APEC Telecenter Workshop, APEC Telecommunication and IT Working Group
Singapore, September 19, 2004

Opening ICT Public Access and the Cybercrime Pandora Box in Indonesia - ‘04 Update

Idris F Sulaiman PhD
International Affairs Advisor
Indonesia Information Technology Federation (IITF~FTII)

Donny B. Utoyo
Coordinator, Indonesia ICT Watch Foundation &
Director, Center of ICT Studies, Jakarta

Michael Baker
Executive Director,Asia Oceania
Electronic Marketers Association (AOEMA)

The views expressed in this presentation are those of the authors and not necessarily those of the above organizations nor of the Government of Indonesia

Topics

- 1) Indonesia ICT & Public Access Status
- 2) Internet Kiosks - Update '04
- 3) Cyber Fraud & Crime Issues
  - Indonesia's status
- 4) Recommendations
  - Regional, national & community responses

PANDORA’S BOX

any source of extensive troubles, esp. one expected at first to yield blessings

(in Greek classical mythology,
a box or jar given by Zeus to Pandora,
which contain all human ills).

(1)

Indonesia - ICT Status - Telephony

- Population: 215 mil., over 110 mil. on Java Island
- Telephone density:
  - National: Fixed ~ 3 %; Cell/Mobile ~ 6%; Total ~ 9.1%(Q3'03)
  - Fixed wire line : ~ 8 millions (3.63% at 30.06.2003)
  - Cellular Mobile : ~ 14.5 millions (30.06.2003)
  - Local Fixed Wireless Access : Started in some cities
  - Major cities have adequate teledensity
    - The Metropolitan City of Jakarta > 40%
    - Other major cities (eg Medan, Surabaya, Bandung, Semarang) > 11%
    - Other regions : Eastern Indonesian towns: 2.04%
    - **Remote Rural Areas** : 0.2% (43,000+ villages with no telephone lines out of 70,000 villages)
    - World average of rural connectivity ~ 50%
    - Over 65% unconnected villages: Higher than World Average
  - Telephone Kiosks/Cafes : over 200.000

(1.1)

Indonesia ICT Status - Internet

- Internet/ISP subscribers: 1,200,000 (est.)
- Internet users: 9,500,000 (est.) of 215 m. population - less 1% penetration one of the lowest in the Asia Pacific region
- ISPs: over 200 licenses but only 43 operational and 10 ISPs have nearly 80% of the Internet users market share
- Warnet (Internet Kiosk): over 2,500 in 2002 (Warnets are populars place in large cities in main islands as centers of ICT access) but now less than 2000
- Computer ownership: 0.01-0.05% (less than one to 5 PCs per 100 household for rural and urban areas) but there is a high rate of public access (Warnets are growing in the major cities).

(1.3)

Indonesia Warnet Status - 2004

- **70% Warnets are closing down in some large cities** as they are being increasingly replaced by other forms of access to the Internet
  - Schools and Universities: many state secondary students now have access (Rp.10k=USD1.08/month)
  - Office: Dial-up Telkomnet Instan/PT Telkom & CableTV/ADSL
  - RT-RW-Net (Local Neighbourhood Broadband/Wireless Networks - initiated by Onno Purbo & Michael S. Sunggiardi - Warnet/ISP operator in Bogor, West Java, 60 Km south of Jakarta)

- **2004-5: less than 2000 Warnets** (0.4% of target - the over-optimistic government target of 500,000 Warnets by 2005 (SIBM-Business and Community Centres) based on 200,000 Wartels (Phone Kiosks) and 2,500 Warnets in 2001.

- **The reality now is that most Warnets are facing a very difficult time to survive as viable businesses**. Some of them are turning to crimes related to “carding” (credit card fraud, sales of expensive items, etc).
  - High average investment (Rp.61m~$6560/each with 8 computers+access eqmt, AC, tables and chairs) with long break even points (only Rp.6.7m~$716/month) is made worse by high Internet access cost (Rp4m~$430/month for 64Kbps) and dwindling users; many have turned into Network Game Parlours or some have become “carding” centres.

(1.3)

Indonesia Warnet Status - 2004 (2)

- **10 ISPs in Yogyakarta, Central Java were forced to close down** by the authorities for "illegal wireless equipment use". Result: 70 warnets, 41 schools/regional government access points closed down as a result of the "sweeping" action (www.detik.com, 19/9/2004)

- **Compared to 2001-2, the last 2 year has seen a consistent decline in the use of Warnets**: no special incentive from government. Rather than trying to bring new users on line, Warnets have been mainly in fiercely competing for the dwindling users while facing ever higher operating costs.

- **Internet connection tariff is relatively still too high** particularly cable services (from PT Telkom's dial-up, leased-line or ADSL)

- **Alternatives are illegal:** many Warnet obtain "illegal wireless" equipment (esp. 2.4GHz) bandwith or satellite bandwidth (from overseas without licence/'legal footprint'). National legal satellite providers are also too costly.

