Cyber Defence:
Trends & Global Warfare

Outline

- Art of the war
- Cyber Warfare
- Cyber Battleground
- Cyber War Weapon
- Cyber War Phenomenon
- Cyber Defence
- Q & A
- References

Pasal 1:

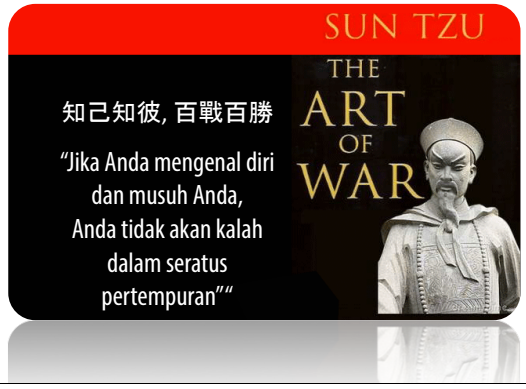
Tidak ada komputer yang aman

Pasal 2:

Kalau ada orang yang mengatakan bahwa komputernya aman, harap kembali ke Pasal 1.

Art of the war…

Sun Tzu Bingfa…..



是故）百戰百勝，非善之善者也；不戰而屈人之兵，善之善者也

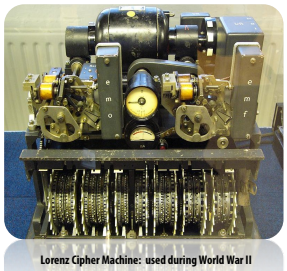
"Bertempur dalam seratus pertempuran dan memenangkan seratus kemenangan bukanlah suatu cerminan strategi yang paling hebat. Kemampuan untuk mengalahkan musuh tanpa pertempuran sama sekali adalah cerminan strategi yang paling hebat"

Sun TZu Bingfa (philosophy)

1. Perdaya Langit untuk melewati Samudera
2. Pinjam tangan seseorang untuk membunuh
3. Gunakan kesempatan saat terjadi kebakaran untuk merampok lainnya
4. Berpura-pura menyerang dari timur dan menyeranglah dari barat
5. Pantau api yang terbakar dari seberang sungai
6. Pisau tersarung dalam senyum
7. Permainkan harimau untuk meninggalkan sarangnya
8. Pada saat menangkap, lepaslah satu orang
9. Melempar Batu Bata untuk mendapatkan Giok
10. Lukai diri sendiri untuk mendapatkan kepercayaan musuh

War in evolution…

History



Lorenz Cipher Machine: used during World War II

French Cyber Machine : 16 Century

Enigma: Cryptanalysis Machine

Cyber Warfare….

Is Cyber Warfare Best Strategy?

Cyber Warfare Characteristics

- No Command
- Difficult to identify private or state sponsored hacking
- Citizens of other regions and countries can also volunteer

Cyber Targets

- Military Networks
- Government Systems and Websites
- Ecommerce and Financial Institutes
- Telecommunication Companies
- Transportation System
- **Business Network Infrastructure**
- Others

Modern Warfare Motivations

- For fun (**31.4**%)
- Want to be best defacer (**17.2**%)
- No reason specified (**14.7**%)
- Political peasons (**11.8**%)
- Patriotism (**10.9**%)
- As a challenge (**10.8**%)
- Revenge (**3.3**%)

Cyber Weapons

- **Software Based Weapons**
  - Availability
  - Capability
- **Hardware Based Weapons**
  - Availability
  - Cost of Manufacturing
  - Capability

Cyber Battleground…

Palestine And Israel

History

- 28th September 2000 – Israeli teenage hackers attacked Hezbollah and Hamas websites in Lebanon.
- Call for Cyber Jihad from Palestine

The Middle East Cyber War

- Elite Hackers around 100
  - *–How Elite Hackers work?*
- Volunteers around 1200
  - *–How Volunteers work?*

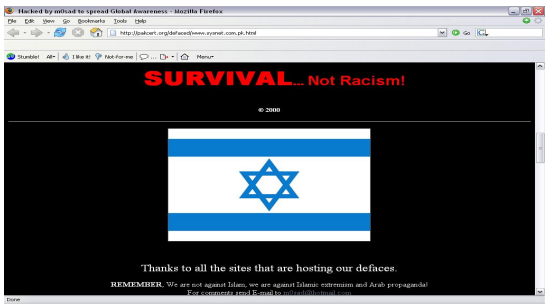
Targets in Middle East Conflict

- **Pro-Israeli Attacks**
  - –Extremist Websites
  - –Government Websites
- **Pro-Palestinian Attacks**
  - –Israeli official Websites
  - –Media, technology, financial and telecommunication corporations

