Information Security @ ITB

Yudi Satria Gondokaryono

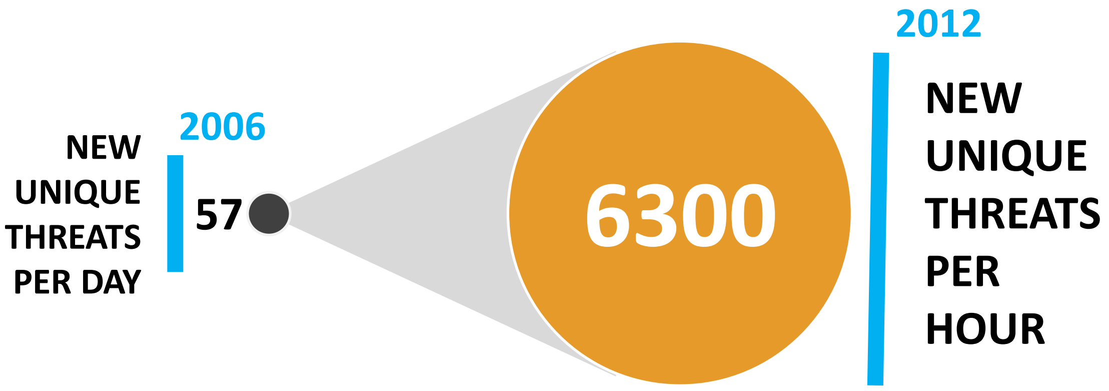
Direktur ITB-Korea Cyber Security R&D Center

Intro: Security

Pengguna internet di seluruh dunia: lebih dari **2 Milyar***

Hampir semua device terhubung ke internet

Kemudian muncul berbagai *security threats* dengan tren yang meningkat tajam tiap tahunnya.



NEW UNIQUE THREATS PER DAY

2006

57

6300

2012

NEW UNIQUE THREATS PER HOUR

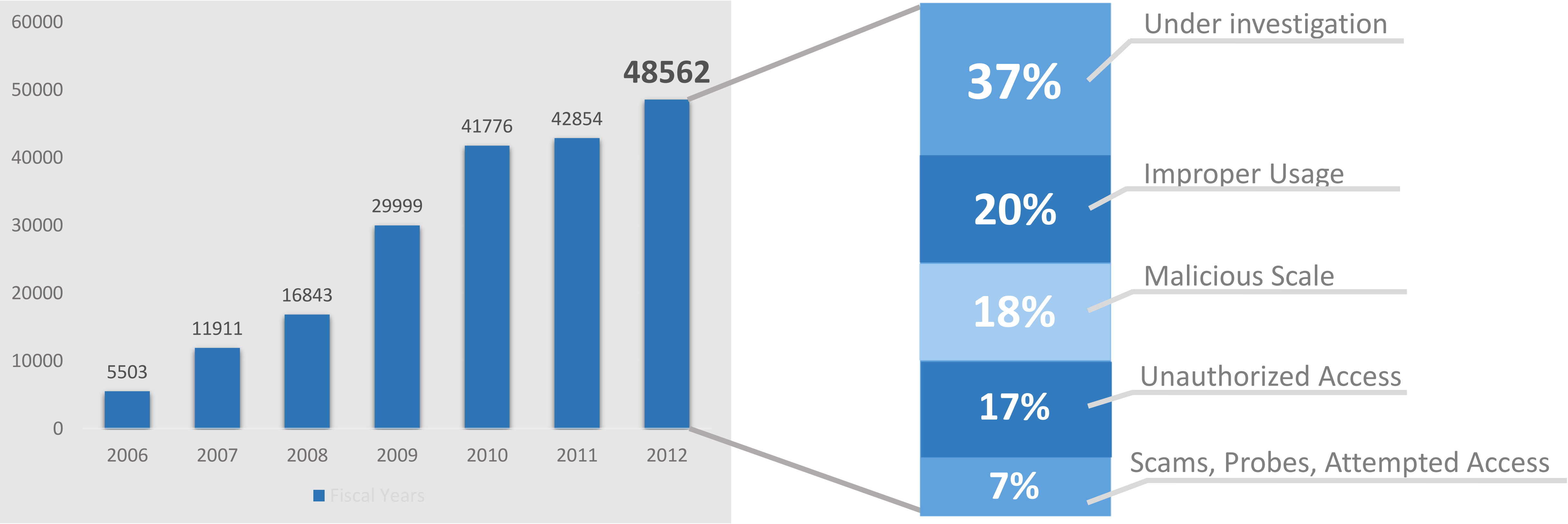
Spam Phising Malware Bad URL Identity Theft

Ransomware Stuxnet ZeuS Shamoon Agent.A

* sumber: http://www.thecultureist.com/2013/05/09/how-many-people-use-the-internet-more-than-2-billion-infographic/

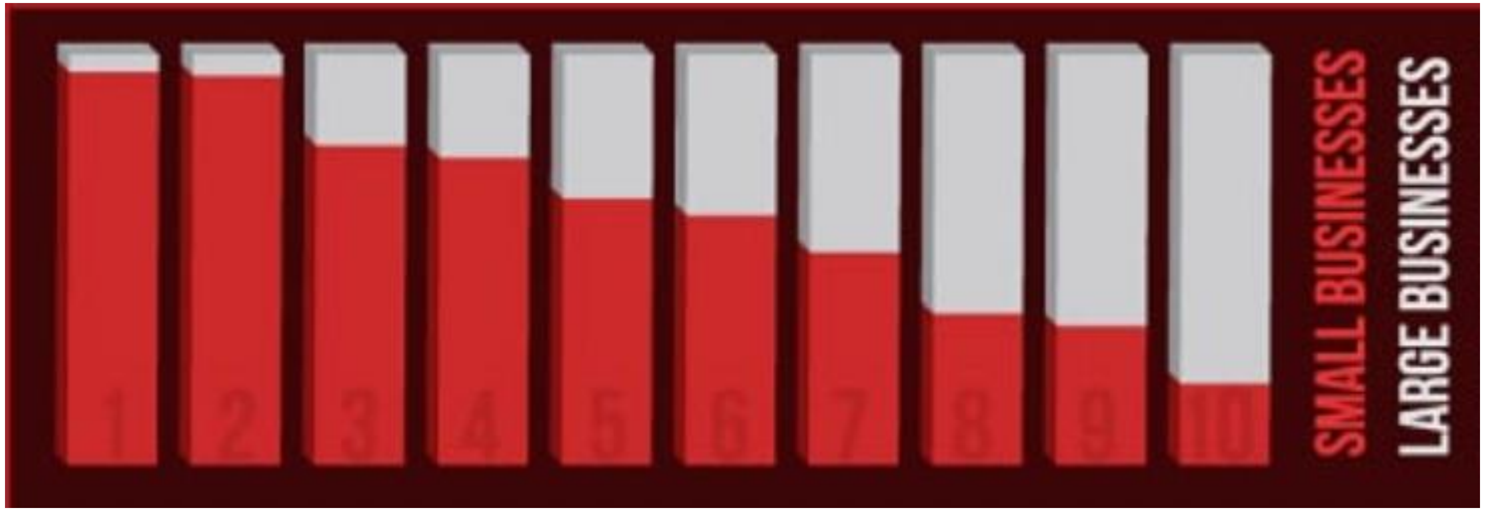
Intro: Security

Number of Security Incidents Reported to US-CERT Fiscal Years 2006-2012 From Federal Agencies



Sumber: http://www.govloop.com/profiles/blogs/infographic-cybersecurity-in-focus

What do the attackers take?



1. Payment card numbers/data
2. Authentication credential
3. Copyrighted material
4. Medical records
5. Classified information
6. Bank account detauils
7. Personal information
8. System information
9. Sensitive organizational data
10. Trade secrets

Average cost to **a small-bussiness** from cyber attack is **$ 188,242**

Sumber: infographicarchieve.com

Strategi Ketahanan Cyberspace Nasional

- ***Tujuan strategi nasional cyberspace***

  "Menjamin ketahanan informasi dan sistem pendukungnya dalam rangka menyelesaikan permasalahan strategis bangsa dan meningkatkan kualitas kehidupan bangsa Indonesia"

FREEDOM is the GLORY OF ANY NATION.
INDONESIA for INDONESIANS!
Nederlandse Fotomuseum Rotterdam
CasOorthuys 1 1946

Permasalahan Dunia Siber

	Prioritas 1	Prioritas 2	Prioritas 3	Prioritas 4	Prioritas 5	Prioritas 6
Pengguna alat komunikasi personal	✗	✗	✗			
Pengguna komputer rumahan / Industri kecil dan menengah	✗	✗	✗	✗		
Perusahaan besar (termasuk universitas, korporasi, lembaga pemerintahan)	✗	✗	✗	✗	✗	✗
Sektor atau infrastruktur kritikal	✗	✗	✗	✗	✗	✗
Skala nasional	✗	✗	✗	✗	✗	
Internasional						✗

Prioritas 1

Membangun sistem yang menjamin ketersediaan informasi bagi bangsa dan negara

Prioritas 2

Membangun organisasi dan tata kelola sistem penanganan keamanan *cyberspace* nasional

Prioritas 3

Sistem untuk memperkecil kelemahan dan ancaman pada keamanan *cyberspace* nasional

