



Id-SIRTII



---

# INDONESIA COUNTRY UPDATE

---

“Internet Security 2009 and 2010 Projection: Latest Trend”



# STATISTICS

# INTERNET STATISTICS

- \* Indonesia population 242,968,342 (July 2010, est.)
- \* More than 180 ISP's, 40 NAP's, 3 IX's (national exchange)
- \* 1 million internet users (1999), 45 million users (June 2010)
- \* 100.000 internet subscribers (1999), 7 million (June 2010)
- \* More than 25 million online media regular visitors every day!
- \* 25 Gbit/s aggregate national IX traffic, 50 Gbit/s international
- \* +3 million computers (2 million notebooks) sales (March 2010)

# MOBILE STATISTICS

- \* 175 mil. numbers, 135 mil. unique users, 85 mil. GPRS phone
- \* 31.824 villages within the country will be connected in 2014
- \* 31.000 (Telkomsel), 29.000 (Indosat), 26.000 (XL) cellular BTS. Already serving 99% of 5.748 district (kecamatan). Most of BTS are GPRS/EDGE (data / internet) ready
- \* +3 mil. broadband users, 12 mil. 3G subs., 45 mil. active GPRS
- \* +1.000.000 Blackberry service subscribers (January 2010)
- \* 10 cellular operators AXIS, XL, ISAT, TSEL, 3 (GSM/GPRS/3G); ESIA, FLEXI, FREN, SMART (CDMA/EVDO); CERIA

# STUDENTS STATISTICS

- \* [http://nisn.jardiknas.org/cont/data\\_statistik/index.php](http://nisn.jardiknas.org/cont/data_statistik/index.php)
- \* Students Population 34.389.195 (in the end of 2009)
- \* More than 40 million students will be connected to the Internet in the year 2012 (Jardiknas Project - Depdiknas) \*) terminate
- \* 40 million = overall students population in Europe Union
- \* 40 million = 25% of overall students population in ASEAN
- \* 40 million = 20% share of ICT potential market in Indonesia
- \* Early in 2010 all cellular providers engaged students market

# CYBER LIFESTYLE

# ICT MARKET PROFILE

- \* Telecommunication services price war, promotion package
- \* Low ARPU, application/value added services revenue increasing
- \* Computer hardware for internet use, price < 5 million (US\$500)
- \* Combination of Netbook + cellular data service modem (US\$300)
- \* Internet gadget, price < 1 million (US\$ 100, lower everyday)
- \* Broadband access plan price (flat), cellular < 200K (US\$ 20)
- \* Broadband access plan price (flat), home < 200K (US\$ 20)

# ALWAYS ON GENERATION

- \* Always connected 24 / 7 to the internet, online communication
- \* Trend: using mobile / portable device (PDA, Laptop, Netbook)
- \* Highest gadget ownership ratio within the region (ASEAN)
- \* Lifestyle: news, social net, blogs, micro blog, chat, fun/games
- \* 40 % internet access origin: from office, school/campus (day)
- \* 40 % internet access origin: cyber cafe, hotspot, home (night)
- \* 60 % internet access device: gaded, netbook, laptops, mobile

# BLACKBERRY BOOMING

- \* US + Canada is the largest Blackberry population in the world
- \* 1 million in US (2000 - 2009), 41 million worldwide (2010)
- \* Largest Blackberry Black Market (70% non operators handset)
- \* US + Canada Blackberry users are Corporate account (BES)
- \* 1 million in Indonesia (2007 - 2009) GSM XL 335K, TSEL 290K, ISAT 290K, AXIS 45K, 3 30K, SMART 10K (CDMA)
- \* Most of Indonesian Blackberry users are Personal account (BIS)
- \* Price drop from 300K monthly to 90K flat rate Rp. (US\$ 9)