Middle East Cyber War- A Global Cyber War

Israeli Hackers

- Mossad
- Wizel
- Israel Hackers United
- Israeli Internet Underground
- Small Mistake
- Analyzer
- ViRii



Targets of Israeli Hackers

- Government Systems
- Palestinian National Authority
- HAMAS
- Hizballah
- VISA

Pro-Palestinian Hackers

- G-Force Pakistan
- Dr. Nuker
- Pakistani Hackerz Club
- Arab Hackers
- Xegypt
- Arab Hax0rs
- Al-Muhajiroun

Palestinian Targets

- Israeli Army
- Israeli Central Bank
- Bank of Israel
- Israel's Educational Institutes
- Government System
- AT&T
- TA Stock Exchange

Counter Attack

- Pro-Palestinians hacked more than 50 websites.
- Paralyzed Israel's email system for days many times
- Israel's e-commerce websites

Israel: Cyber Target

- Extensive targets
- Israel **losing** the cyber war
- Hackers of all Arab countries combined

Cyber Battleground of China, Cuba And USA

How Cuba is better than USA in Cyber Warfare?

Bejucal Base

- 1100 engineers, computer scientists, technicians, staff
- Three groups of antennas/satellites.
  - General USA telecommunications
  - Pre Designated phones and computers
  - Voice recognition capacity
  - Ability to interfere USA computer networks

Paseo

- Transmission and reception of radio waves
- Ability to interfere radio telecommunications in USA, mainly in airports and strategic places.

Cojimar Electronic Complex

- Research Department
- Main focus High Radio Frequency

Wajay Electronic Base

- Weather Change Research
- Radio Interference
- More than 100 very high antennas

Chinese in Cuba

- Mutual Understanding
- Trade Cooperation
- Financial Support
- Strategic Location

What FBI hates more than Osama Bin Laden?

Capabilities and interests of Al Qaeda

- Training Process
  - Khalid Sheikh Mohammed
  - PhD Cyber Security
- Reconnaissance of critical infrastructures
- Communications and Cryptography techniques
- Cyber Propaganda
- Call for Jihad
- How Bin Laden is better than NSA in Tech

Capabilities and interests of Al Qaeda

- Big Damage……less investment
- High Anonymity

Al Qaeda's Cryptography

- Cryptography Techniques and methods used
- Example

These three tools bolster the original 'Mujahideen Secrets' tool that have primarily been used for email by Al-Qaeda since 2007.

NEW Al-Qaeda ENCRYPTION TOOLS

1. **Tashfeer al-Jawwal,** a mobile encryption platform developed by the Global Islamic Media Front (GIMF) and released in September 2013.
2. **Asrar al-Ghurabaa**, another alternative encryption program developed by the Islamic State of Iraq and Al-Sham and released in November 2013, around the same time the group broke away from the main Al-Qaeda following a power struggle.
3. **Amn al-Mujahid,** an encryption software program developed by Al-Fajr Technical Committee which is a mainstream al Qaeda organization and released in December 2013.

The massive surveillance conducted by the *National Security agency* may lead to the change in communication behavior of terrorists and criminals. Cybercriminals have to just secure their communication before performing any crime, Whereas terrorists need an undetectable communications along with the secure one, because for them nothing is more important than operational security.

Cyber Attacks on Al-Qaeda by US

- Bin Laden's Financial Network
- Damage to Financial Network of Bin Laden by U.S Hackers
- Calls Interception
- Decrypting Messages
- Avenues for US hackers by Al Qaeda

Cyber War Weapons…

Modern Weapons Economics


What does a stealth bomber cost? **$1.5 to $2 billion**


What does a stealth fighter cost? **$80 to $120 million**


What does an cruise missile cost? **$1 to $2 million**


What does a cyber weapon cost? **$300 to $50,000**

Find the Weapons Facility

Nuclear Weapons Facility

Cyber Weapons Facility

Where's the Cyber Weapons Facility?