(1.4)

Indonesia Warnet Status - 2004 (4)

- **Wages of staff members (daily operators) have been squeezed** because of difficult economic circumstances faced by Warnet owners

- **As a result, many owners and staff member have even become "permissive"** to allow:
  - customers to use their premises to conduct "carding" activities;
  - some "nurture" and coach carding groups in their Warnet to get extra income;
  - employ "known hackers" (often are local IT-students and unemployed graduates)
  - some profess doing it for a political cause (e.g. Aceh separatist movement; as "revenge against infidel Westerners", and so on) ;
  - assist with the distribution of the illegally ordered expensive goods that have been obtained (computer laptops, golf clubs, sports equipment and so on).
  - Organise/let premises become meeting places for hackers after hours
- **Other criminal activities are being "promoted" by some unscrupulous operators**:
  - Bookmarking Vice Internet Relay Chat & Websites: Pornography, Prostitution, Credit Card Swapping, "meet rich foreign guys/girls" sites, etc.
  - Paedophiles access: Especially Warnets with DSL -512k broadband- access, webcams access is currently very popular with many youth (some underage) interested to have Internet "video conference" and "flesh-meet" interaction with foreigners who use promises of expensive gifts and travel to exotic places to attract unsuspecting victims.

(2)

Internet Kiosks Survey

- Preliminary survey by Center for ICT Studies, ICT Watch & ICT/MoCI, PEG-USAID Project
- Field survey: August, 2003
- Qualitative approach (structured questionnaire + focus group discussion)
- Field research locations: Makassar, Medan, Bandung, Jogja and Jakarta suburban (5 main cities - 10 Internet kiosks, each location)
- Respondents : administrators and/or owners of the Internet Kiosks

(2.1)

Legal Entity & Gov't Policy

City	Legal Entity? [1]	Local Gov Policy[2] on Warnet Response?
Makassar	Yes:4 / No:6	Yes:7 / No:3
Medan	Yes:3 / No:7	Yes:6 / No:4
Bandung	Yes:5 / No:5	Yes:4 / No:6
Jogja	Yes:2 / No:8	Yes:4 / No:6
Jakarta suburban	Yes:5 / No:5	Yes:5 / No:5

1) Limited Partnership (CV) or Incorporated (Inc/Ltd)

2) Policy on licensing, permits, etc.

YES

- If licensing is without complicated procedures & no big costs involved
- Regulations - OK if only affects business competition

NO

- Let the competition happen naturally
- The need to increase performance of self-regulating institutions

FTII

(2.2)

Investment & Rent Fees

City	Investment (US$1=Rp 8-8.500)	Rent Fee * (standard per hour)
Makassar	>= Rp 80 million (4)	Rp 3500 – Rp 4000
Medan	>= Rp 80 million (9)	Rp 2500 – Rp 4500
Bandung	>= Rp 80 million (7)	Rp 3000 – Rp 4500
Jogja	>= Rp 80 million (6)	Rp 3000 – Rp 3800
Jakarta suburban	>= Rp 80 million (5)	Rp 4000 – Rp 6000

*

- Varied, depends on the facilities provided and the time schedule (the lowest rent fee is after midnight until morning); for example “super-cheap” wee-hour specials (2300-0600 for Rp.1,500-2,000 per hour)
- Most of the respondents say the rent fee is not ideal. The fee should be higher (up to Rp 2000 more)
- 1-2 years ago, the rent fee is higher (up to Rp 2000 to Rp 4000 more), but the “price war” drastically crashed the price

(2.3)

Computers & Net Income

City	No. Computers (No of Warnets)	Net Income * (average per month)
Makassar	5 – 10 (5) 11 – 20 (5) > 20 (0)	Rp 2 – Rp 4 Million
Medan	5 – 10 (0) 11 – 20 (3) > 20 (7)	Rp 2 – Rp 6 Million
Bandung	5 – 10 (0) 11 – 20 (8) > 20 (2)	Rp 5 – Rp 10 Million
Jogja	5 – 10 (4) 11 – 20 (4) > 20 (2)	Rp 2 – Rp 4 Million
Jakarta suburban	5 – 10 (8) 11 – 20 (0) > 20 (2)	Rp 0.5 – Rp 2 Million (housing area) Rp 5 – Rp 10 Million (campus area)

FTII

(2.4)

O/S and Internet Access

City	Operating System (server)	Internet Access
Makassar	Windows (1) Linux (9)	Wireless / 16-64 Kbps
Medan	Windows (8) Linux (2)	Wireless / 16-64 Kbps
Bandung	Linux (10)	Wireless / 32-64 Kbps
Jogja	Windows (1) Linux (9)	Wireless / 32-64 Kbps
Jakarta suburban	Windows (8) Linux (2)	Dial Up (housing area) ADSL 512 (campus area)

Note: Most of respondents use Windows 98 for their client computer operating system.