# FACEBOOK STATISTICS

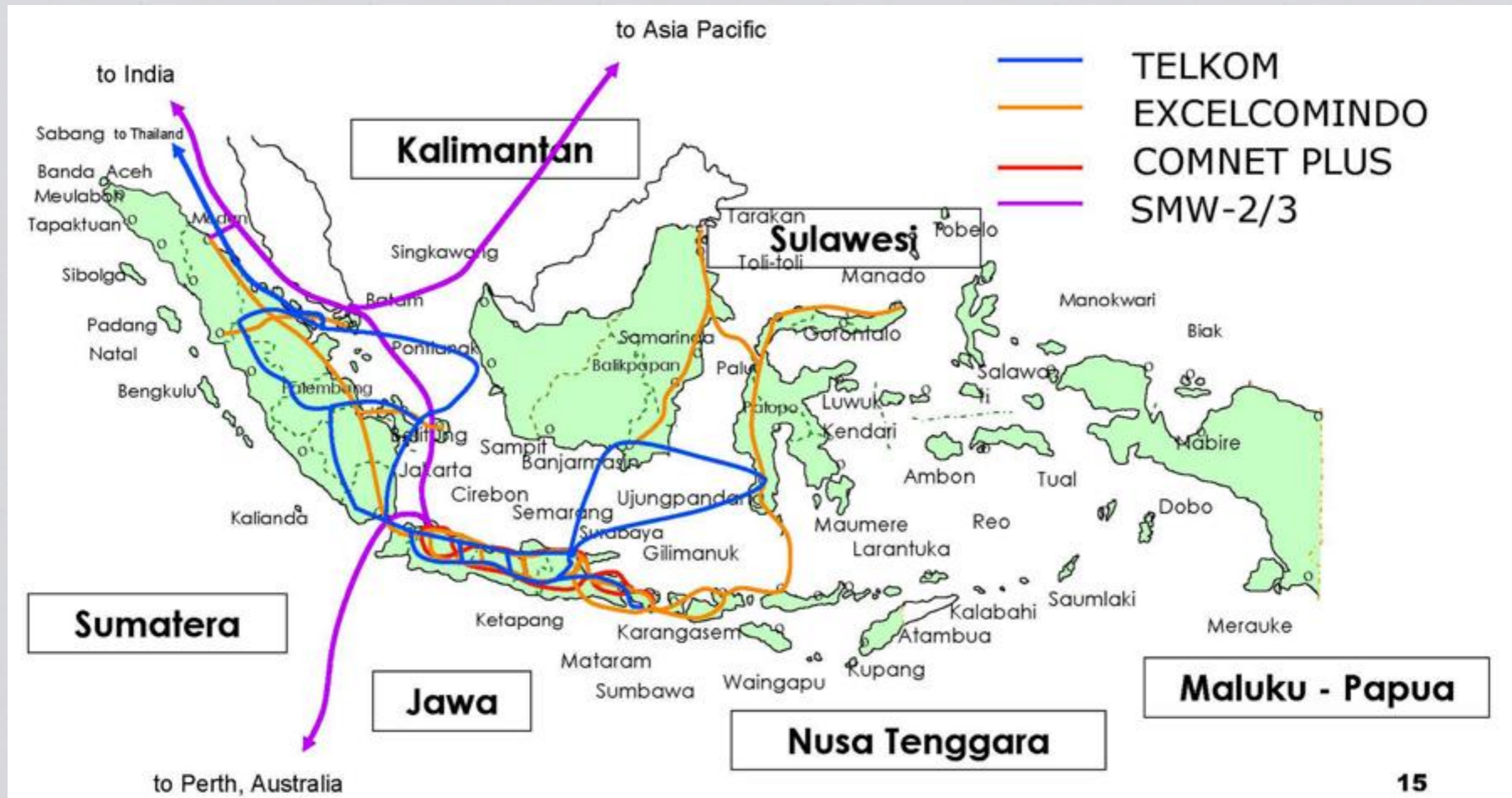
- \* US (125,881,220), UK (26,543,600), Indonesia (25,912,960)
- \* Number of male users on Facebook in Indonesia: 15,303,500
- \* Number of female users on Facebook in Indonesia: 10,489,980
- \* Penetration in Indonesia to population: 10.78 %
- \* Penetration in Indonesia to online population: 86.38 %