45

Messages

- Cyberwar adalah sebuah ide evolusioner penting yang memiliki potensi untuk efek signifikan pada warga dunia,
- Cyberattacks di tingkat cyberwar sudah terjadi, dan sedang terjadi dengan meningkatnya frekuensi dan efek,
- Cyberwar dapat digunakan sebagai tuas politik bagi peningkatan kontrol pemerintah mengenai dunia maya

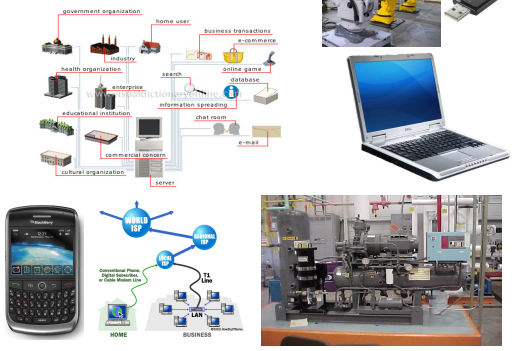
Definition of Cyber Warfare

- "***Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption***" – Richard A. Clarke, "Cyber War"
- "… a new domain in warfare" – William J. Lynn, U.S. Deputy Secretary of Defense

Related Terms and Issues

- **Cyber-terrorism – parallel definition, different actor**
  - actions by *terrorists* to penetrate another nation's computers or networks for the purposes of causing damage or disruption
- **Cyber-spying / cyber-espionage**
  - actions by *parties outside of a country or organization* to penetrate another nation's computers or networks for the purposes of stealing information
- **Increasingly difficult to distinguish countries and organizations**
  - Countries may be (increasing evidence that they are) using 3rd parties (organized crime, other organizations) to do their work

Cyberspace



Cyber War Phenomenon…

Titan Rain (2003-on)

- Serangan terkoordinasi pada militer AS dan sistem komputer industri
- Mendapatkan akses untuk sistem komputer dan jaringan, termasuk Lockheed Martin, Sandia National Laboratories, dan NASA
- Tujuan dan identitas penyerang masih belum jelas, meskipun asal tampaknya militer China
  - Meskipun bisa "melalui" militer China

Syria (Sept. 2007)

- Pemboman udara oleh Israel pada fasilitas di Suriah, fasilitas nuklir yang diduga dibangun oleh Korea Utara
- Jaringan pertahanan udara Suriah melihat ada pesawat, dan pada layar sistem radar 'membaca' serangan berasal dari Rusia (manipulasi)
- Penyebab pasti tidak diketahui, tetapi pilihan semua titik untuk manipulasi perangkat lunak sistem radar tidak dapat dikendalikan

Estonia (April 2007)

- Disebut sebagai "1st Cyber Warfare"
- Canggih dan besar set penolakan layanan (DoS) serangan terhadap parlemen estonia, bank, departemen, surat kabar, situs web lain
- Efek yang parah pada institusi di atas selama kurang lebih tiga minggu

Tallinn Manual

or opinion existed as to their precise application to particular actions.

5. Clearly, conducting cyber attacks related to an armed conflict qualifies as an act of direct participation, as do any actions that make possible specific attacks, such as identifying vulnerabilities in a targeted system or designing malware in order to take advantage of particular vulnerabilities. Other unambiguous examples include gathering information on enemy operations by cyber means and passing it to one's own armed forces and conducting DDoS operations against enemy military systems. On the other hand, designing malware and making it openly available online, even if it may be used by someone involved in the conflict to conduct an attack, does not constitute direct participation. Neither would maintaining computer equipment generally, even if such equipment is subsequently used in the hostilities. A more difficult situation arises when malware is developed and provided to individuals in circumstances where it is clear that it will be used to conduct attacks, but where

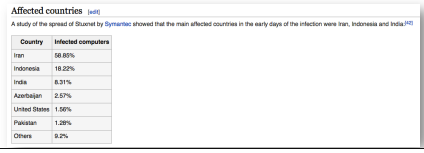
Betapa seriusnya NATO dan para ahli-nya menanggapi ancaman serangan cyber, diungkapkan dalam penempatan yang mengklasifikasikan pelaku serangan. Mengacu pada bagian "Aturan 35 – Partisipasi langsung Sipil dalam Peperangan", menempatkan hacker sipil sebagai peserta perang yang aktif. Dikutip dari halaman 120 tertulis ***"Clearly, conducting cyber attacks related to an armed conflict qualifies as an act of direct participation,.."***

Stuxnet

- Sangat kompleks worm komputer Windows spesifik yang menginfeksi komputer dan peralatan kontrol industri terhubung (PLC)
  - Worm pertama yang diketahui menyerang infrastruktur industri
- Menyebar melalui USB thumb drive serta koneksi jaringan
- Memanfaatkan empat "zero-day" eksploitasi
- Pencurian sertifikat keamanan yang valid

Stuxnet (contd.)

