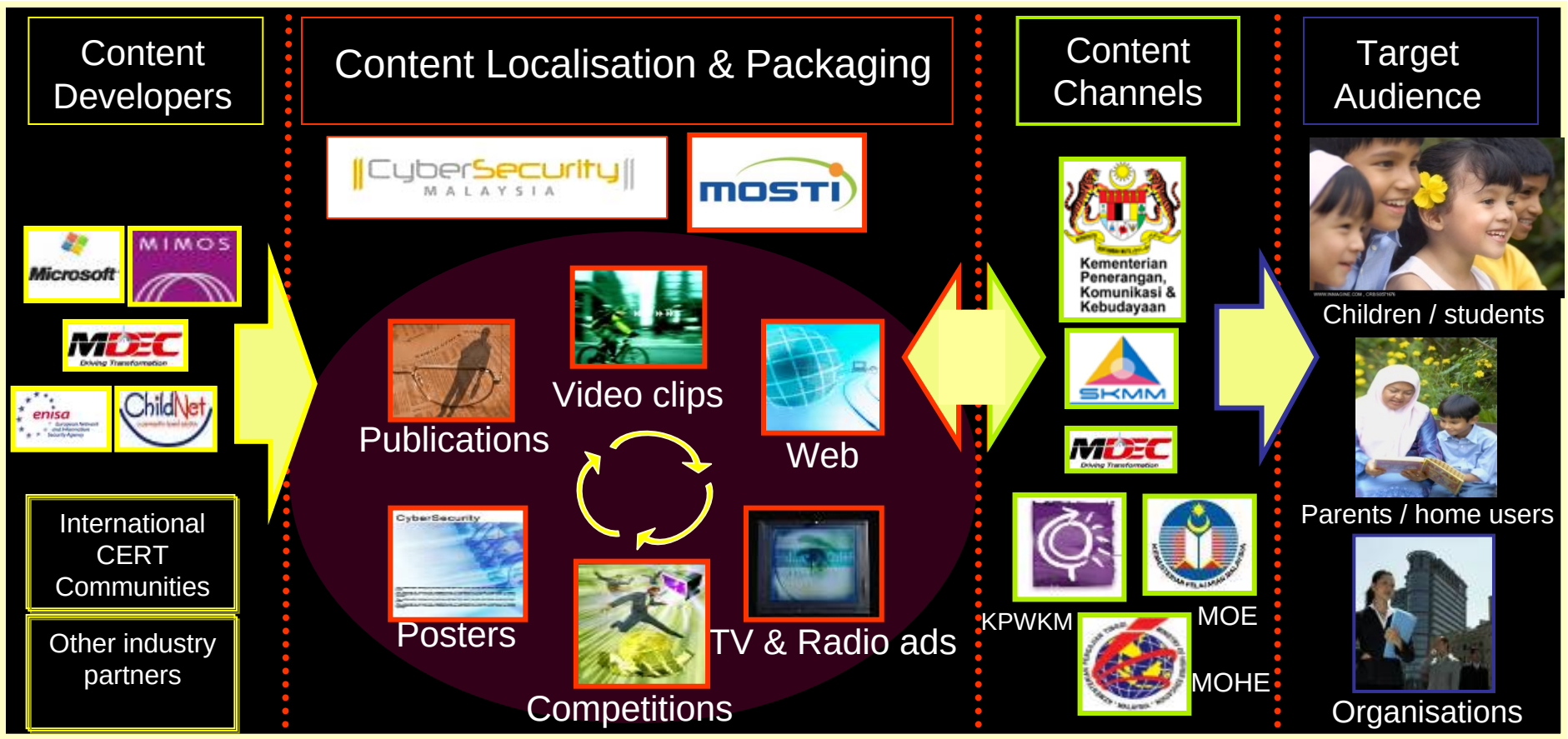
Critical Infrastructure CIi Institute

- Professional in Critical Infrastructure Protection (PCIP)

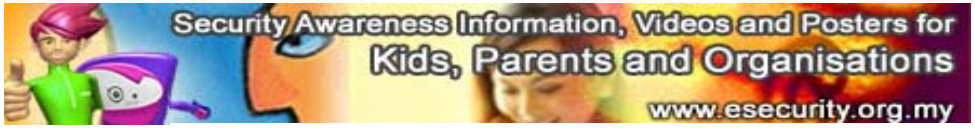
Securing Our Cyberspace

Reduce no of Infosec incidents through improved awareness & skill level

PT 4: CULTURE OF CYBER SECURITY & CAPACITY BUILDING - Awareness



Let's Make The Internet A Safer Place



Securing Our Cyberspace

PT 4: CULTURE OF CYBER SECURITY & CAPACITY BUILDING – Awareness Materials

Securing Our Cyberspace

PT 5: RESEARCH & DEVELOPMENT TOWARDS SELF RELIANCE - R & D Roadmap

Development of the National R&D Roadmap for Self Reliance in Cyber Security Technologies is facilitated by MIMOS