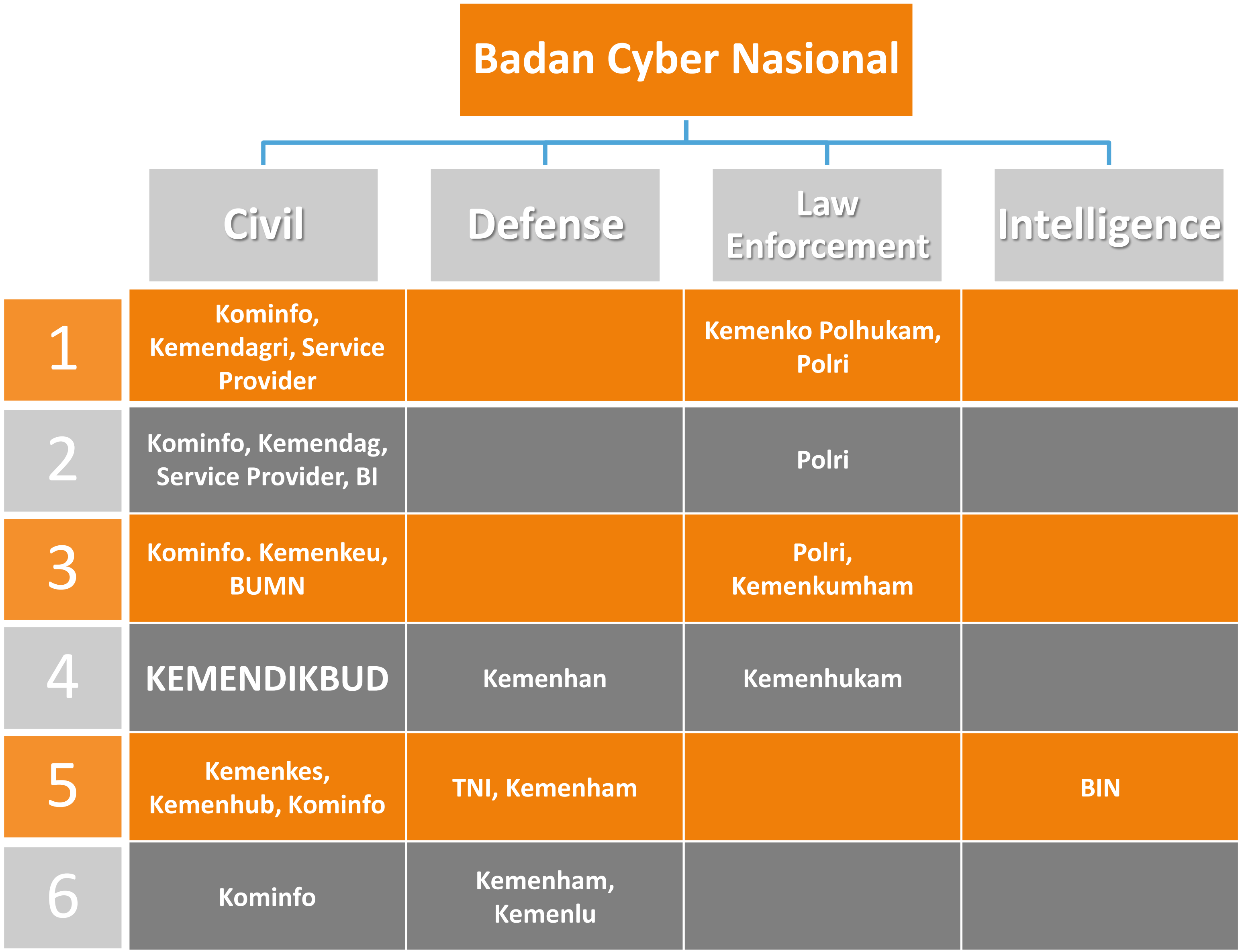
Prioritas 4

Program nasional pendidikan pelatihan tentang kesadaran keamanan *cyberspace*

Prioritas 5

Program nasional pendidikan pelatihan tentang kesadaran keamanan *cyberspace*

Prioritas 6: Kerjasama internasional untuk meningkatkan keamanan sistem *cyberspace*



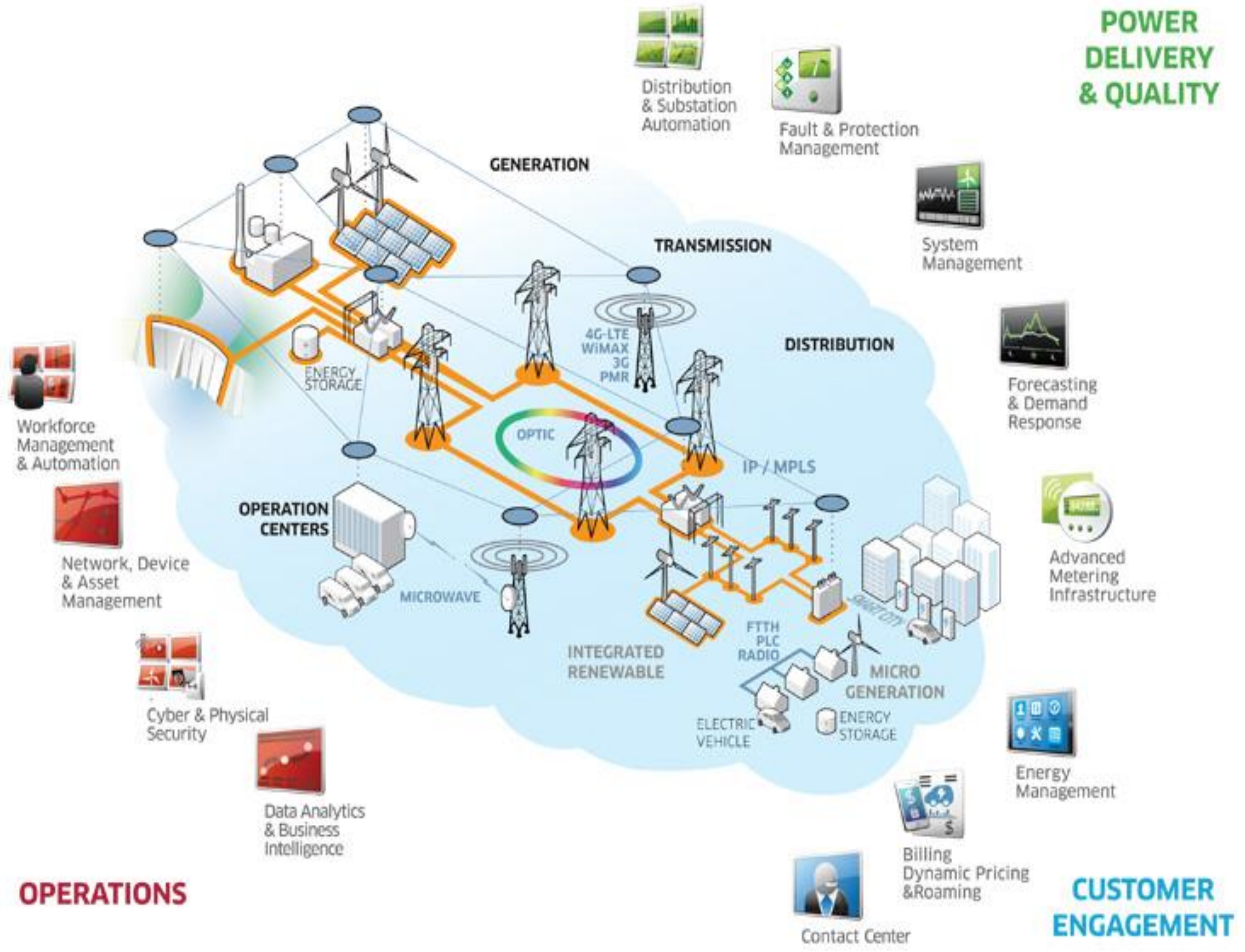
Badan Cyber Nasional

	Civil	Defense	Law Enforcement	Intelligence
1	Kominfo, Kemendagri, Service Provider		Kemenko Polhukam, Polri	
2	Kominfo, Kemendag, Service Provider, BI		Polri	
3	Kominfo. Kemenkeu, BUMN		Polri, Kemenkumham	
4	KEMENDIKBUD	Kemenhan	Kemenhukam	
5	Kemenkes, Kemenhub, Kominfo	TNI, Kemenham		BIN
6	Kominfo	Kemenham, Kemenlu		

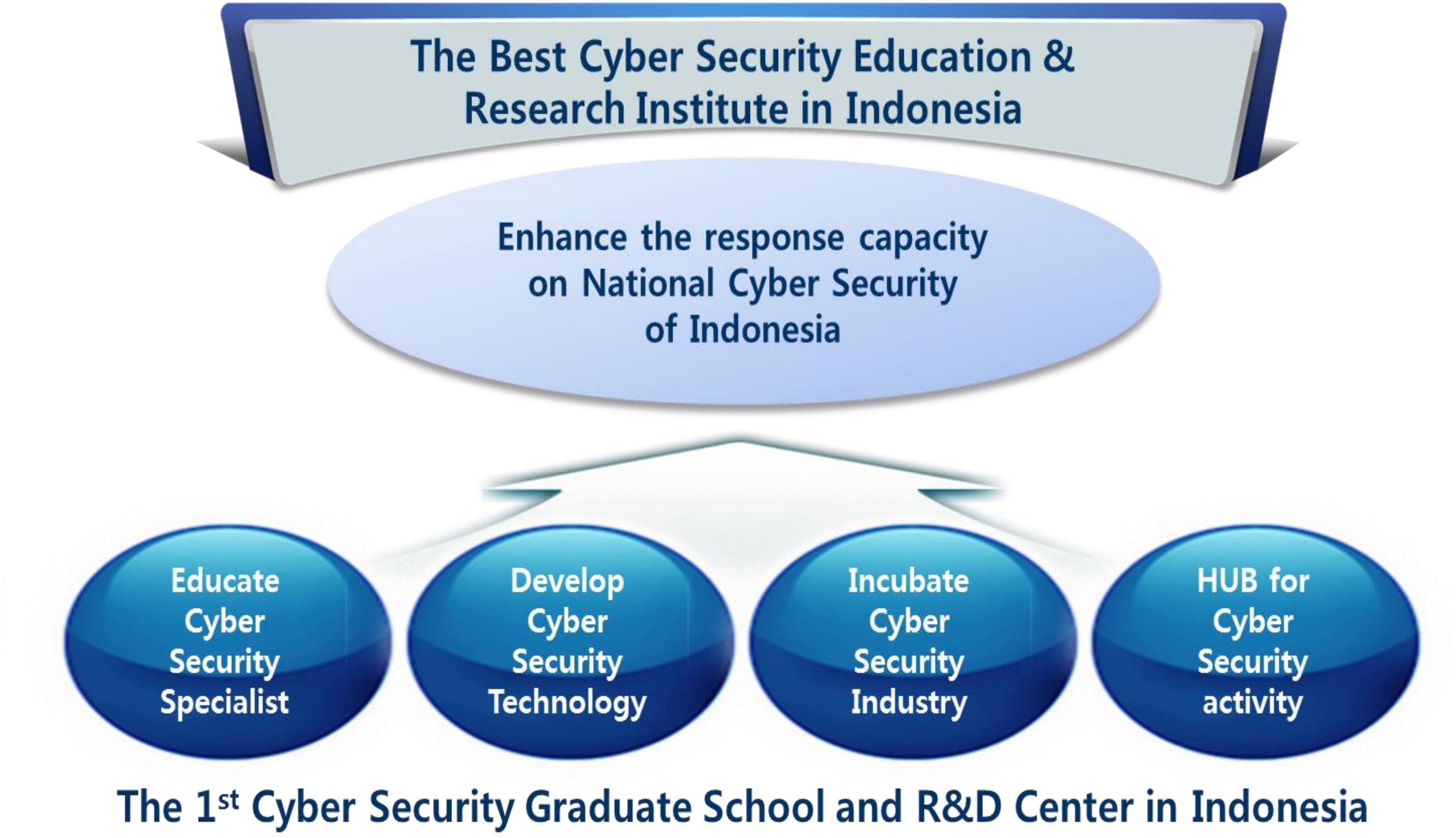
Critical Infrastructure

Kementrian	Sektor
Kementrian Komunikasi dan Informatika	Informasi dan Komunikasi (Komersial)
Kementrian Perhubungan, Kementrian Pekerjaan Umum	Transportasi (penerbangan, kereta api, infrastruktur jalan, dll)
Kementrian Kesehatan	Kesehatan
Kementrian Pertanian	Ketahanan Pangan
Kementrian Energi dan Sumber Daya Mineral	Energi dan Sumber Daya Mineral
Kementrian Lingkungan Hidup	Air bersih, Pengolahan limbah
Kementrian Pertahanan	Industri pertahanan
Kementrian Keuangan	Perbankan dan Keuangan
Kementrian BUMN	Industri Strategis (PTDI, PT. PAL, dll)