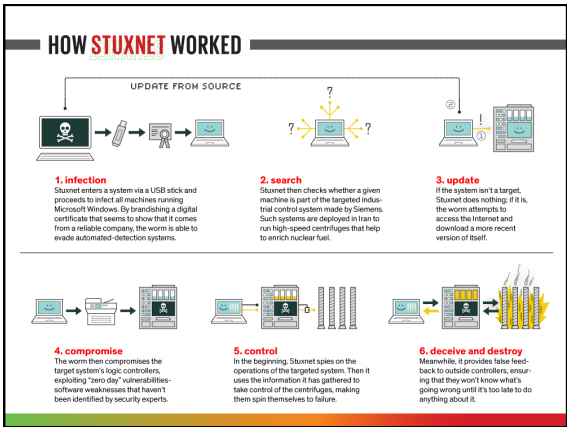
- Tingginya tingkat awal infeksi di Iran, khususnya ditemukan di fasilitas nuklir
  - Mungkin pemerintah (Israel, AS, Inggris?) Upaya untuk merusak fasilitas nuklir Iran
  - Jelas apakah penundaan atau kerusakan benar-benar terjadi
- Worm telah menyebar ke banyak negara lain (termasuk infeksi besar sistem Cina)

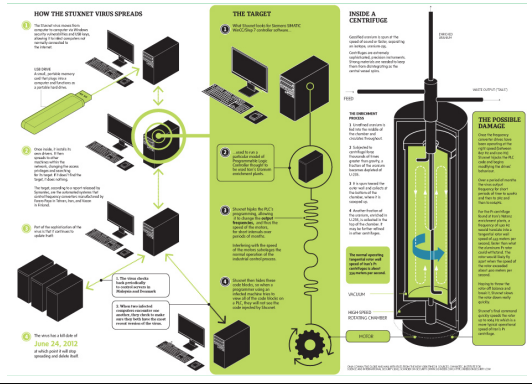


Affected countries [edit]

A study of the spread of Stuxnet by Symantec showed that the main affected countries in the early days of the infection were Iran, Indonesia and India.[42]

Country	Infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Others	9.2%





Defense on Globalization

- Dengan dijadikannya Internet atau dunia maya menjadi matra baru, maka beberapa negara Barat maupun negara 'pendatang baru' seperti China dan Rusia membuat berbagai macam berlomba-lomba membangun infrastruktur keamanan dan pertahanan,
- Bahkan, pemerintah Negara-negara tersebut merekrut para ahli yang sangat kompeten di dunia Internet melalui kompetisi di universitas-universitas ternama maupun pengamatan di jejaring sosial.

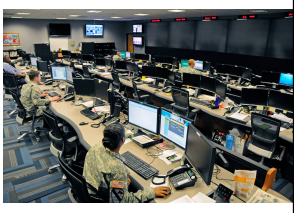
Defense on Globalization (Contd..)

- Richard Clarke, mantan staf gedung putih yang bertanggung jawab atas kontraterorisme dan keamanan cyber mengatakan efek dari perang cyber bisa bermacam-macam,
- Diantaranya adalah bug komputer bisa menghentikan sistem email militer, kilang dan pipa minyak meledak, kendali sistem lalu lintas udara terhenti, kereta api barang dan metro tergelincir, data keuangan jadi acak-acakan, pembangkit listrik berhenti dan satelit yang mengorbit lepas kontrol.

Countries Readiness…

United State

- Membentuk sebuah unit khusus bernama *United States Cyber Command* (USCYBERCOM) dibawah *United States Strategic Command* (USSTRATCOM) yang mulai diaktifkan pada tahun 2009 sebagai reaksi atas banyaknya serangan cyber terhadap fasilitas jaringan komputer dan Internet Negara adikuasa tersebut.



China

- China yang merupakan kekuatan baru dunia walau secara diketahui sedang gencar merekrut dan membangun prajurit dunia maya yang dikenal sebagai "**blue army**" untuk dipersiapkan untuk bertahan atas serangan cyber terhadap kepentingan china sekaligus mempersiapkan serangan balik yang lebih mematikan.