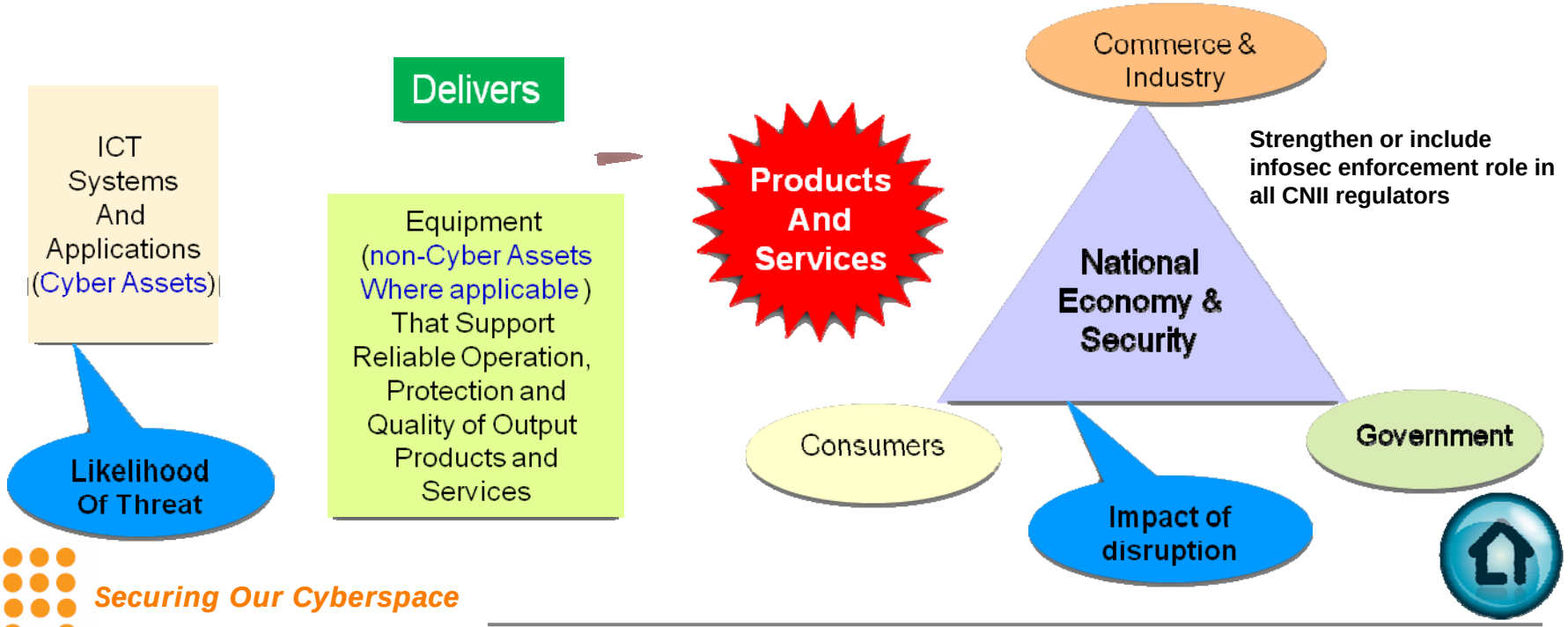
Acceptance & utilization of local developed info security products

- To Identify Technologies That Are Relevant and Desirable by the CNII
- To Promote Collaboration with International Centres of Excellence
- To Provide Domain Competency Development
- To Nurture the Growth of Local Cyber Security Industry
- To Update the National R&D Roadmap