PLN SmartGrid



ITB Vision on InfoSec



The Best Cyber Security Education & Research Institute in Indonesia

Enhance the response capacity on National Cyber Security of Indonesia

Educate Cyber Security Specialist

Develop Cyber Security Technology

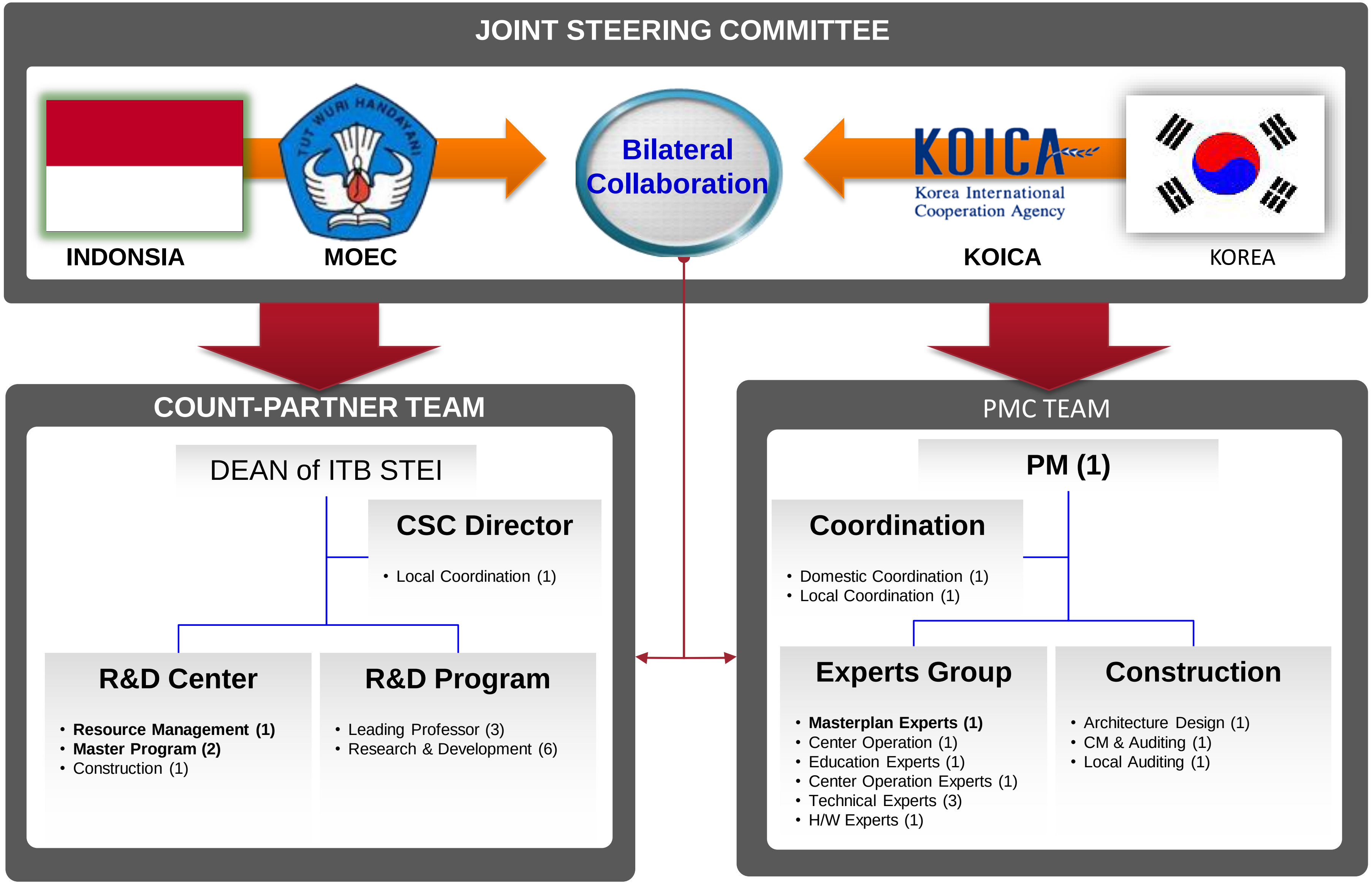
Incubate Cyber Security Industry

HUB for Cyber Security activity

The 1st Cyber Security Graduate School and R&D Center in Indonesia

ITB Cyber Security Center

Organization



JOINT STEERING COMMITTEE

INDONSIA

MOEC

Bilateral Collaboration

KOICA

KOREA

COUNT-PARTNER TEAM

DEAN of ITB STEI

CSC Director

- Local Coordination (1)

R&D Center

- **Resource Management (1)**
- **Master Program (2)**
- Construction (1)

R&D Program

- Leading Professor (3)
- Research & Development (6)

PMC TEAM

PM (1)

Coordination

- Domestic Coordination (1)
- Local Coordination (1)

Experts Group

- **Masterplan Experts (1)**
- Center Operation (1)
- Education Experts (1)
- Center Operation Experts (1)
- Technical Experts (3)
- H/W Experts (1)

Construction

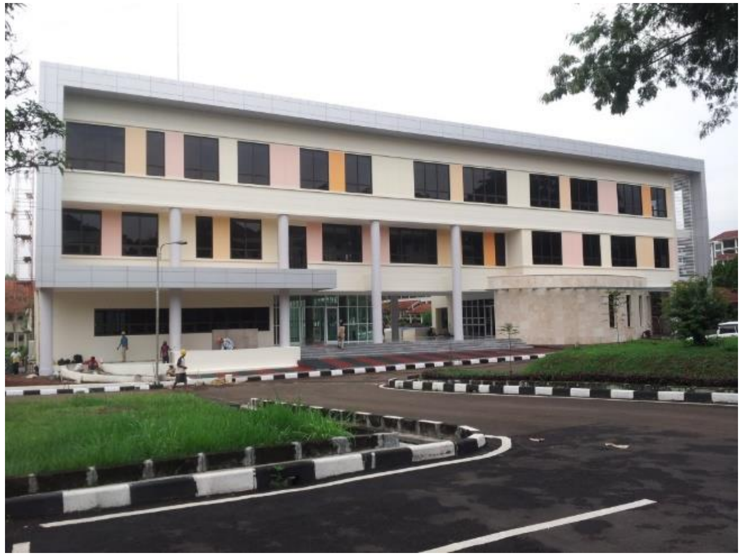
- Architecture Design (1)
- CM & Auditing (1)
- Local Auditing (1)

ITB CSC Center Construction

Ground Breaking Ceremony (Jan. 30th 2013)

GROUND BREAKING CEREMONY
OF "THE LABORATORY OF CYBER SECURITY CAPABILITY OF INDONESIA PROJECT" IN JATINANGOR, BANDUNG
Wednesday, 30 January 2013
KOICA

Construction Progress (10th Dec. 2013, Completed)



Masterplan

MASTERPLAN ACTIVITIES

❑To provide the education and R&D systems for ITB CSC

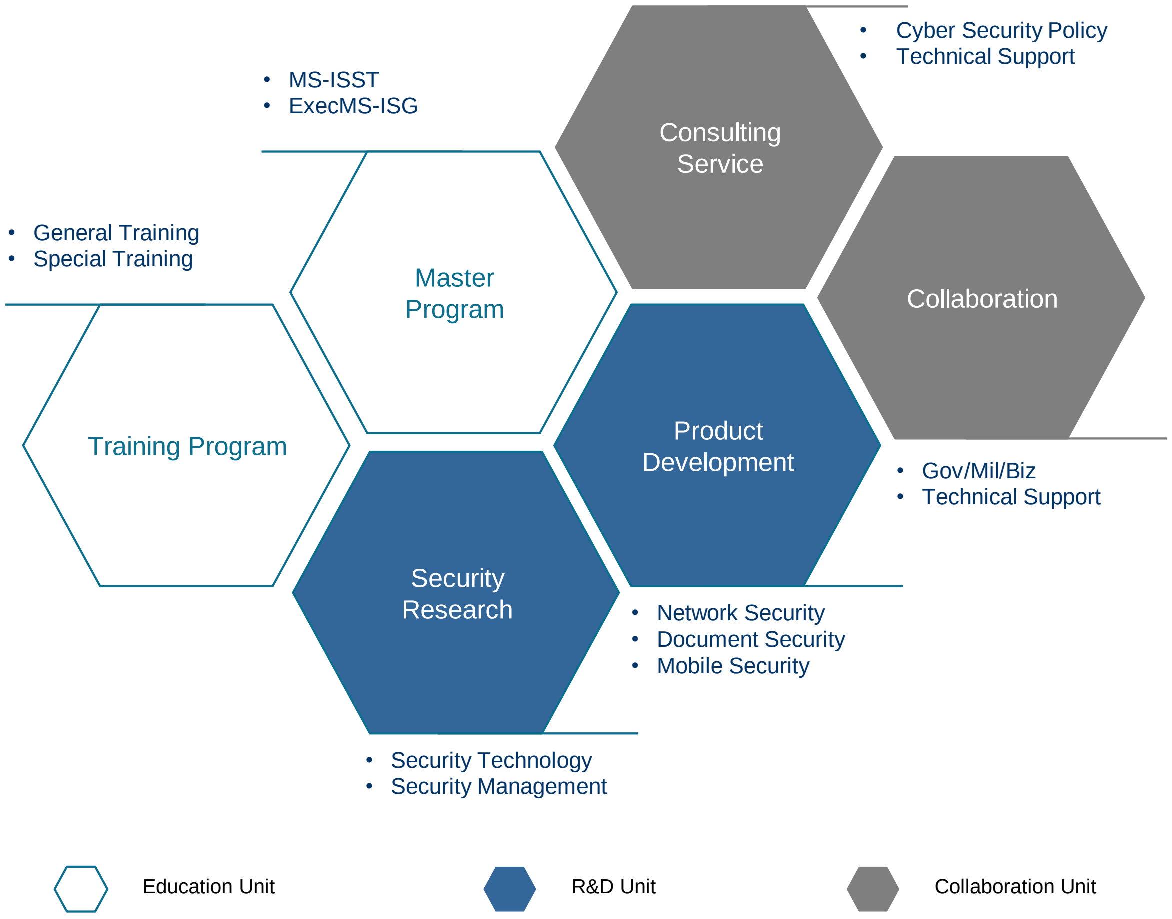
❑To provide operational strategy of ITB CSC

- Organization, Curriculum, R&D Program, Recruiting faculty and Student, Facilities and Equipment

❑To provide core strategy for ITB CSC's sustainability

- Strategy for financially independent center
- Promoting and Collaboration
- Long-term networking strategy