(2.5)

Number of users, types & activities

City (First - Last Warnet Est'mt. Date)	No. Users/day (No of Warnets)	User categories (in descending order) Cybercrime-CC(..);Porn-P(..)*
Makassar (04/1999-05/2003)	40 – 50 (5 - 15 hours op.) 50 – 70 (5 - 24 hours op.)	High-School & Univ. Students CC(-7;+3) ; P (+4 - warning esp. HS Students)
Medan (04/1999-05/2003)	40 – 50 (5 - 15 hours op.) 70 – 100 (5 - 24 hours op.)	Univ. & High-School Students CC(-10) ; P (-10)
Bandung (06/1998-06/2002)	40 – 50 (3 - 15 hours op.) 70 – 170 (7 - 24 hours op.)	Univ. & High-School Students CC(-5; +5) ; P (-5; +1 - warning esp. HSS; +4 - blocking access with filter)
Jogja (02/1999-10/2001)	20 – 30 (3) 50 – 70 (3) >100 (3) >350 (1)	Univ, High-School Students & Workers CC(- 8;+2) ; P (+1 - warning esp. HS Students)
Jakarta suburban (12/1999-02/2003)	40 – 50 (8 - 16 hours op.) 70 – 170 (2 - 24 hours op.)	Univ, High-School Students & Workers CC(- 7: +3) ; P (-8 -no warnings)

*Note: ("+") Signifies the number of Warnets who take positive action against CC/P and ("-") signifies the numbers of Warnets who are resigned to CC/P usage

(2.10)

Take-up Barrier Assessments

- Lack of Sustainability of Internet Kiosks might be due to:

(1) **Computers are still unaffordable** (price too high relative to income, tendency to plan finances only for the short term)

(2) **Access is still unaffordable** (price too high relative to income)

(3) **Low awareness about what computers can do** and tendency to avoid complicated technology

(4) **English language barrier**

(5) **Community-based solution (such as RT-RW.Net are still too limited hardware - software solution)**

(3.3)

Cyber Crime Status

- **IT-based Crime Credit Card Fraud is often done from Warnets**

- **20 percent of the total number of credit card transactions in Indonesia on the Internet were cyberfraud**.
- Indonesia's country identifier in an **Internet address, 202, has been blocked** by most e-merchants. So hackers use a technique called "IP spoofing" to falsify this with the number of another country.
- **Shipping companies regularly refuse to ship goods to Indonesia** so the hackers give an address like "Jakarta, Holland" or "Jakarta, Japan"

- **Ebay.com and PayPal.com blacklisted Indonesia:** no access for visitors with ".ID" IP-address and **e-commerce blockage for 215 million Indonesians**
- **Internet Fraud in Indonesia is serious -**
  - **2003: Indonesia ranks second after Ukraine** on the list of countries of origin of cyberfraud ('carding') according Texas-based security company ClearCommerce (**www.clearcommerce.com**) survey: conducted from mid 2000 until end of 2001 and involved 1137 merchants, six million transactions and 40,000 customers)
  - **2004: Indonesia ranks first replacing Nigeria**

Cyber Fraud Status : Indonesia joins the Top-10

#1 by percentage & #3 by total volume

Top Countries by of Fraudulent	Total Volume Transaction	Top Countries by of Fraudulent	Percentage Transactions
Country	Ranking	Country	Ranking
USA	1	**Indonesia**	1
Canada	2	Nigeria	2
Indonesia	3	Pakistan	3
Israel	4	Ghana	4
United Kingdom	5	Israel	5
India	6	Egypt	6
Turkey	7	Turkey	7
Nigeria	8	Lebanon	8
Germany	9	Bulgaria	9
Malaysia	10	India	10

Source:

January 2004 edition of US VeriSign's “Internet Security Intelligence Briefing” report

(3.5)

Network Security - Type of Incidents

- Web deface: 2 or more/week (2/2004-elections)
- Spamming & Mailbombs
- Probe/Scan Intrusions
- Account/Root Compromise
- Packet Sniffer
- Harassments/Exploitation of Trust
- Denial-of-service (DDoS)
- Malicious Code/Virus and worm attacks
- Internet Infrastructure Attacks

- See ISP Association (APJII)'s website for the latest statistics on the above (www.apjii.or.id)
- Source: Standard CERT Classification (www.cert.org/encyc_article/tocencyc.html)