Securing Our Cyberspace

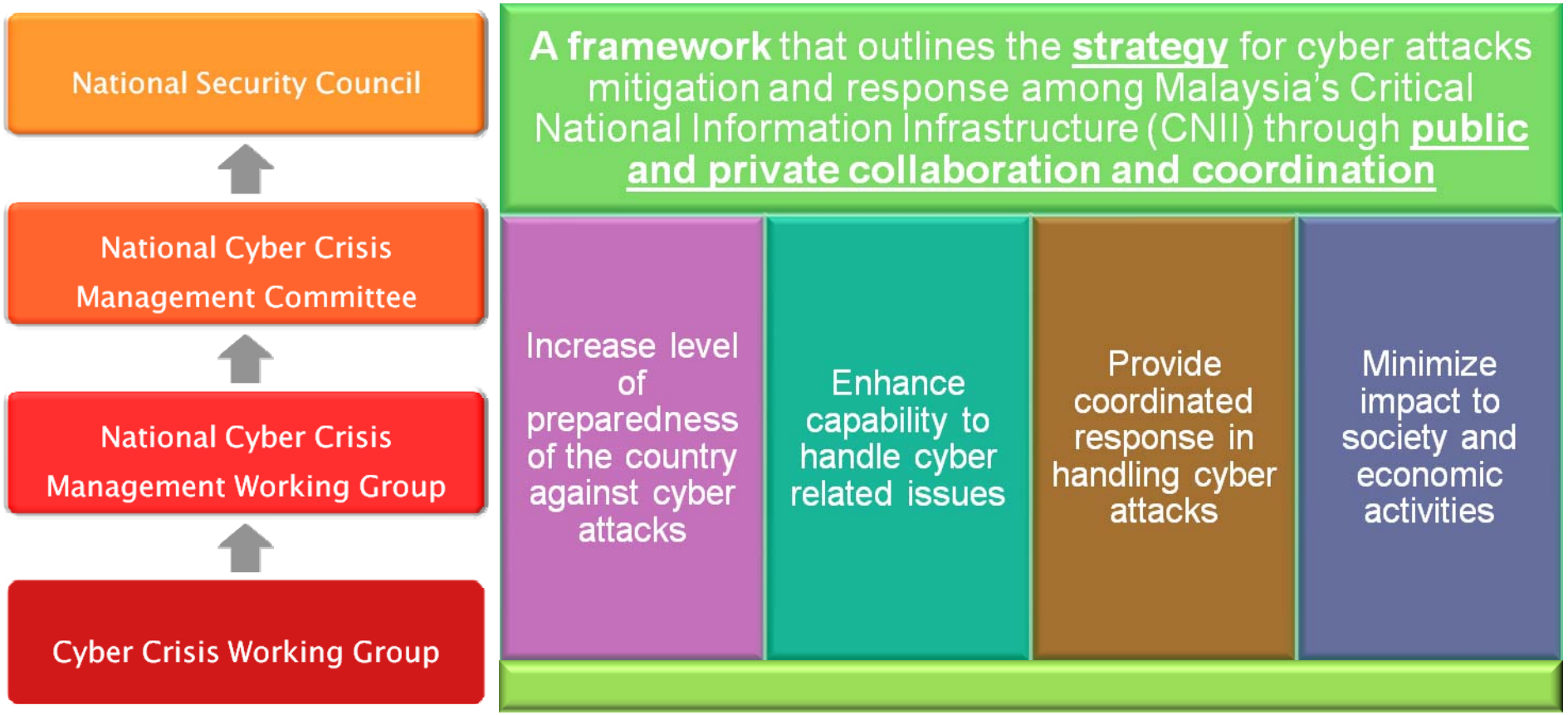
Risk Assessment Focus in NCSP :

Risk Assessment (in NCSP-PT6 context) looks at the **likelihood** of threats exploiting vulnerabilities to **Cyber Assets** disrupting/compromising delivery of **Products and Services** and the **consequence or impact** of the disruption/compromises of the **Products and Services to the Nation**, Commerce, Industry, Government, Consumers and other beneficiaries