KOICA-ITB CSC SERVICE & PROGRAM - MASTERPLAN SETUP



Consulting Service

- Cyber Security Policy
- Technical Support

Master Program

- MS-ISST
- ExecMS-ISG

Training Program

- General Training
- Special Training

Collaboration

- Gov/Mil/Biz
- Technical Support

Product Development

- Network Security
- Document Security
- Mobile Security

Security Research

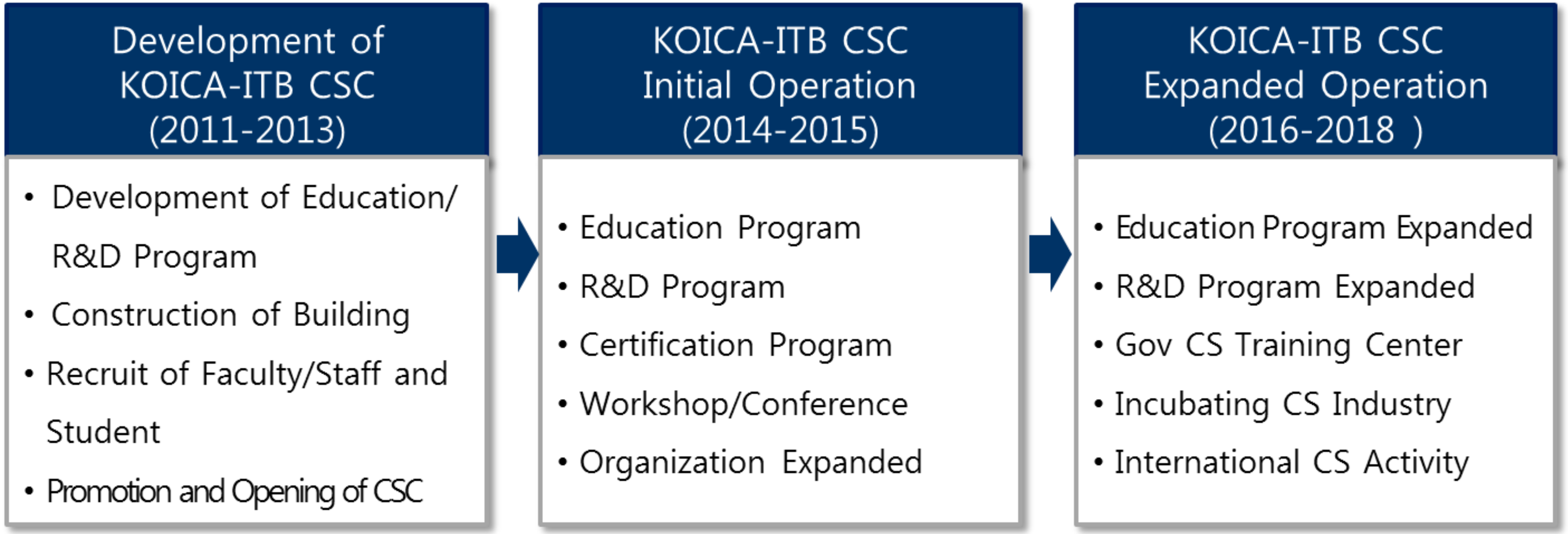
- Security Technology
- Security Management

⬡ Education Unit

⬢ R&D Unit

⬢ Collaboration Unit

Roadmap



Development of KOICA-ITB CSC (2011-2013)

- Development of Education/ R&D Program
- Construction of Building
- Recruit of Faculty/Staff and Student
- Promotion and Opening of CSC

KOICA-ITB CSC Initial Operation (2014-2015)

- Education Program
- R&D Program
- Certification Program
- Workshop/Conference
- Organization Expanded

KOICA-ITB CSC Expanded Operation (2016-2018)

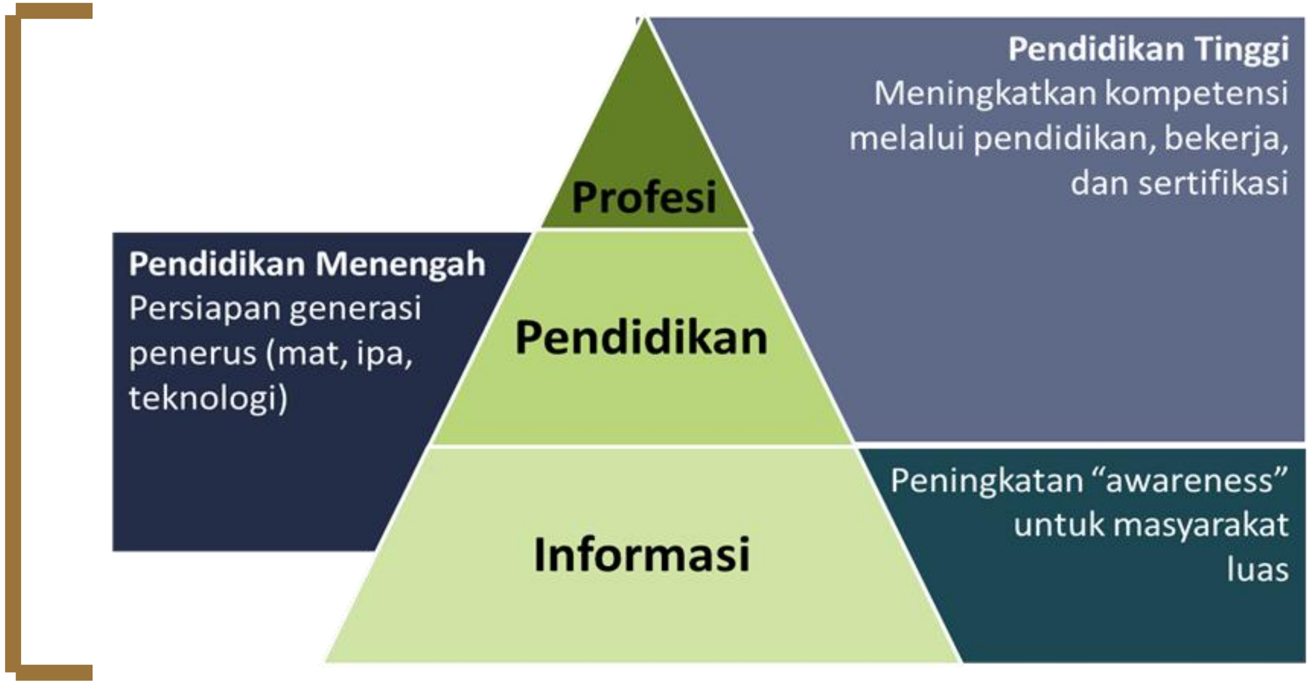
- Education Program Expanded
- R&D Program Expanded
- Gov CS Training Center
- Incubating CS Industry
- International CS Activity

Sumber Daya Manusia dan Awareness

Goal:

- Meningkatkan kesadaran akan resiko beraktifitas di dunia cyber
- Mempersiapkan sumber daya manusia yang capable dalam mendukung keamanan siber nasional
- Mengembangkan dan memelihara *cybersecurity workforce* yang kompetitif dan mampu bersaing secara global

Program peningkatan kapabilitas SDM dalam bidang keamanan siber dapat dibagi ke dalam tiga komponen penting


Pendidikan Tinggi
Meningkatkan kompetensi melalui pendidikan, bekerja, dan sertifikasi

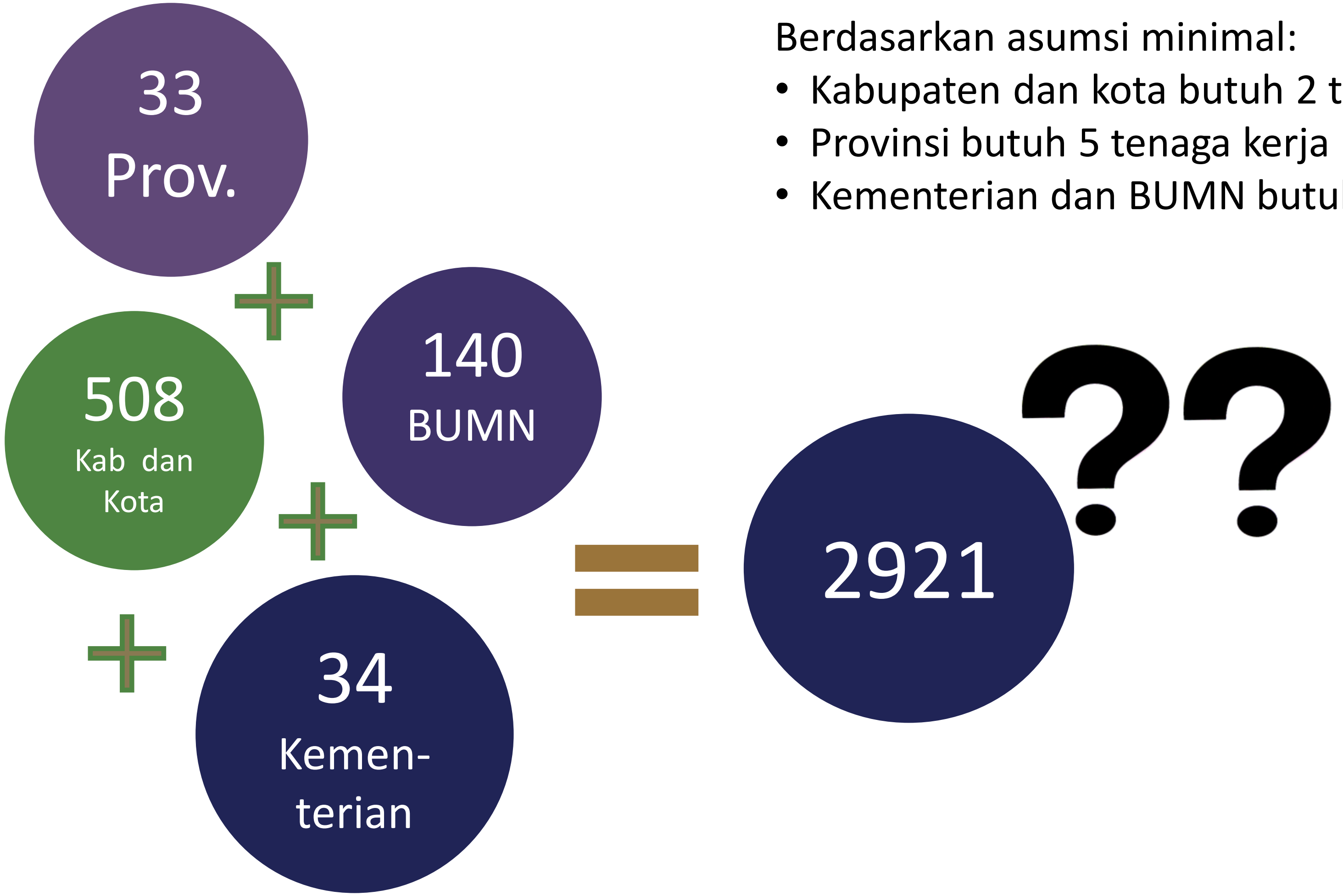
Pendidikan Menengah
Persiapan generasi penerus (mat, ipa, teknologi)