(3.6) Face of Cybercrime - Credit Card Fraud: suspect and evidence

SUSPECTS -

•Mostly young educated, some with IT qualifications

•Many amateurs but some maybe organized

•Need for employment opportunities

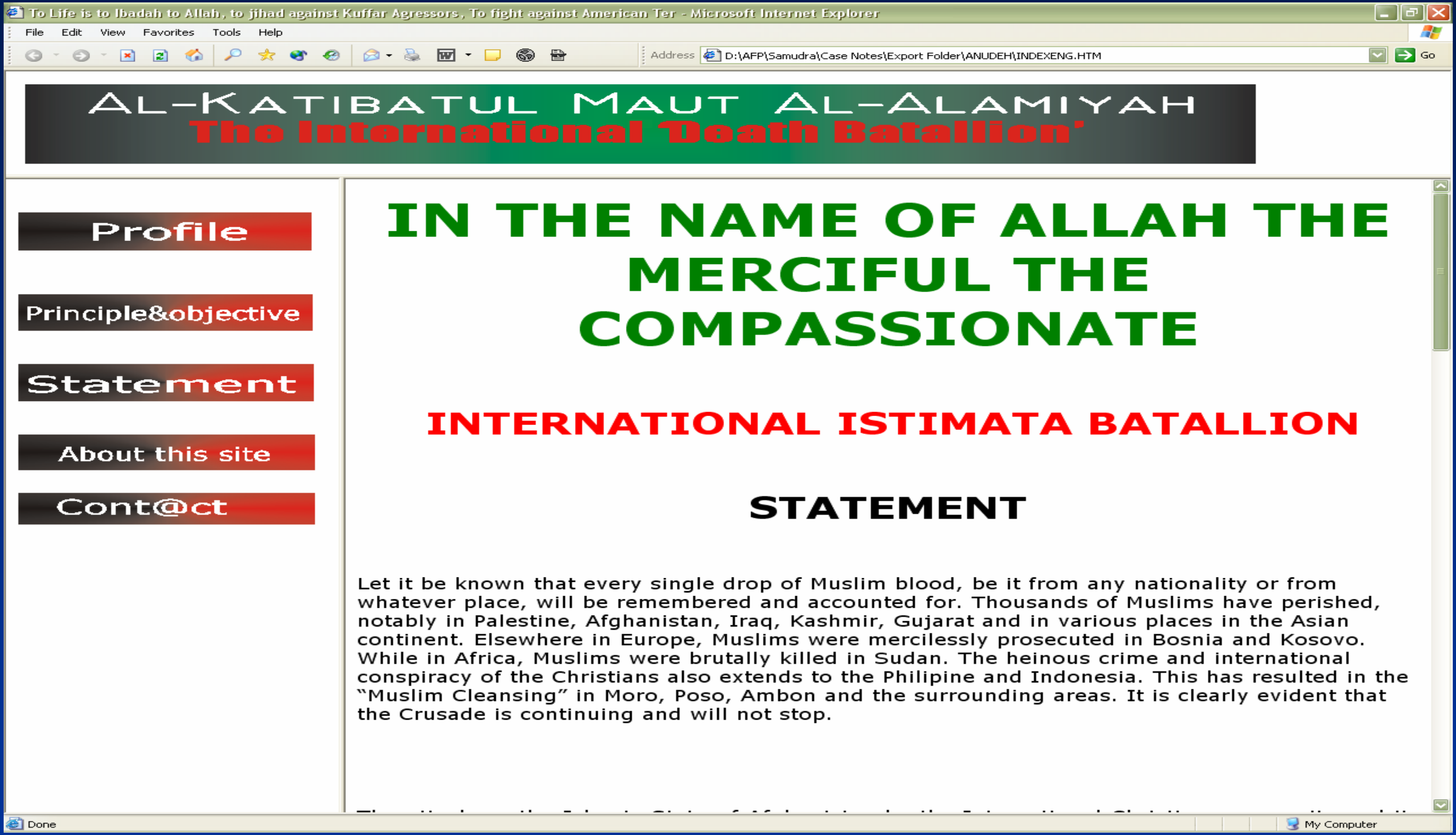
MERCHANDIZE:

•Various objects which can be easily exchanged for cash: laptop computer and parts, musical instruments, sports & hobby items (golf, baseball), security products (bullet proof vest, etc.)

•Most of relatively small value < $ 1000 but some items (part of organized crime) can be substantial (e.g. radar equipment)

(3.7)

Face of Cyber Terror: Website to spread fear and hate


To Life is to Ibadah to Allah, to jihad against Kuffar Agressors, To fight against American Ter - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Address
D:\AFP\Samudra\Case Notes\Export Folder\ANUDEH\INDEXENG.HTM
Go
Profile
Principle&objective
Statement
About this site
Cont@ct
Done
My Computer

AL-KATIBATUL MAUT AL-ALAMIYAH

The International Death Batallion'

IN THE NAME OF ALLAH THE MERCIFUL THE COMPASSIONATE

INTERNATIONAL ISTIMATA BATALLION

STATEMENT

Let it be known that every single drop of Muslim blood, be it from any nationality or from whatever place, will be remembered and accounted for. Thousands of Muslims have perished, notably in Palestine, Afghanistan, Iraq, Kashmir, Gujarat and in various places in the Asian continent. Elsewhere in Europe, Muslims were mercilessly prosecuted in Bosnia and Kosovo. While in Africa, Muslims were brutally killed in Sudan. The heinous crime and international conspiracy of the Christians also extends to the Philipine and Indonesia. This has resulted in the "Muslim Cleansing" in Moro, Poso, Ambon and the surrounding areas. It is clearly evident that the Crusade is continuing and will not stop.