PT 7: CYBER SECURITY EMERGENCY READINESS - National Cyber Crisis Management Plan

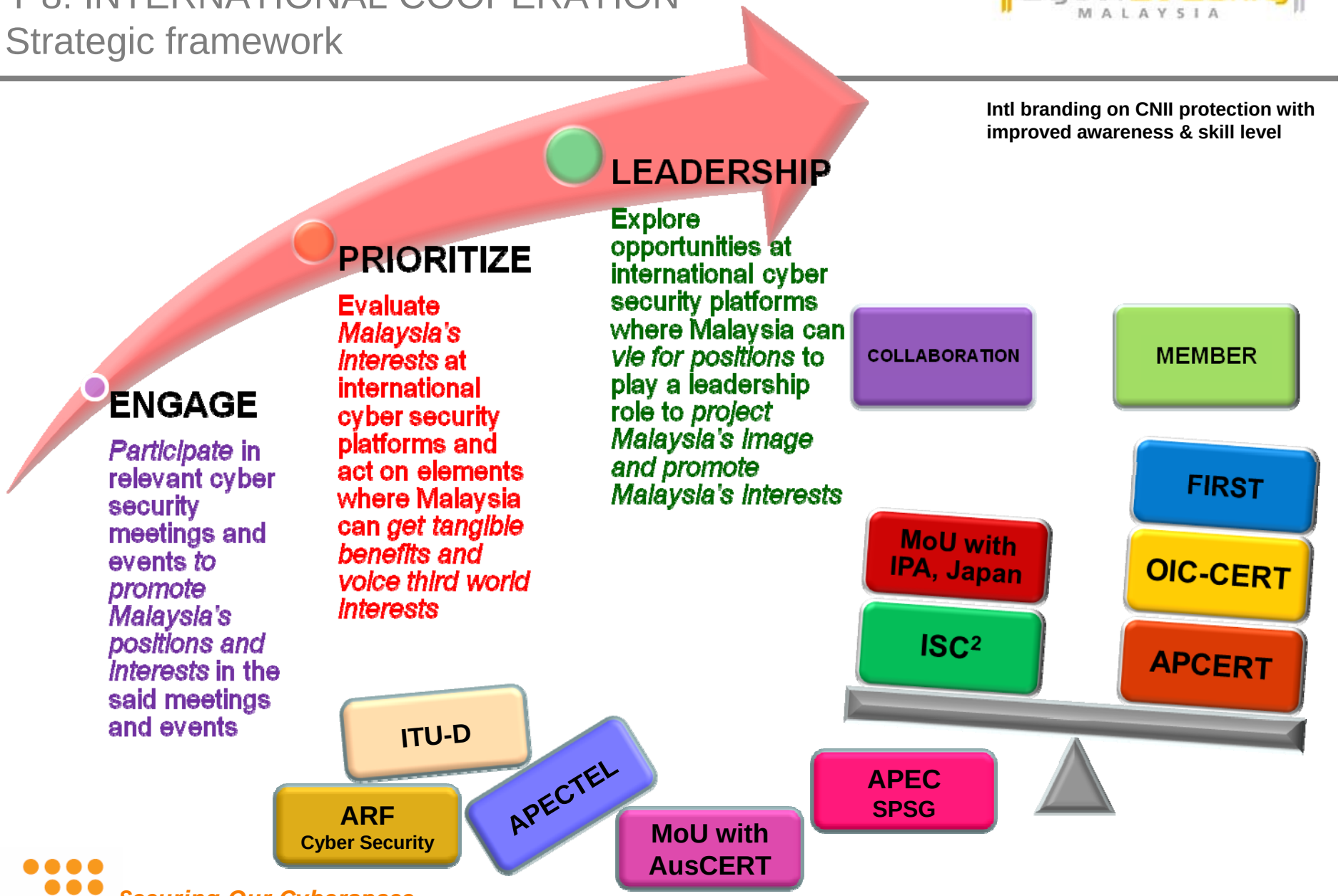
CNII resilience against cyber crime, terrorism, info warfare