Israel

- Israel diketahui mempunyai sebuah unit khusus bernama Unit 8200 yang mempunyai spesialisasi cyber walfare dibawah Israel Defense Forces (IDF).
- Salah satu catatan keberhasilan yang fenomenal dari unit ini adalah ketika Unit 8200 berhasil menghentikan operasi radar senjata anti pesawat udara suriah.
- Bahkan serangan worm Stuxnet terhadap sistem komputer fasilitas nuklir iran pada awal tahun 2011 ini disebebut-sebut merupakan hasil kerja dari unit ini.

Australia

- Australia diketahui mempunyai beberapa badan yang bertanggung jawab terhadap keamanan jaringan intenet diantaranya adalah *Australian Computer Emergency Response Team* (AusCERT) yang merupakan organisasi non pemerintah yang berbasis di University of Queensland.

NATO

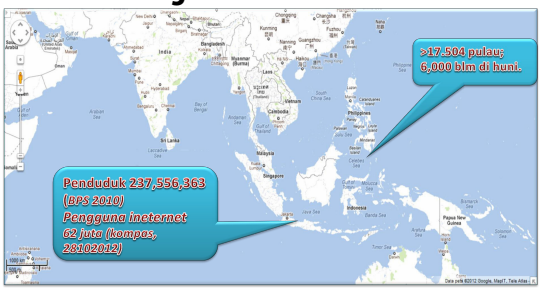
- NATO *Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE) merupakan badan keamanan cyber pakta pertahanan arlantik utara (NATO) yang didirikan pada 14 Mei 2008 dalam rangka meningkatkan kemampuan pertahahanan cyber NATO.
- NATO CCD COE bermarkas di kota Tallinn, Estonia. Pusat keamanan cyber ini merupakan hasil kerjasama berbagai Negara anggota NATO.

Indonesia?

Indonesia VS World

55 million Internet connected consumer**	2.3 billion**
1.9 million Wired Broadband Subscribers*	0.5 billion*
220 million Mobile Cellular Subscribers*	6 billion*
38 million Fixed Telephone Subscribers*	1 billion*
43 million Facebook users**	800 million**
19.5 million Twitter users***	383 million***

Letak Strategis Indonesia



Posisi strategis Indonesia yg terletak diantara 2 benua dan samudra banyak menguntungkan Indonesia. Tetapi itu juga bisa menimbulkan suatu ancaman, a.l : terrorisme, perdagangan manusia, perdagangan narkoba, dll.

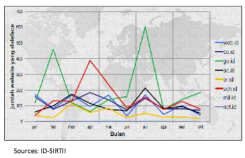
Penanganan Insiden Keamanan Siber

- Membangun Military CERT (Unit Cyber TNI)
- Mengembangkan sistem deteksi dini dan sistem pencegahan dgn berkoordinasi bersama :
  - ACAD CSIRT
  - GOV-CSRTI
  - ID-SIRTII,
  - ID-CERT,
  - BANK CERT
  - **Indonesia Cyber Army (ICA)**
  - Badan Cyber Nasional (BCN)
  - dll

71

Is Indonesia Under Attack???

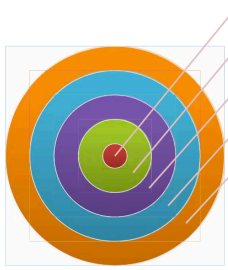
- Over the last three years, Indonesia was attacked 3,9 millions in cyber space. (Sources: Minister of ICT, April 3rd, 2013).
- During January-October 2012, The most attacked website is Government websites/domain: go.id (Sources: ID-SIRTII, 2012).



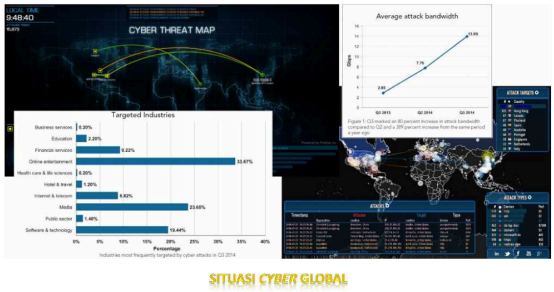
Sources: ID-SIRTII

Sources: Detikinet, 2013

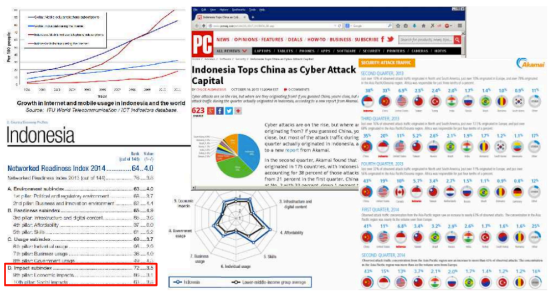
LAYERS OF CYBER SECURITY



- Implementation of cyber security technologies and processes performed at each layers.
- Cyber security at every layer is called defense in depth.
- Defense in Depth strategy is to achieve the main objectives of security, namely Availability, Integrity, Confidentiality (AIC Triad).