FTII

(3.8) Victims of Cybercrime - mostly in industrialized countries: reported cases

NO	MODUS OPERANDI	TOTAL	RESIDENCE OF VICTIMS	RESIDENCE OF SUSPECTS
01	Credit Card Fraud	152	84 USA 25 Canada 11 Spain 8 Germany 8 Australia 4 British 3 Denmark 1 France 1 Austria (Vienna) 3 Japan 3 Singapore 1 Korea	62 Yogyakarta 43 Central Java 36 West Java 24 Jakarta 18 Sumatra 12 East Java 3 Kalimantan 3 Sulawesi 17 Others
02	Banking Offences	4	1 Solo,1 Yogyakarta 2 Jakarta	2 USA , 1 Malaysia, 1 Australia
03	E-mail Threats	2	1 Germany, 1 Australia	1 Bandung, 1 Jogyakarta
04	Terrorism	1	Australia, UK, USA, Japan, Korea and other allied nations (including Indonesians - over 250 lives lost)	1 (Imam Samudra - a major suspect of the recent Bali Bombing case)
**	Grand Total	159	159	225

The associated financial loss of reported cases caused by this type of fraud alone amounted to over than **US$ 1,296,597**.

(3.9)

Many “Hackers” Clubs in Indonesia

- Notorious and well-known “carder” (credit card fraudsters, IRC) clubs:
  - K-elektronik.org
  - Indosniffing
  - Medanhacking
  - Hackerlink
  - Antihackerlink, etc.
- **Recent increased activities by Indonesian Cybercrime Unit has made a difference**
  Clubs come and go but the number of reported cases of credit card fraud fell from 218 (2002) to 113 (Aug ‘04),
- Increased well-publicized arrests and surveillance activities, more media exposure helps.
  “Jogja - Bandung are carding heavens”, Gatra (magazine), Sept. 13, 2003

(4)

Counter-Cyber Crime Strategies

- **Asia Pacific Regional Responses**
  - Future APEC Economic Leaders Meeting (prioritize).
  - APECTEL - eSecurity Task Group (on-going activities)
  - APEC Computer Emergency Response Teams (AP-CERT) - 24X7 Point of Contact Network, Capacity Building
  - New Regional efforts: InfraGuard Asia
- **Indonesian National Responses**
  - Long-Term and Short-Term Solutions
  - National strategy and concensus building
- **Community Responses**
  - Businesses, NGOs, Law Enforcement, Legislation
  - Computer Incident and Abuse Handling - CERT, ISPs, Warnets
  - Industry Code of Conduct, Community Enforcement (WARPs)

(4.1) National Counter-Strategies

- **Long-Term (Institutional Enablers)**
  - **Allowing a conducive business environment for Warnet business by Government (ICT Ministry): -** direct concessions on licensing (2.4GHz & satellite bandwidth) or indirect concessions (directing telecom operators to lower tariff of connectivity for Warnet, Schools, Hospitals, Libraries, etc)
  - **Negotiate a "discount-scheme" for Warnets, Educational, Health and other Key Community Institutions, support IT Multinationals to provide concessions to them**: the government could provide awareness raising & training activities for the relevant operators
  - **Place ISPs and Warnets on equal footing**: Warnets no longer as merely "re-sellers of ISPs" but also ensure them to be viable business centers

(4.2) National Counter-Strategies

- **Medium-Term (better conditions for W-operators)**
  - **Conduct an awareness raising for Warnet business by Government (ICT Ministry):** - direct appeal about the gender education to Warnet, Schools, Hospitals, Libraries, and others to say that if there is any suspecting case, there will be "raids" and Warnet servers can be held for months.
  - **Warnets must adopt a "code of conduct" for training and for general managers for Warnet operators** (a draft has been put together by Indonesia Net and other operators).