Peningkatan "awareness" untuk masyarakat luas

(Contoh) Kebutuhan Tenaga Kerja IT *Security* Indonesia

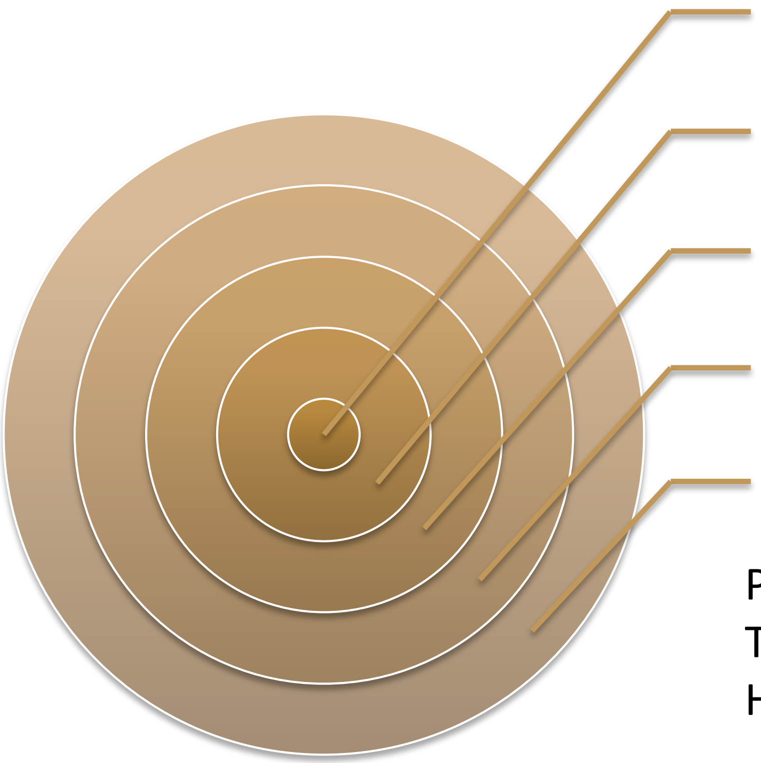
Berdasarkan asumsi minimal:

- Kabupaten dan kota butuh 2 tenaga kerja
- Provinsi butuh 5 tenaga kerja
- Kementerian dan BUMN butuh 10 tenaga kerja



33 Prov. + 508 Kab dan Kota + 140 BUMN + 34 Kemen-terian = 2921 ??

(Contoh) Kebutuhan Tenaga Kerja IT *Security* Indonesia



S3 : 300

S2 : 3,000 (10%)

S1 : 12,000 (25%)

S1 Teknik : 120,000 (10%)

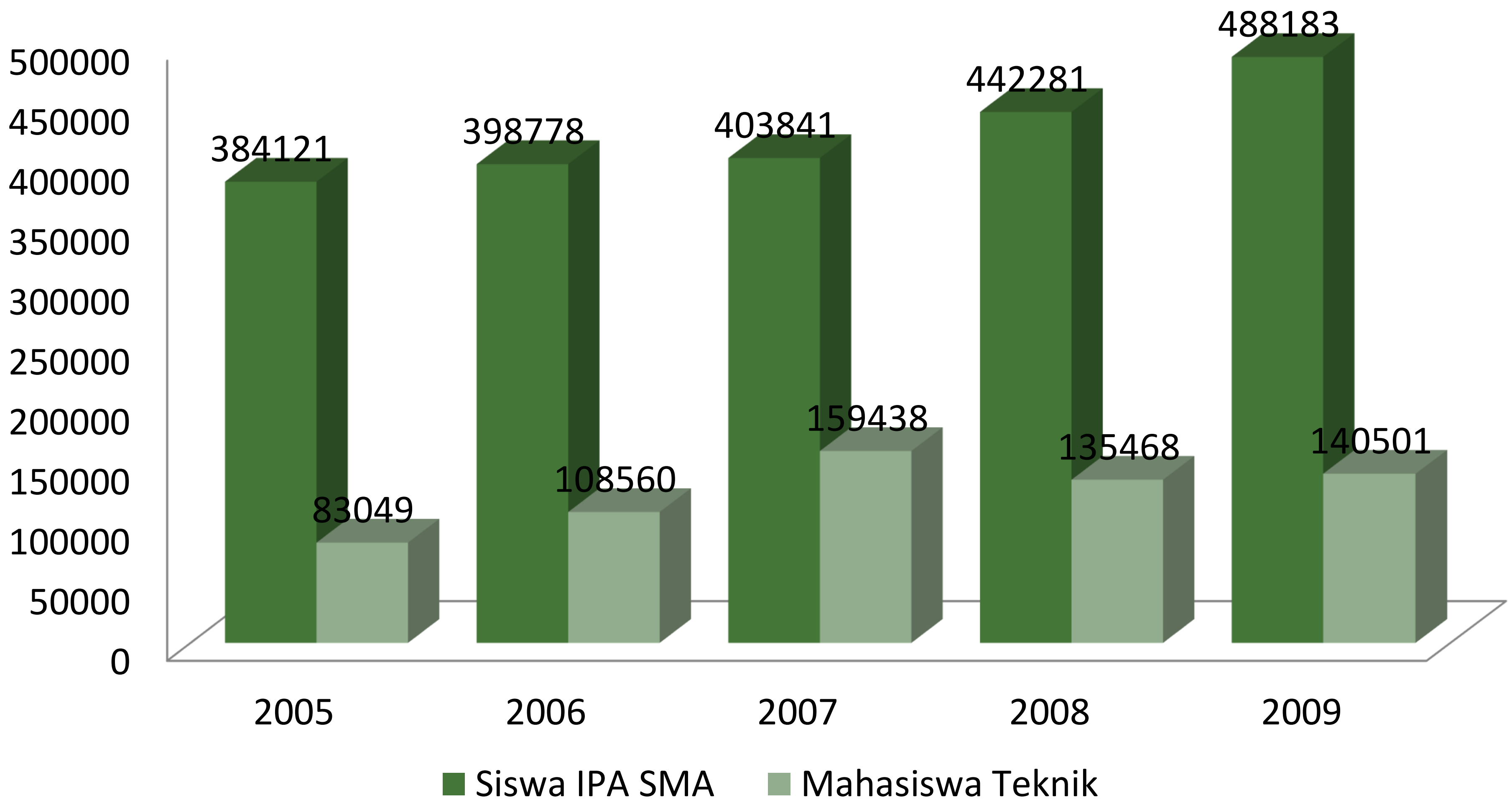
SMA IPA : 360,000 (30%)

Pengembangan kapabilitas riset dan industri keamanan:

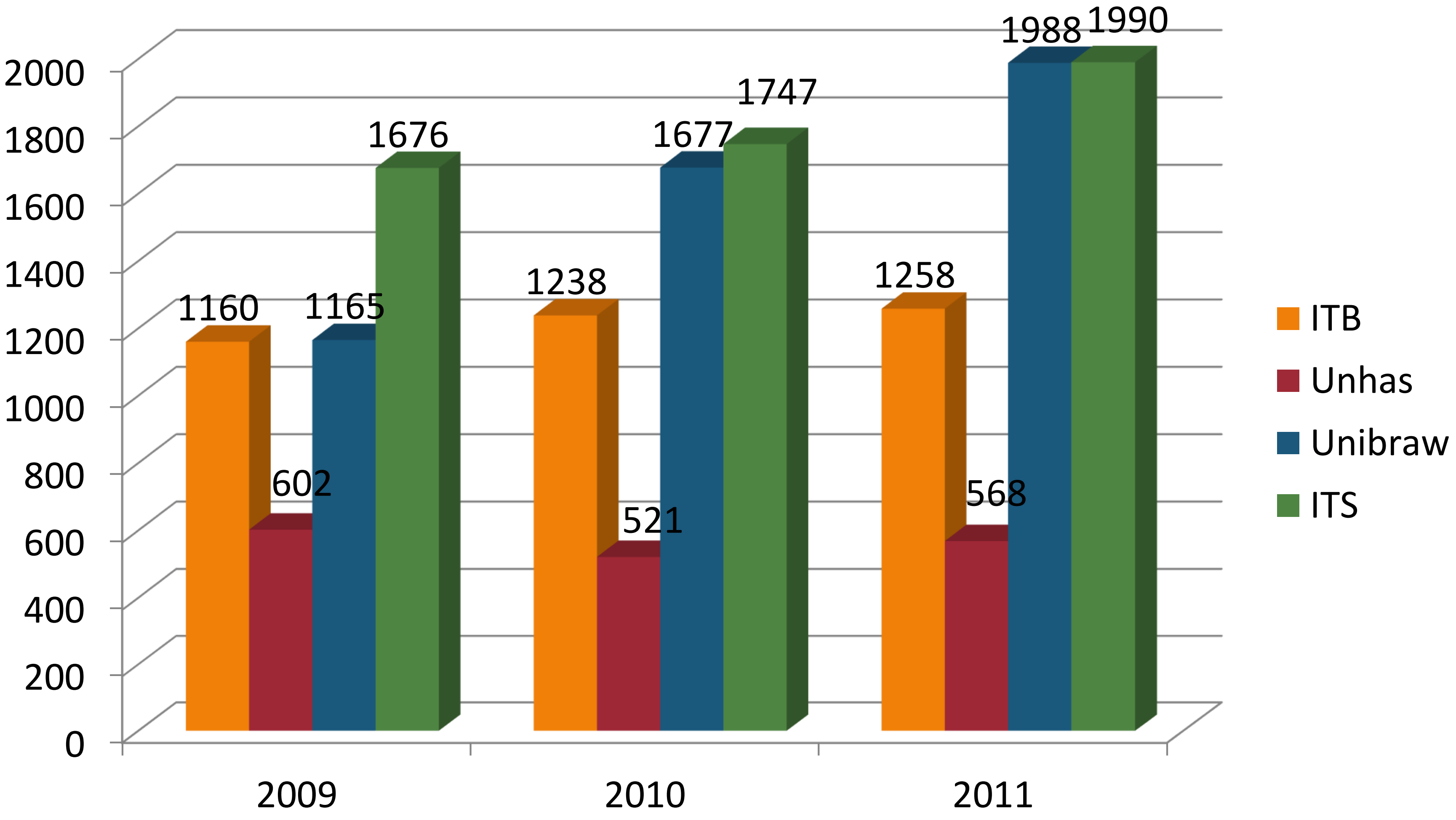
- Berbagai Negara ~ 3000 S3 per bidang
- Indonesia ~ 10% == 300 S3 per bidang

Perkiraan siswa IPA 450,000 per tahun
Tidak mungkin 70% masuk ke satu bidang
Harus menaikkan jumlah siswa IPA + jangka panjang

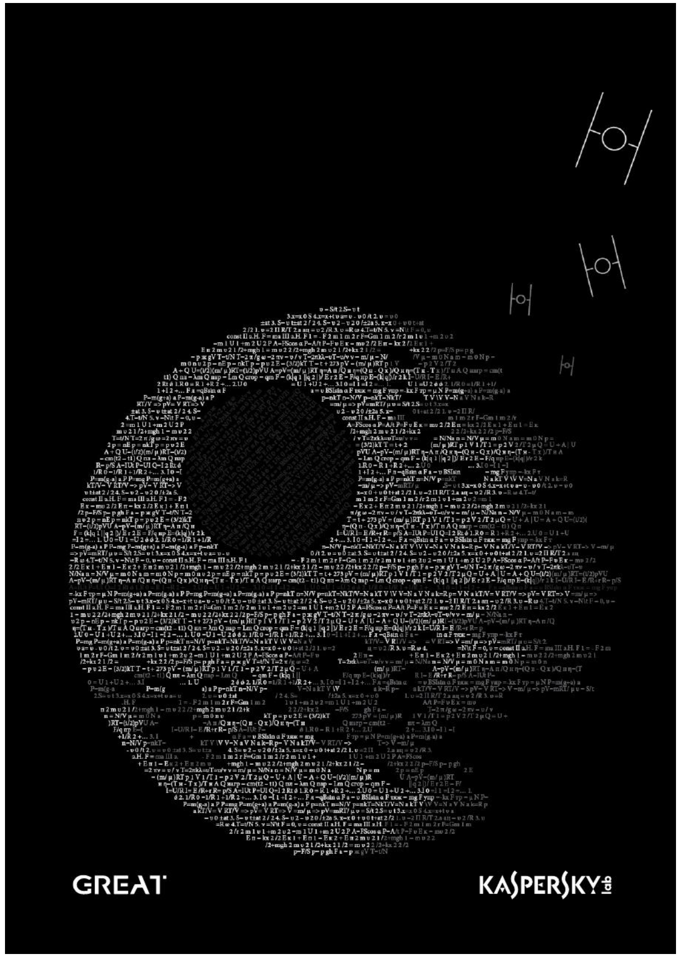
Grafik Beberapa Tahun Terakhir



Jumlah Mahasiswa Baru yang Berhubungan dengan IT Security



Kompetensi SDM ?