Securing Our Cyberspace

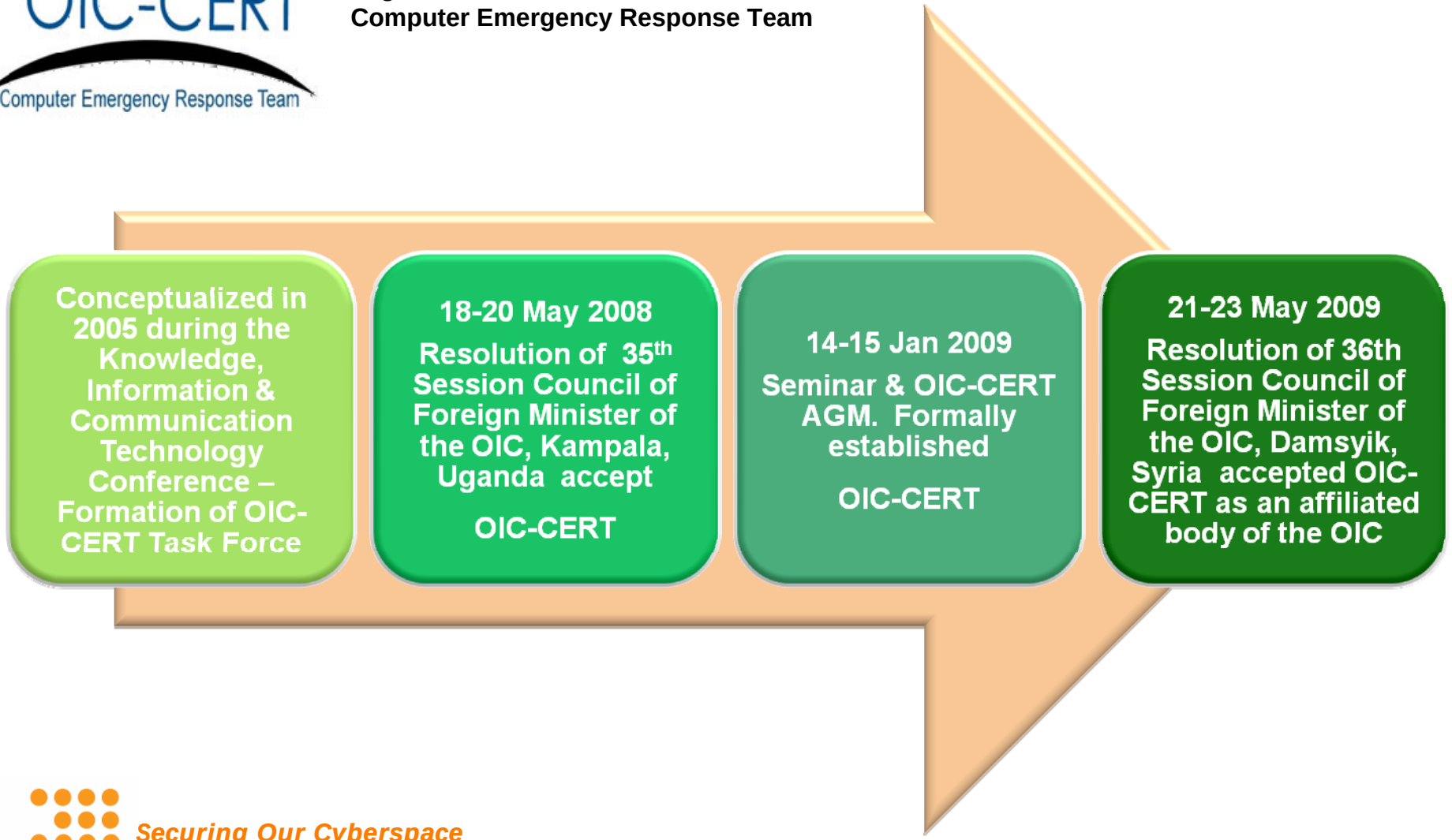
PT 8: INTERNATIONAL COOPERATION
- Strategic framework

Intl branding on CNII protection with improved awareness & skill level



PT 8: INTERNATIONAL COOPERATION
- OIC –CERT History

Organization of the Islamic Conference
Computer Emergency Response Team



PT 8: INTERNATIONAL COOPERATION
- OIC –CERT Members

MALAYSIA (Chair)
- CyberSecurity Malaysia

SAUDI ARABIA
- Computer Emergency Response Team – Saudi Arabia

NIGERIA
- Consultant Support Services

EGYPT
- Ministry of Communications & Information Technology

LIBYA
- Center for Economic Information & Documentation

INDONESIA
- Indonesian Security Incident Response Team on Internet

OMAN
- Information Technology Authority

BANGLADESH
- Bangladesh Computer Emergency Response Team (BDCERT)

TUNISIA (Secretariat)
- National Agency for Computer Security (NACS)

PAKISTAN
- National Response Center for Cyber Crimes

IRAN
- Ministry of ICT (IRCERT)

MOROCCO
- Ministry of Industry & New Technologies

BRUNEI
- ITPSS Sdn Bhd (BruCERT)

JORDAN
- National Center for Security & Crisis Management

SYRIA
- Ministry of Communication & Technology

TURKEY
- Brunei Computer Emergency Response Team (TR-CERT)

Securing Our Cyberspace

OIC-CERT
Computer Emergency Response Team

OBJECTIVES

- Strengthen relationship amongst CERT/CSIRT in the OIC countries
- Information sharing
- Prevent/reduce cyber terrorism activitiesTs
- Education and Outreach ICT Security Programs
- Promote collaborative technology research, development and innovations
- Promote Good Practices and / or recommendation to address legal and regulatory issues
- Assist member countries to establish National CERTs

PT 8: INTERNATIONAL COOPERATION
- OIC –CERT Seminar & AGM 2009

KL Resolution 2009

The OIC-CERT will intensify efforts in areas of:

- Strategic Cooperation
- Technical Cooperation
- Awareness & Capacity Building
- Law Enforcement & Regulatory Cooperation
- Funding

Securing Our Cyberspace