(4.3) National Counter-Strategies

- **Short-Term (restricting "carding"-activity)**
  - **Issue directive for Warnets to start obtaining copy all users Identity Card for the Government:** each user must provide a copy of their KTP or SIM or Passport (National ID is coming)
  - **Warnets must carry a posters to warn about the "dangers of cyber fraud and cyber crime" for all to see.**
  - **Warnet administrators must maintain a watchful eye on the log file (while there is some on-line activity) or install a remote software to monitor such cyber-fraud activities (example: one software brand is "VNC", see www.tightyvnc.com).**
  - **NOTE that the above are excellent examples of preventive action to monitor Warnet usage pattern but privacy issues should be looked after.**
  - **Ensure that Warnet backup the log activity files of users to CDs (as an alternative piece of evidence rather that confiscation of servers)**

(4.1)

REGIONAL CYBERSECURITY EFFORTS

TEL26 RU - TEL27 KL- TEL28 TW - TEL 29 HK - TEL 30 SG

Sewa Koneksi Hanya Rp 2500/ jam
(Bawa Laptop/Notebook sendiri)
HORE.... ADA WEB CAM
Scanning Rp 2000/file , Printing
Teknologi ADSL 512 kbps
Net 21

- Meetings of the Telecommunications and Information Working Group of the Asia Pacific Economic Cooperation (APEC)
  - 21 members and many observer economies/NGOs
  - **APECTEL** key cybersecurity activities:
    - Business Facilitation Steering Group (BFSG)
    - E-Security Task Group (ETG) part of BFSG
    - AP-CERT Meetings
  - **Legal Workshop to Combat Cybercrime** (Aug 17-18, 2002,Tel 27)
  - **Cybercrime Legislative and Enforcement Capacity Building** (July, 2003, Bangkok)
  - **Computer Emergency Response Teams (CERTs**
    - **TEL27 KL- TEL28 TW - TEL 29 HK**
    - **TEL30 SG: Wireless Security, CSIRT Workshops**
  - **BUT something MORE is needed to address Cyber Fraud & Crime**
    - **TEL30+ : Workshop on "cyber-fraud" counter-strategies**

(4.2)

APEC Cyber Security Strategy

- Good 5 initiatives but enough on-the-ground action? (APEC Digital Opportunity Center and Training) might address people-centred issues relating to:

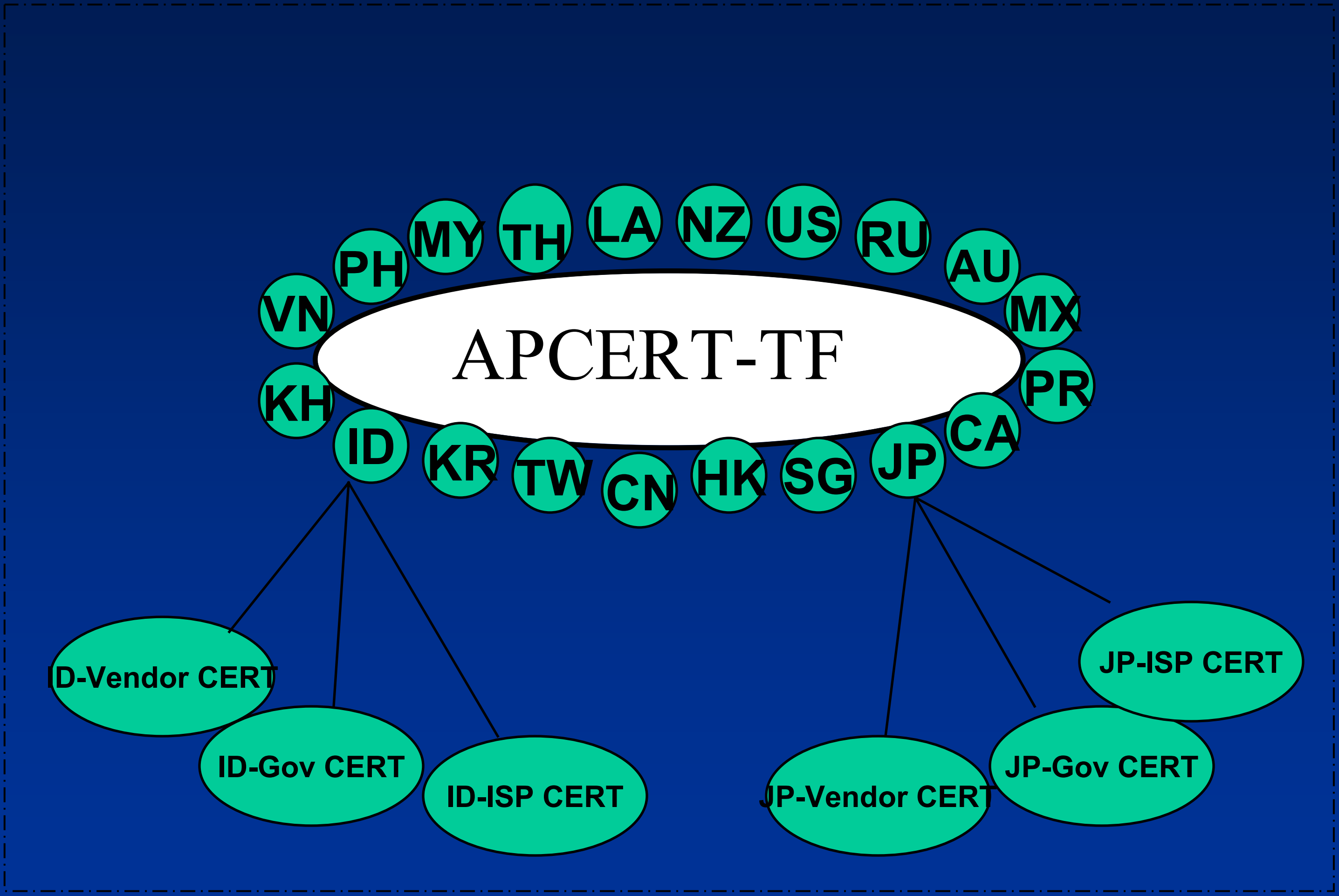
darm@-net
24 JAM
INTERNET & MULTYPLAYER GAMES
Counter Strike - Command & Conquer Generals - dll
TELP. (021) 7888 067