# INFRASTRUCTURE

# INFRASTRUCTURE FACTS

- \* Most of penetration rely on limited wireless infrastructure i.e. GPRS/EDGE, 3G, LTE, WiMAX, WiFi services based on non renewable natural resources: frequency
- \* Degradation of network handling capacity: saturation on frequency re-use policy may causing degradation of services
- \* Cable broadband distribution less than 9 million, zero growth after 20+ years industry protection, only available in major cities (most populated island Java, Bali, Sumatera, Kalimantan, Sulawesi), more than 50% capacity was deploy only in Jabodetabek area
- \* In most rural area using limited & high cost VSAT services

# EXISTING FIBER OPTICS



# MORE CABLES NEEDED

- \* In the near future bandwidth consuming interactive multimedia application (i.e. triple play) will be widely used by users. Only end to end reliable cable networks could handle such traffic
- \* Wireless networks only fits to mobile services. It's not intended to be used as carrier (inter city) or distribution (inter BTS) links
- \* For fixed data & internet services, wireless networks are just for temporary solution to accelerate penetration & growth boosting
- \* Only cables solution could solve the problem, to extend network handling capacity, to provide more reliable backhaul links
- \* Metro Ethernet Networks only available at several major cities



# PALAPA RING FACTS

- \* Investment US\$ 1.524.515.000, initial capacity 640 Gbit/s. ISAT, XL & others investors consortium members has canceled the implementation. Only Telkom just start at NTB – NTT segment
- \* Total of 35.280 km subsea cable (16.000 shallow sea, 12.885 middle sea, 6.394 deep sea) including buoy
- \* Total 20.739 km land cable (Sumatera 7.402,5 km, Jawa 3.542, Kalimantan 5.345,5 km, Sulawesi 5.813 km, Maluku 2.988 km, Nusa Tenggara 3.480 km, Irian 4.958 km)
- \* Consist of 2.063 km Connecting Rings (redundancy, fail over loops) 7 Rings connecting 465 municipalities city within 33 Province

# THE RISK

# INCREASING RISK

- \* Real incident reported: phishing, identity theft, data (information resources) stealing & forgery - bot attack, defamation, fraud, industrial espionage, critical information resources hostages, corporate information leakage, insider attack (i.e. virus spread)
- \* Cases: cyber war, fraud, defamation, hoax, gambling, trafficking, child predator, pornography, prostitution, money laundering & terrorism, underground economy - UU ITE 11 / 2008
- \* Malicious code & common vulnerabilities attack - fraudulent software are widely used (not updated), political (ID vs MY)
- \* Hatred & racism causing mass protest & content blocking policy

# RECENT INCIDENT REPORT

- \* Web defacing rally (vandalism) are the most favourite action
- \* Incident caused by political issues mostly comes from Malaysia
- \* 1 million events (possible attack) daily, mostly CN & US IP's
- \* Most incidents caused by KNOWN application and or network vulnerability + virus (using illegal and or counterfeit OS/apps.)
- \* Cyber fraud, phishing, nigerian scam (email, SMS), local virus, malware (from warez activity), local SPAM increasing last 2 years
- \* Social network attack, messaging service attack, targetted attack

# CYBERWARFARE

# BACKGROUND

- \* ICT changed the world: people interaction, workplace, lifestyle, business, government, art & culture. More dependencies to the technology & more risk. Now, this is the world of online society
- \* Competition to gain ICT supremacy will be easily burn political issues causing uncontrolled widespread cyber warfare involving many group of interest that could be very difficult to identify who they really are & to detect their presence. So how to prevent, protect & manage national ICT resources are the most necessary & prior things to do & how to build effective preemptive measure
- \* ICT will become the most fragile & critical infrastructure. Since it was internetworked so every node are related. There is no way to stop the threat or attack by simply turning off the system

# INFORMATION WARFARE

- \* ICT offenses to prevail, take over, dominate & control targetted others entity ICT's resources to gain supremacy amongs others, build propaganda to raise public opinion, international perception
- \* Not an open direct attack. Always silent, anonymous, randoms, distributed, undercover, untraceable & continuously operations
- \* Using widespread any unrelated potential attacking resources, cross borders, internetnetworked & way beyond any jurisdictions
- \* Nobody's know who is the real enemy & who is attacking who. Cyberwarfare use complex strategy & involving many different parties, amateur, professionals, military & civilians, organization