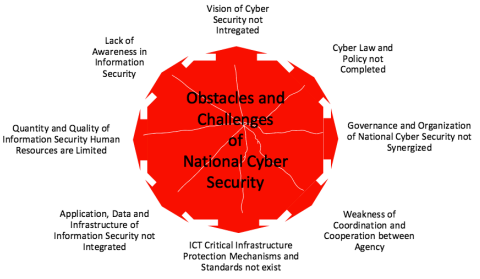


SITUASI CYBER GLOBAL



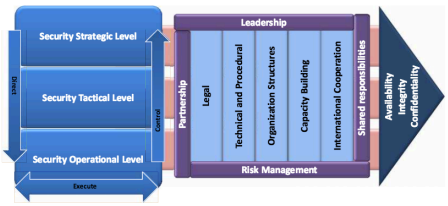
SITUASI CYBER REGIONAL

OBSTACLES AND CHALLENGES OF INDONESIA NATIONAL CYBER SECURITY



Sources: Indonesia National ICT Council, DETIKNAS 2013

Indonesia National Cyber Security Conceptual Framework (INCS)



Sources: Indonesia National ICT Council, Detiknas 2012

6 STRATEGIC PRIORITY OF INDONESIA NATIONAL CYBER SECURITY

Sources: Indonesia National ICT Council, DETIKNAS 2013

THE CONCEPT OF NCS ORGANIZATION STRUCTURE

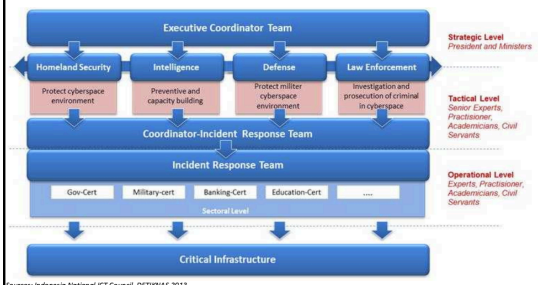
- The Concept of Indonesia NCS organization structure consists of multi-organization.
- INCS organization contains of skilled, proficient, and experienced employees with prosperous information security knowledge inside their parts of specialization.

Sources: Indonesia National ICT Council, DETIKNAS 2013

COMPARISON OF CYBER SECURITY ORGANIZATION

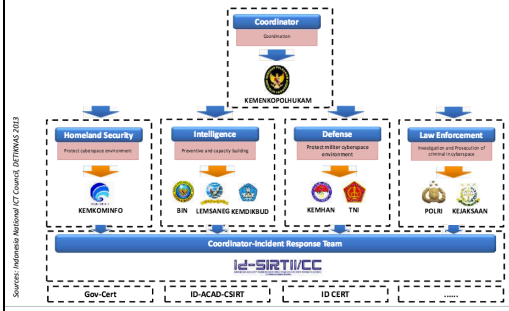
Level	Australia	UK	Indonesia
Strategic	Cyber Security Policy and Coordination Committee (Lead Agency: The Attorney-General's Department) Function: interdepartmental committee that coordinates the development of cyber security policy for the Australian Government.	Office of Cyber Security (OCS) function: to provide strategic leadership for and coherence across Government;	BCN - Badan Cyber Nasional (Office of National Cyber Security)
Tactical	Cyber Security Operations Centre (CSOC) (Under Directorate: Defense Signals Directorate) Function: provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cyber security events of national importance.	Cyber Security Operations Centre (CSOC) Function: actively monitor the health of cyber space and co-ordinate incident response; to enable better understanding of attacks against UK networks and users; to provide better advice and information about the risks to business and the public.	Cyber Security Operations Centre (TBD)
Operational	CERT Australia	GovCertUK	ID-SIRTII GovCert ID-Cert