  - ■ Legal developments
  - ■ Information sharing and cooperation
  - ■ Security and technical guidelines
  - ■ Public awareness and education
  - ■ Wireless security
- Economic Security - job-creation to bridge the digital divide (Development Cooperation Steering Group for TEL26) Major result: Digital Divide Blueprint for Action, Supporting Micro/SMEs, and Considering Next-Generation Technologies and their role in Infrastructure Development
  - – ICT Investor Dialogue (low cost emerging market examples - Thailand & India): Jakarta & Singapore

(4.3)

APEC Computer Emergency Response Teams

APCERT-Task Force for Network Security Incidents Response & Coordination



APCERT

24x7 Point 0f Contact List

(4.4) Building blocks for combating cybercrime

- National "Cybersecurity Strategy" development:
  - Define architecture, Roles and Responsibilities
  - Business Model, Funding and Contributions
  - Technical Assistance (APCERT and others)
  - Legal Framework and New Guidelines
- Expand Incident Abuse Report Email Contact
  - ID-ISP-CERT: Abuse@apjii.or.id
- Improve information in Indonesian language
- Ticketing system for incident reporting handling
  - ID-ISP-CERT - IODEF: incident information exchange format standard: http://www.terena.nl/tech/task-forces/tf-csirt/iodef/
- IT Business Community Forum : ID-FIRST (Indonesia-Forum for ICT-incidents Response and Security Team) sponsored by Indonesian IT Industry Federation (FTII) - in search of partners and sponsors

(4.5)

Improve IT-Investment Environment & Cybercrime Reduction

- **Worsening IT educated unemployment** most official figures underestimate true situation; mainly heavily concentrated in the cities of Jakarta, Bandung, Jogyakarta, Semarang and Surabaya which accounted for over 40% of all senior high and nearly half of all graduate unemployed in urban areas in 1999 (no recent statistics are collected)
- **Unemployment rates were also highest in these cities:** 19 % and over versus a 14% unemployment rate among high school graduates in all Indonesia in 1999.
- **For many unemployed graduates: many Internet cafes or Warnets provide heaven for "carding" (credit card fraud),** hacking and other cybercrime activities; few convictions but lightly punished - no deterrent in the existing laws (even Warnet operators are allegedly involved)
- **Improving employment by providing opportunities for IT/ software development SMEs -** scale up successes of the development of software incubation Balicamp to Balige Tobacamp, Bogorcamp, Bandung High Tech Valley (BHTV)

(4.6)

Private Sector Initiatives

- **Expand Information Sharing Network coordinated by ID-FIRST:-** Loose voluntary network of entities including CERTs, WARPs (not a technical but capable of reporting including Warnets), ISACs and other key organizations interested in sharing warnings, vulnerabilities, threats and incident reports)
- **Expand links with "InfraGuard Asia"** (PH, US)
- **Model: UK's "Cyber-Neighbourhood Watch" Warning, Advice and Reporting Point (WARP)**
  - Based on ICT Neighborhood Groups in Indonesia:e.g. RT-RW.net
  - Provides warning, advice and reporting services on Internet Network & IT security-related matters
  - Similar to a CERT but without a capability for responding to incidents (other than providing advice - not able to issue technical "patches" against virus, troyan horses, mal-ware in general)
  - Warnets will cooperate with ISPs (as in recent case of Jakarta-Bali fraud)

(4.7)

ID-FIRST/FTII approach to cybersecurity

(1) Improve Trust & e-Security through (5 elements):

- Awareness Raising, Training and Education
- Strengthen Legal and Policy Framework
- Capacity Building in Technology Tools and Computer Emergency Response Teams (ID-ISP-CERT, ID-CERT, ID-FIRST, ICT Security TF)
    - "First step in stopping attacks is to understand how hackers think, work and organize then make sure security systems are nimble enough to shift gears when they do" - e-security expert.
    - Coordination, Incident Reporting/Data Collection and Crisis Management
- Partnership between Private Sector, Academia, Government including Law Enforcement Agencies (LEAs)
- Private sector leadership role (while government is in transition)