Who is the Equation Group?

Kaspersky declined to outright name the United States National Security Agency (NSA) as the governing body behind the Equation Group, but there are a number of factors that point to the NSA as the responsible party.

Read more at http://observer.com/2015/02/equation-group/#ixzz3XM9qc2B5

Equation group victims map

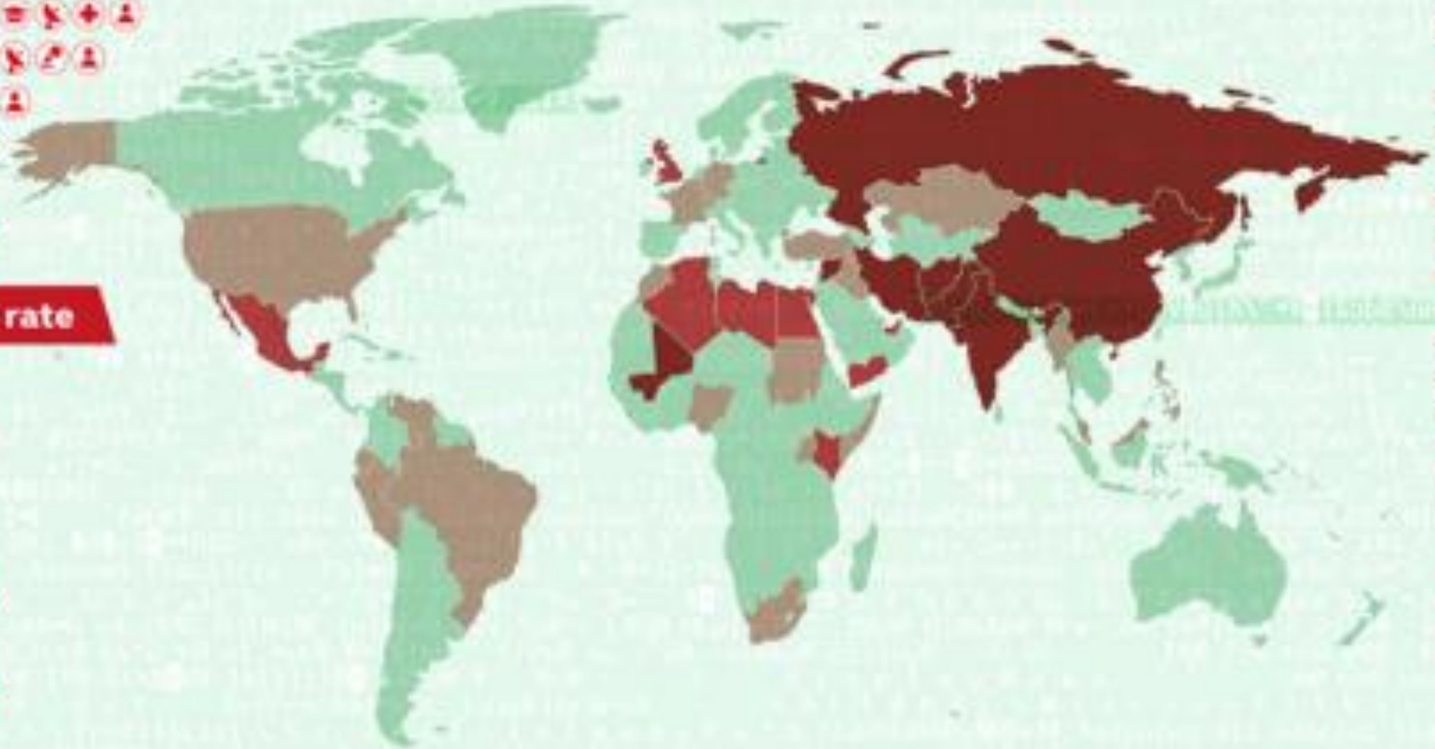
- Finance
- Government
- Diplomatic / Embassies
- Research institution
- Energy / Infrastructure
- University
- Military
- Aerospace
- Telecommunications
- Medical
- Islamic Scholars
- Media
- Other / Unknown

High infection rate

Iran	Finance, Government, Diplomatic / Embassies, Research institution, Energy / Infrastructure, University, Aerospace, Telecommunications, Other / Unknown
Russian Federation	Government, Research institution, Energy / Infrastructure, University, Military, Aerospace, Telecommunications, Medical, Other / Unknown
Pakistan	Government, Research institution, Energy / Infrastructure, University, Telecommunications, Medical, Other / Unknown
Afghanistan	Finance, Government, Diplomatic / Embassies, Telecommunications, Media, Other / Unknown
India	Research institution, Military, Aerospace, Other / Unknown
China	Diplomatic / Embassies, Other / Unknown, University
Syria	Diplomatic / Embassies, Other / Unknown
Mali	Government, Telecommunications, Other / Unknown

Medium-level infection rate

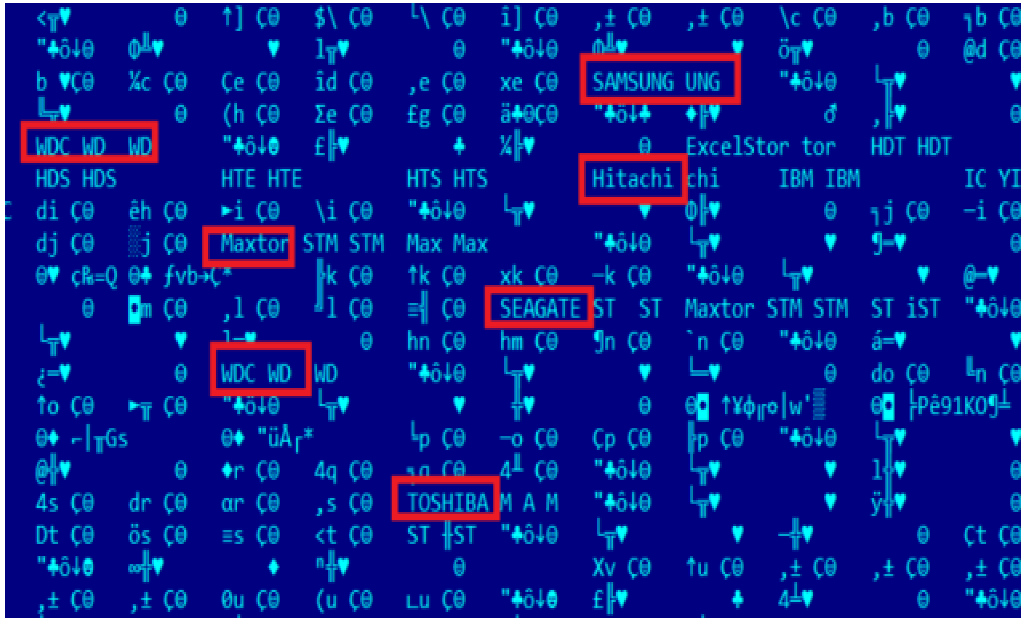
Lebanon	Other / Unknown
Yemen	Telecommunications, Other / Unknown
United Arab Emirates	Media, Other / Unknown
Algeria	Energy / Infrastructure, Other / Unknown
Kenya	Government, Other / Unknown
United Kingdom	Finance, Islamic Scholars, Other / Unknown
Libya	Military, Other / Unknown
Mexico	Finance, Government, Other / Unknown
Qatar	Other / Unknown
Egypt	Military, Other / Unknown



Low infection rate

Government, Other / Unknown	Turkey
Telecommunications, Other / Unknown	Somalia
Other / Unknown	Myanmar
Telecommunications, Other / Unknown	Germany
Other / Unknown	South Africa
Military, Other / Unknown	Nigeria
Islamic Scholars, Other / Unknown	United States
Other / Unknown	Venezuela
Telecommunications, Other / Unknown	Sudan
Media, Other / Unknown	Palestinian
Government, Diplomatic / Embassies	Morocco
Other / Unknown	Malaysia
Energy / Infrastructure, Other / Unknown	Kazakhstan
Finance, Aerospace	Iraq
Aerospace, Other / Unknown	Brazil
Other / Unknown	Uganda
Other / Unknown	Switzerland
Other / Unknown	Singapore
Other / Unknown	Philippines
Other / Unknown	Peru
Other / Unknown	France
University	Equador
Finance	Belgium
Other / Unknown	Bahrain

Why are these hackers so frightening than others?



- The first is just how deep their work penetrates a computer system. Kaspersky uncovered Equation Group malware that infiltrates a system’s firmware, or the software that loads before your OS even has a chance to boot up.

Read more at http://observer.com/2015/02/equation-group/#ixzz3XMBk5T9D

Apa itu RMKI?

REKAYASA:

- KRIPTOGRAFI DAN APLIKASINYA
- SECURE SOFTWARE & OS SECURITY
- DIGITAL FORENSIC & COMPUTER CRIME, DSB...