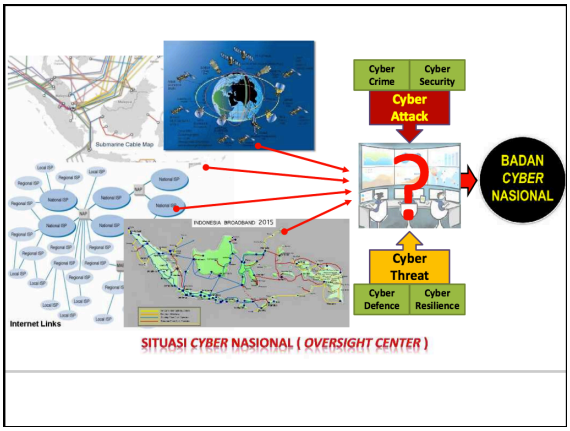
INDONESIA NATIONAL CYBER SECURITY ORGANIZATION STRUCTURE FRAMEWORK

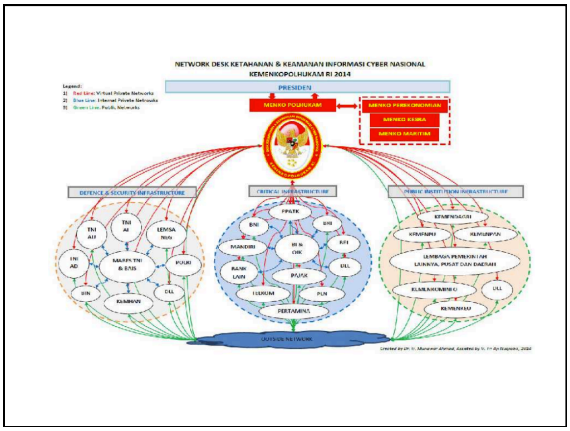


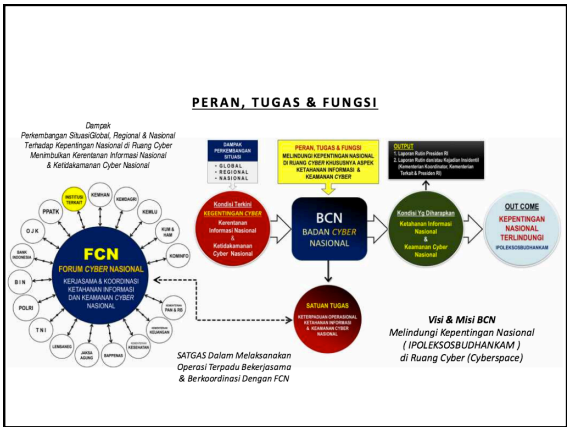
Sources: Indonesia National ICT Council, DETIKNAS 2013