(2) Improve Business/Investment Climate, Employment Opportunities in Indonesian IT industries

*** Collaboration with interested multi-lateral and bi-lateral donor organizations can accelerate local programs**

(4.8) Cybersecurity Recommendations

- **Awareness:** Internet Kiosks (Warnets) are critical ICT access points but also are systemic security vulnerability points
- **Design Cybersecurity Strategy on the Outset**: Building blocks and strategize - legal, technical and investment issues - must be seriously considered by both private sector & government - BEFORE - credit card & Internet fraud, cyber/terror attacks gets worse (Ignore e-security "at your peril" - Lessons from Microsoft).
- **Some late-comer advantages for Indonesia & other developing countries** - practical response & policy work:
  - Regional (APECTEL-eSTG, 24X7 POCs) & International (FIRST.org)
  - UN-General Assembly (latest: Resolution A/C.2/58/L.19, Cybersecurity and the Protection of Critical Information Infrastructure)
- **Outcome depends on all of us: Trust-building, Affective Preparatory and Post-Incident Action at all levels** (Individuals, Community NGOs, Industry Orgs, LEA, Governments, etc.)

Thank You/Terima Kasih

- **Please provide feedback to:**

  Idris F. Sulaiman

  Cell/Mobile: +62-811-111-312 or +65-9811-2827 (Sept. 19-21)
  Fax: +62 21 8370-7643
  Email: idriss@indo.net.id

- **Related Websites:**
- Indonesia IT Federation: : www.ftii.or.id
- Business Security Forum: www.Secure-Indonesia.FIRST.or.id
- ICT Neighborhood Associations (RT-RW-Net), http://www.bogor.net/idkf/michael/rt-rw-net/ File: rt-rw-net.pdf

URLs - References

- Last APECTEL28: http://www.apectel.com.tw Next APECTEL29, HongKong, Mar'04
- E-Security Task Group (APECTEL)
  - http://www.apectelwg.org/apec/atwg/preatg.html
- APEC Cybersecurity Strategy:
  - http:// www.apectelwg.org.sg/download/tel/TEL_CybersecurityRecmdn.pdf
- TELMIN Statement on the Security of Information and Communication Networks
  - http://www.apectelwg.org/apec/are/telmin5sub03.html
- APEC Leader Statement:
  - http://www.apecsec.org.sg/downloads/pubs/LeadersStmFightTerrorNGrowth.pdf
- Some Computer Emergency Response Team sites:
  - Japan: http://www.JpCERT.or.jp
  - Malaysia: http://www.mycert.org.my http://www.mycert.org.my http://www.niser.gov.my ,
  - Singapore: http:// www.singcert.org.sg
  - Thailand: http://thaicert.nectec.or.th
  - Taiwan: http://www.cert.org.tw
  - US: http://www.cert.org/
- UN Resolutions on: Cybersecurity & Protection of Critical Information Infrastructure (debated Dec 2003): Creation of Global Culture of Cybersecurity (No57/239-20Dec02), Establishing Legal Basis for Combating the Criminal Misuse of Information Technologies (No.55/63-4Dec00;56/121-19Dec01),Developments in the Field of Information and Telecommunications …Security (No.53/70- 4Dec98,54/49-1Dec99,No.55/28-20Nov00, No.56/19-29Nov01, No.57/53-22Nov02)

Indonesia IT Federation

Indonesian Information Technology Federation (IITF/FTII)

Phone: +62-(0)21-5296-0634 Fax: +62-(0)21-5296-0635
Email: secretariat@ftii.or.id Website: www.ftii.or.id

FTII - consists of:

1) Internet Service Providers Association (APJII),
2) Computer Business Association (APKOMINDO)
3) Software Business Association (ASPILUKI)
4) Indonesian Association of Animators (ANIMA)
5) Wireless LAN Association (WLI Indonesia)
6) Internet Kiosk Association (AWARI)
7) Phone Kiosk Association (APWI)
8) Indonesia Satellite Association (ASSI)
9) Indonesia Cellular Operator Association (ATSI)

Affiliated organizations: Indonesia Telecommunications Users Group (ID-TUG), School 2000 Foundation, Indonesia ICT Watch, Global Internet Policy Initiative (GIPI), National Internet School Network (JIS).

ICT watch!
www.ictwatch.com
Center for ICT Studies Foundation

ICT Watch
Address : Jl. Damai Poncol II no. 61
Pondok Gede - Bekasi 17411
Phone / Fax : (021) 848 - 3652
e-Mail : info@ictwatch.com
URL : www.ictwatch.com