+

MANAJEMEN:

- INFORMATION SECURITY MANAGEMENT
- INFORMATION SYSTEM ASSURANCE
- SECURITY ARCHITECTURE AND DESIGN

=

VISI

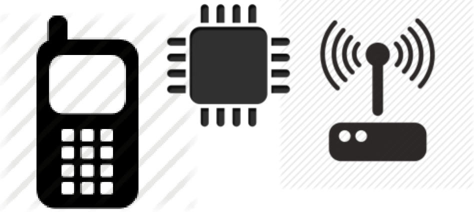
Meningkatkan Sumber Daya Manusia untuk Menjamin Keamanan Sistem Informasi Nasional Masa Depan

*Rekayasa dan Manajemen Keamanan Informasi

Output Program RMKI:

Output Program RMKI:

Hardware berbasis security

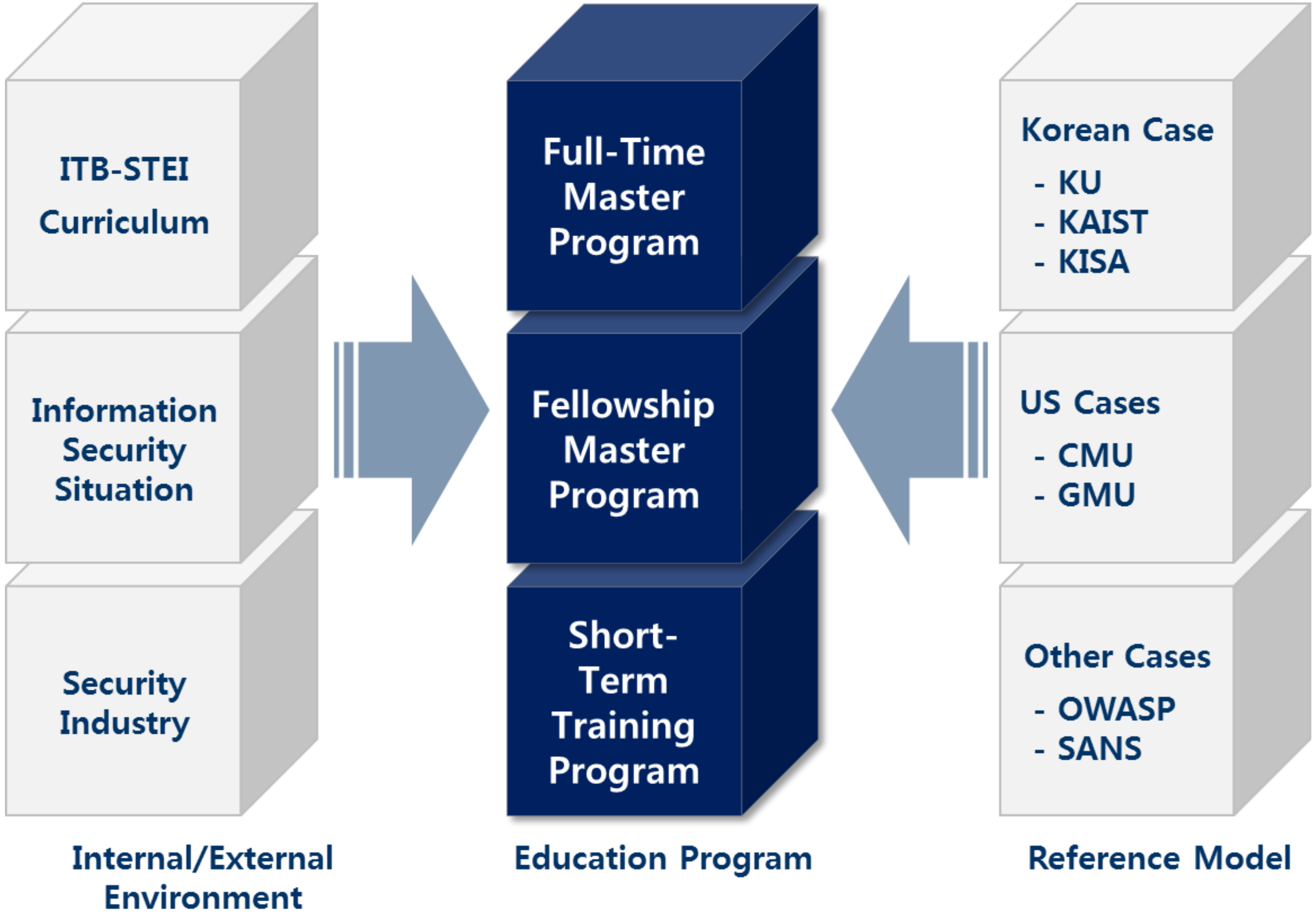


Software berbasis security

Manajemen berbasis security

Education Program

Bachelor, Masters, Doctoral, Training, Cont. Education



ITB-STEI Curriculum

Information Security Situation

Security Industry

Internal/External Environment

Full-Time Master Program

Fellowship Master Program

Short-Term Training Program

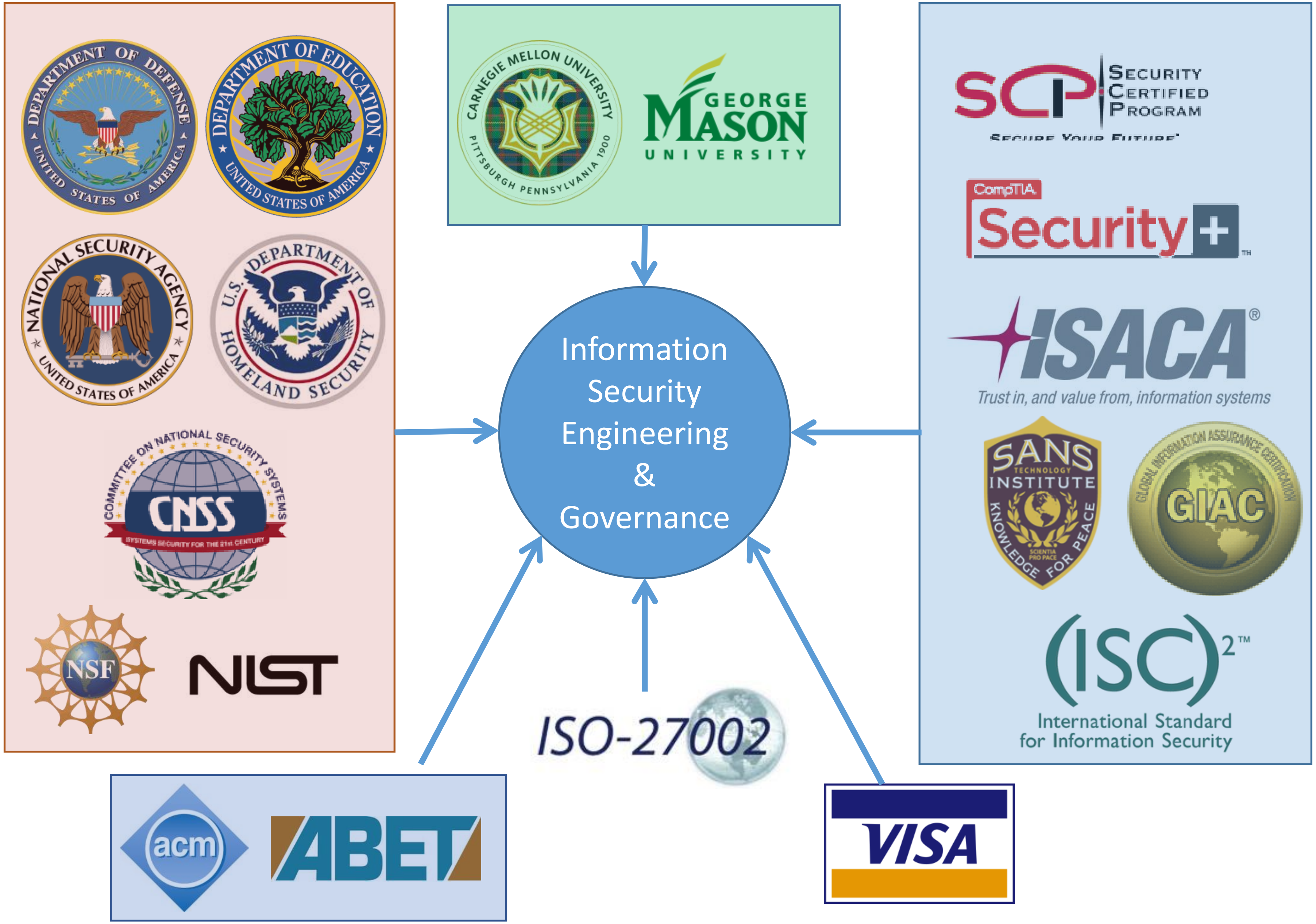
Education Program

Korean Case
- KU
- KAIST
- KISA

US Cases
- CMU
- GMU

Other Cases
- OWASP
- SANS

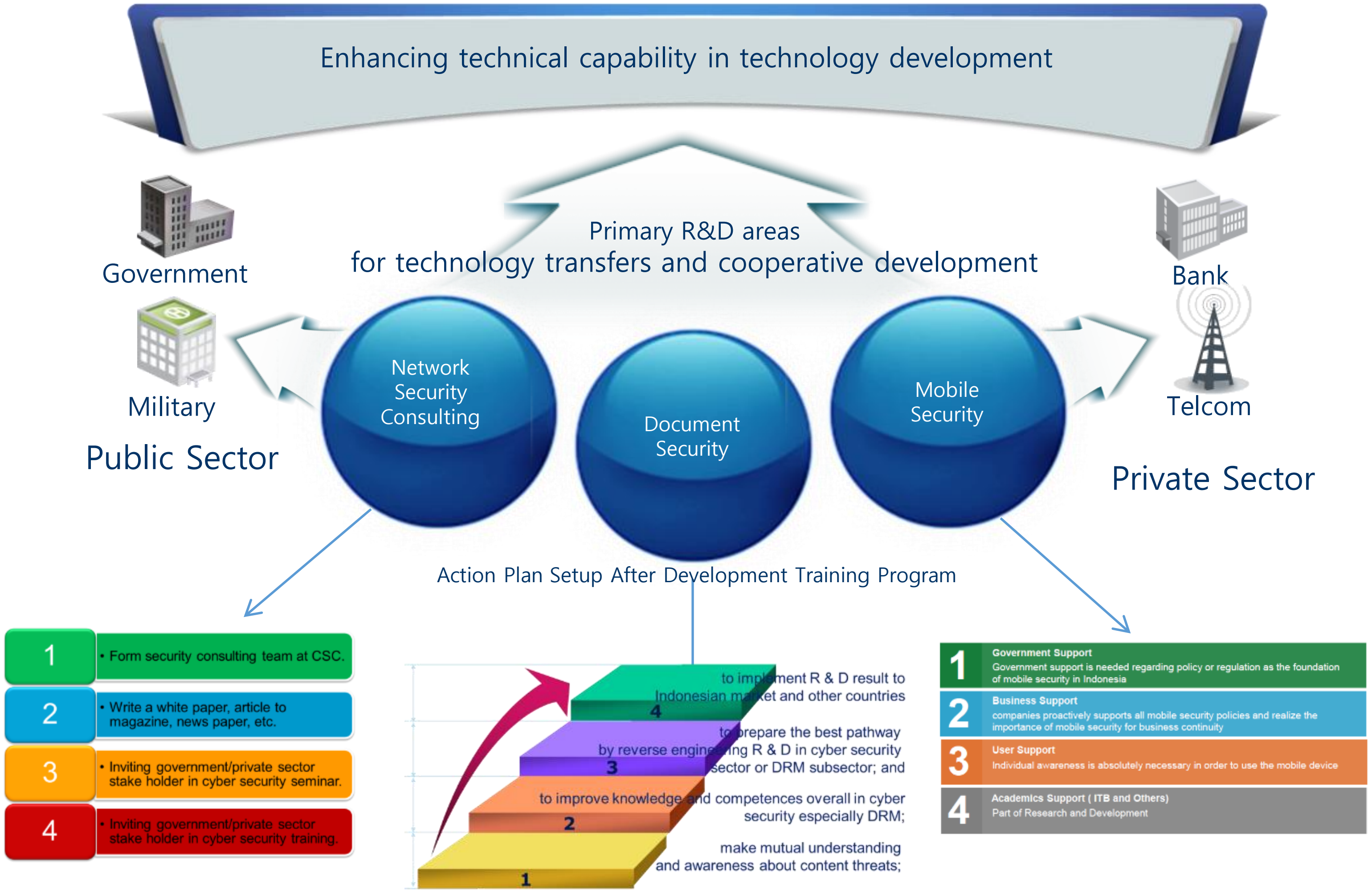
Reference Model



Information Security Engineering & Governance

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
DEPARTMENT OF EDUCATION UNITED STATES OF AMERICA
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA
U.S. DEPARTMENT OF HOMELAND SECURITY
COMMITTEE ON NATIONAL SECURITY SYSTEMS
CNSS
SYSTEMS SECURITY FOR THE 21st CENTURY
NSF
NIST
CARNEGIE MELLON UNIVERSITY PITTSBURGH PENNSYLVANIA 1900
GEORGE MASON UNIVERSITY
SCP SECURITY CERTIFIED PROGRAM
SECURE YOUR FUTURE
CompTIA Security+
ISACA
Trust in, and value from, information systems
SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
(ISC)²
International Standard for Information Security
ISO-27002
acm
ABET
VISA

R&D Program & Development



Enhancing technical capability in technology development

Primary R&D areas
for technology transfers and cooperative development

Action Plan Setup After Development Training Program

1 • Form security consulting team at CSC.