ORGANIZATION MAPPING RECOMENDATION

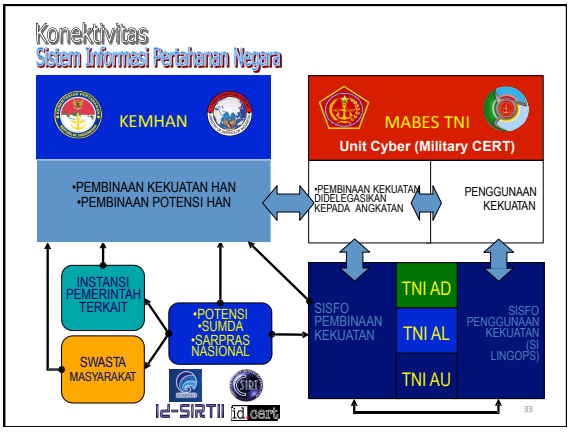


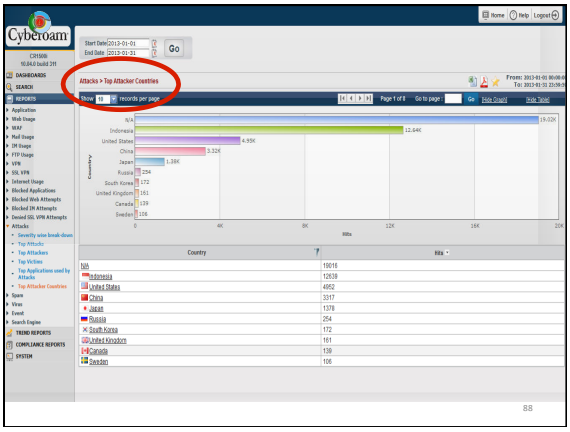




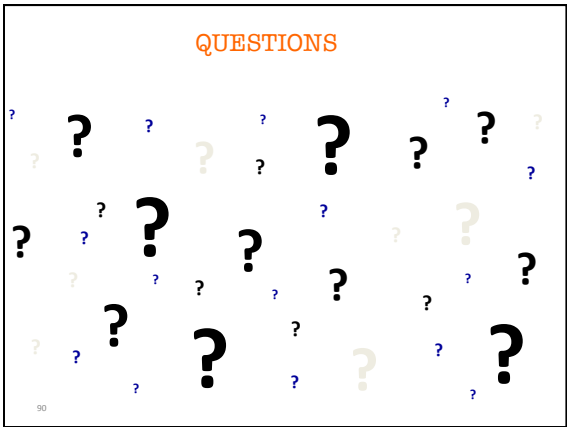

PERAN, TUGAS & FUNGSI
Dampak Perkembangan Situasi Global, Regional & Nasional Terhadap Kepentingan Nasional di Ruang Cyber Menimbulkan Kerentanan Informasi Nasional & Ketidakamanan Cyber Nasional
FCN
FORUM CYBER NASIONAL
KERJASAMA & KOORDINASI KETAHANAN INFORMASI DAN KEAMANAN CYBER NASIONAL
BCN
BADAN CYBER NASIONAL
OUT COME
KEPENTINGAN NASIONAL TERLINDUNGI
SATUAN TUGAS
SATGAS Dalam Melaksanakan Operasi Terpadu Bekerjasama & Berkoordinasi Dengan FCN
Visi & Misi BCN
Melindungi Kepentingan Nasional (IPOLEKSOSBUDHANKAM) di Ruang Cyber (Cyberspace)


Sistem Pertahanan Dunia Maya Indonesia
Sisfohanneg
UNIT CYBER (MILITARY CERT)
Sisfo TNI
Indonesian Cyber Command
TNI AD
TNI AU
TNI AL


Konektivitas
Sistem Informasi Pertahanan Negara
KEMHAN
MABES TNI
Unit Cyber (Military CERT)
•PEMBINAAN KEKUATAN HAN
•PEMBINAAN POTENSI HAN
•PEMBINAAN KEKUATAN DIDELEGASIKAN KEPADA ANGKATAN
PENGGUNAAN KEKUATAN
INSTANSI PEMERINTAH TERKAIT
SWASTA MASYARAKAT
•POTENSI •SUMDA •SARPRAS NASIONAL
SISFO PEMBINAAN KEKUATAN
TNI AD
TNI AL
TNI AU
SISFO PENGGUNAAN KEKUATAN (SI LINGOPS)
id-SIRTII
id cert
33


Cyberoam
Attacks > Top Attacker Countries
88


UNIT CYBER CONTROL TNI
89


QUESTIONS
90

References

- http://zone-h.org/en/stats (ZONE-H Statistics)
- http://www.netforcuba.org/FeatureSection-EN/NewThr.htm (Net For Cuba)
- http://ctp.iccas.miami.edu/FOCUS_Web/Issue58.htm (Focus on Cuba)
- http://www.findarticles.com/p/articles/mi_m0PBZ/is_2_83/ai_106732244/pg_3 (Palestine Israel Cyber War)
- http://journalism.uts.edu.au/subjects/oj1/oj1_a2002/internetactivisminasia/india2.html (Indo-Pakistan Cyber war)
- http://www.srijith.net/indiacracked/stats/index.shtml (Project India Cracked Statistics)
- http://www.attrition.org/mirror/attrition/2000/08/26/gujarat.gov.in/ (Gujrat Government Defaced Mirror)
- http://www.attrition.org/mirror/attrition/2001/01/02/iqcar.ernet.in/ (India Gandhi Centre Defaced Mirror)
- http://pakcert.org/defaced/www.sysnet.com.pk.html (Sysnet Defaced Mirror)
- http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/alqaeda.html (Frontline Cyber war)
- http://www.newsmax.com/archives/articles/2001/2/8/221142.shtml (US war on Bin Laden)
- http://www.fas.org/irp/program/process/echelon.htm (ECHELON)
- http://www.antiwar.com/news/?articleid=2444 (Photos of Abu Ghraib)
- Marcus Murray & Hasain Alshakarti, APTs, Cyber-attacks, Cybercrime, Cyber warfare and Cyber threats exposed, Truesec Security Team, MVP-Enterprise Security x2
- Arif Abdillah, Pemanfaatan CESRT/CSIRT Nasional untuk melindungi aset-aset informasi Vital NKRI
- Ahmad Luthfi, Cyber Defence: Antara Kebutuhan dan Regulasi,