# INTERNATIONAL CONTEXT

- \* Ideology is no longer perceived as major threat, the main reason now is to make more money, winning competition & to dominate
- \* Malaysia claims the Indonesian art & culture to win local tourism market competition, since both have many historical similarities
- \* Singapore conduct marketing campaigns into Indonesia's market to dominate local potential economy, market & product brandings
- \* China, Russia has the most leading, sophisticated, well organized, attack activity that aimed for information espionage, piracy, fraud, business data & information leakage, identity theft, around the globe but mostly targetting US ICT resources. China, Russia also has the largest underground economy in the world, billions \$/yr

# INFRASTRUCTURE ATTACK

- \* **Hijacking**, to intercept & to take over control of ICT resources
- \* **Interruption**, disrupting & to take down Internet infrastructure
- \* **Modification**, change the contents into destructive materials
- \* **Fabrication**, spreading damages, well planned targetted attack
- \* Using techniques: DDOS, DNS, routing poisoning, SPAM, scam, phishing, malware (viruse, trojan, botnet, rootkit), identity theft
- \* Aimed to destroy information infrastructure & to threaten safety of lives, property & public services, since many of critical sectors rely on ICT. Estonia has experienced this massive attack in 2007

# INFORMATION DEFENSE

- \* Conducting cyber defense (monitor, detect, defense, anticipate, prevent, mitigate, recover, countermeasures) our infrastructure
- \* Organize National Cyber Security framework to assure & evaluate periodically our contra intelligence & proactive defense initiatives including best practices over the information security deployment
- \* Building national information data center, backup (DRC), disaster recovery & rehabilitation capability, providing secure emergency channel & resources to establish & maintain critical infrastructure for telecommunication & public services during the hard events
- \* Performing CERT/CSIRT/CC daily activities to coordinate national incident response handling & to join international collaboration

# HOW TO PROTECT

# COMPUTER PROTECTION

- \* Use only updated legal Operating System (OS) and application
- \* Updated legal Anti Virus, Anti Malware & Firewall tools is a must
- \* Periodically updated, cleaning apps trash & backup procedures (computer settings, OS & application configuration, data)
- \* Do backup twice with different external media & keep it safe at several places. Backup cost is always cheaper than recovery cost
- \* Strongly recommended protection tools (Deep Freeze, Windows Steady State etc.) & never log in as Administrator level users
- \* Never trust any of external devices or media, files or applications

# PUBLIC ACCESS PROTECTION

- \* Make sure you always cold boot the computer before you use it
- \* Takes several minutes to check any suspicious or hidden activity at Task Manager, do quick virus & malware scanning check with your own trusted & secure protected portable tools
- \* Beware of hijacking tools i.e. keylogger & remote access utility
- \* Never use public access terminal for critical transaction i.e. email (private), internet banking, e-commerce, company data transfer
- \* Don't leave your terminal unattended & unprotected, not a second

# WIRELESS ACCESS PROTECTION

- \* Always ask for official Wireless SSID's & never trust "Free WiFi Access" alike SSID's. It could be attacker with fake Access Point
- \* Wireless is open network, it is important to know basic knowledge about sniffing, side jacking, MITM, hidden surveillance camera
- \* Don't open your network sharing, make sure & always turn off your others wireless data connection i.e. bluetooth
- \* Never use public access terminal for critical transaction i.e. email (private), internet banking, e-commerce, company data transfer
- \* Don't leave your terminal unattended & unprotected, not a second

# SURFING PROTECTION

- \* Use only HTTPS connection if available, always check validity of CA certificate, use most secure and updated browser available
- \* No script, no pop up, read before you click! You can always has an option to click NO or CANCEL, pay attention in every warning
- \* Always use parental control for your kids (it's a default features in every latest browser), beware of phishing site, use DNS filter, never trust downloadable materials, use "open in a new tab" features not "new windows", employ any others useful browser add on
- \* Make sure clean log out, clear & clean up swap, cache, cookies, history, bookmark (use private browsing features), don't save your username passwords (check browser configuration)