2 • Write a white paper, article to magazine, news paper, etc.

3 • Inviting government/private sector stake holder in cyber security seminar.

4 • Inviting government/private sector stake holder in cyber security training.

4 to implement R & D result to Indonesian market and other countries

3 to prepare the best pathway by reverse engineering R & D in cyber security sector or DRM subsector; and

2 to improve knowledge and competences overall in cyber security especially DRM;

1 make mutual understanding and awareness about content threats;

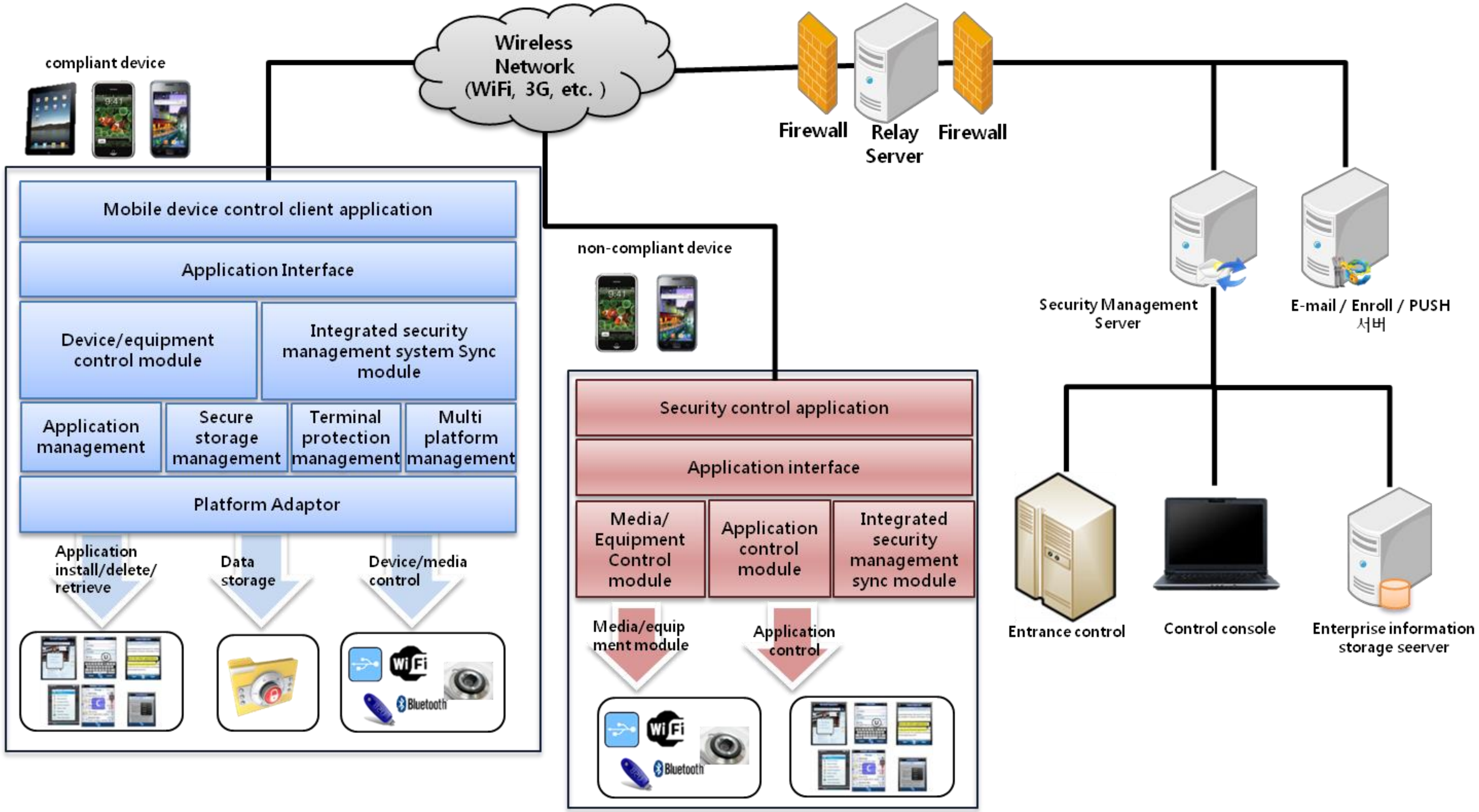
1 **Government Support**
Government support is needed regarding policy or regulation as the foundation of mobile security in Indonesia

2 **Business Support**
companies proactively supports all mobile security policies and realize the importance of mobile security for business continuity

3 **User Support**
Individual awareness is absolutely necessary in order to use the mobile device

4 **Academics Support (ITB and Others)**
Part of Research and Development

Doctoral Research on Mobile Security

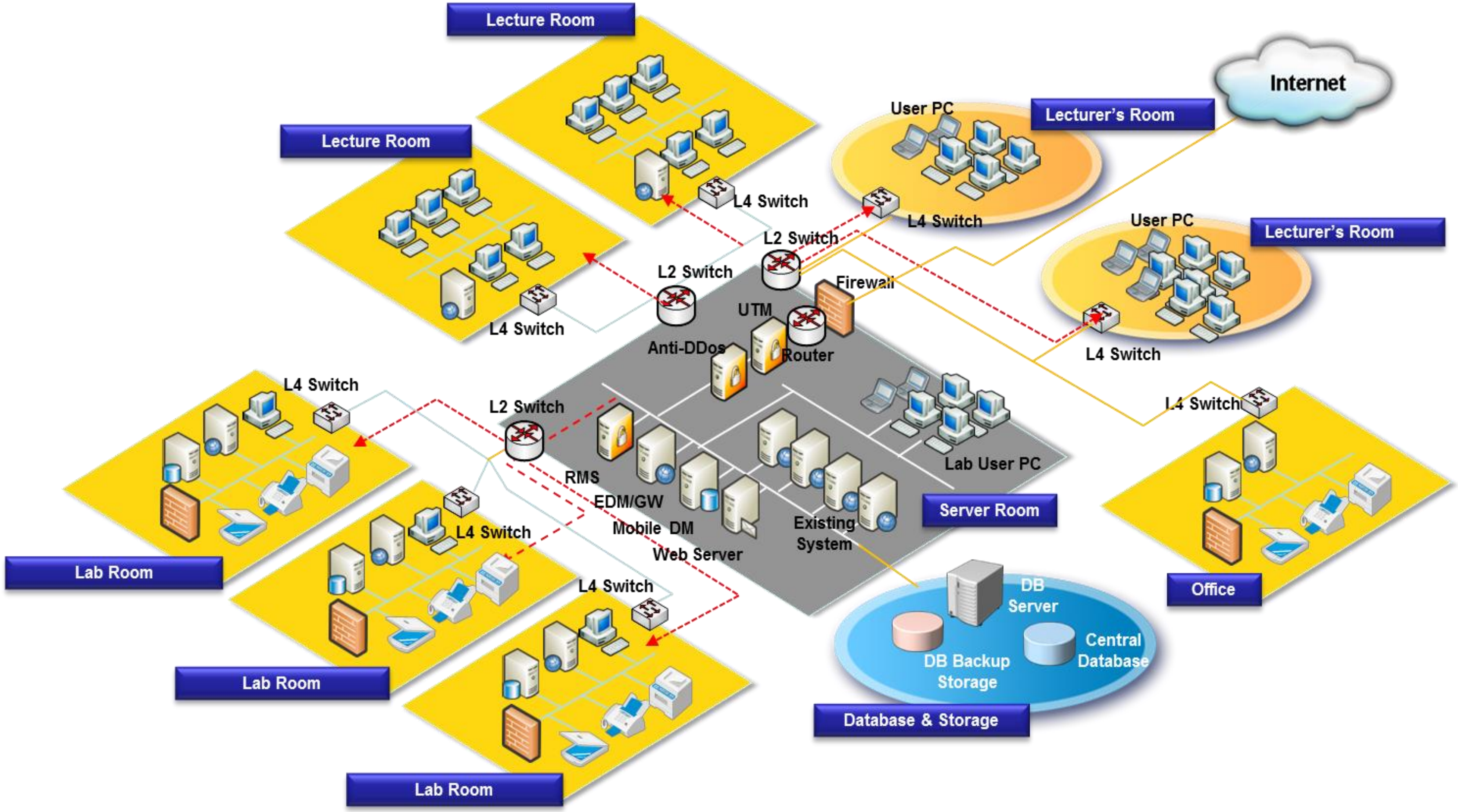


compliant device
Wireless Network (WiFi, 3G, etc.)
Firewall
Relay Server
Firewall
Mobile device control client application
Application Interface
Device/equipment control module
Integrated security management system Sync module
Application management
Secure storage management
Terminal protection management
Multi platform management
Platform Adaptor
Application install/delete/ retrieve
Data storage
Device/media control
non-compliant device
Security control application
Application interface
Media/ Equipment Control module
Application control module
Integrated security management sync module
Media/equip ment module
Application control
Security Management Server
E-mail / Enroll / PUSH 서버
Entrance control
Control console
Enterprise information storage seerver

International Research Collaboration

- Processor’s Secure Zone & Trusted Computing
- MDM-EISP (Mobile Device Management – Enterprise Internal Secure Platform)
- KOICA-KISA-KR-CERT ITB-INA-CERT
- Cyber Patrol Collaboration
- Asymmetric Persistent Threats
- Hacking and Anti-Hacking Technology
- Cyber Forensic

Equipment


Lecture Room
Lecture Room
Internet
User PC
Lecturer's Room
L4 Switch
L4 Switch
L2 Switch
L2 Switch
User PC
Lecturer's Room
Firewall
UTM
Router
Anti-DDos
L4 Switch
L4 Switch
L4 Switch
L2 Switch
L4 Switch
Lab User PC
RMS
EDM/GW
Mobile DM
Web Server
Existing System
Server Room
Office
L4 Switch
L4 Switch
Lab Room
DB Server
Central Database
DB Backup Storage
Database & Storage
Lab Room
Lab Room

Thank You

INSTITUT TEKNOLOGI BANDUNG

1920