# EMAIL PROTECTION

- \* Always use plain text mode not rich text mode (HTML, MIME etc.)
- \* Turn off auto open files (attachment, HTML) mode & always use latest & updated email anti virus and anti SPAM protection
- \* Never trust any attachment files, scan it, you can always ask for confirmation from the sender before you open the attachment
- \* Always use email client at your own trusted computer or you can use portable email client with portable device if applicable
- \* Use PKI (i.e. GPG) to make sure email authorization & transaction
- \* Only use secure encrypted email protocol (POP, IMAP, SMTP)

# MESSAGING PROTECTION

- \* Use latest most secure & updated messaging application & never spread your ID to others peers that you're not trust
- \* Never trust unknown new friends, you can always double check it & ask them first to make sure, & to identify who they really are. Background check are always necessary to the stranger
- \* Never trust DCC files or materials & or links, double check it first
- \* If you have to download files or materials you should scan it with latest anti virus & anti malware before you open it
- \* Use DNS filtering services to protect from most phishing sites, ads, SPAM, malware spreading sites & any others untrusted content

# E-COMMERCE PROTECTION

- \* Never use unsecured or public access terminal. Use your own computer. Make sure it safe & clean before make any transaction
- \* Make sure that you always connected in secure mode (HTTPS) & always checkt the validity of CA certificate, the expiry date etc.
- \* Make sure that you access to the real official web site not a fake one. Beware of phishing attack. Never click external links that was sent to you by email, messaging/chat and or any others pops up
- \* Always use DNS filtering protection, latest anti virus, anti SPAM, anti malware, anti phishing. Make it double if necessary because it will never enough to prevent any such incident possible & losses

# SOCIAL NETWORK PROTECTION

- \* Never add unknown new friends. Always ask for confirmation to mutual friends. Leave direct basic questions message to the suspicious account. If he gives proper responses it could be ok
- \* Be conservative. Limiting exposure of privacy information decide how much you are willing to share. Not everybody needs yours, so think about it again before you decide wich is your secrecy
- \* Never use free mail. Use your own domain & email addresses or your corporate account (if it's allowed), it's cheaper & more safer
- \* If something happens, report to admin, broadcast alert to all of your friends, hope you have backup, make new account & tag your old account as impersonating & fraud. Ask everybody to do it

# ATM & SMS PROTECTION

- \* Knowing the latest & updated technology and service procedures to understanding the weakness, loop holes & fraud techniques & to detect unusual process, consider to use PIN management & one time token if applicable. Ask your banks about latest update
- \* Knowing the card types (magnetic stripes, chip, RFID) & what kind of services (debit, credit, e-cash). Then protecting your card physically, hiding the CVV2 code & use anti magnetic sleeve
- \* Never trust and always double check for any transaction & be careful while in the middle of transaction, watch the EDC machine
- \* Look at the detail of physical environment, check all possibilities: skimming, hidden camera, unauthorized personnel & assistance

# PASSWORD PROTECTION

- \* Change your password periodically, more often are better and never share your password to anybody for any reasons
- \* The longer & more complicated combination are more stronger. Not easy to remember & to reveal. Also use unpredicted phrase
- \* Keep it in the safe secret places. Nobody's know about it. Ever
- \* Use password management application or services or one time token password services. The problem is how to make sure & to secure the token delivery channel from the system to the end user. Most of delivery channel is open public network i.e. SMS
- \* Don't use one for all password, use different for each account

# PORTABLE DEVICES PROTECTION

- \* Password protected any of your rewritable portable devices (flash disk, external drive, gadget, ipod etc.). Consider to use encryption
- \* Use the most possible, secure, limited & sophisticated file system if applicable i.e. NTFS, HFS+ (MacOS), Ext2/Ext3 (Linux) etc.
- \* Always backup your files, use latest Anti Virus & Anti Malware
- \* Keep devices with you all the time. Never lend it to anybody
- \* Beware the safety of your surroundings physical environment
- \* Do the highest secure wiping procedures possible for disposal

# ABOUT ID-SIRTII

# ID-SIRTII BRIEF HISTORY

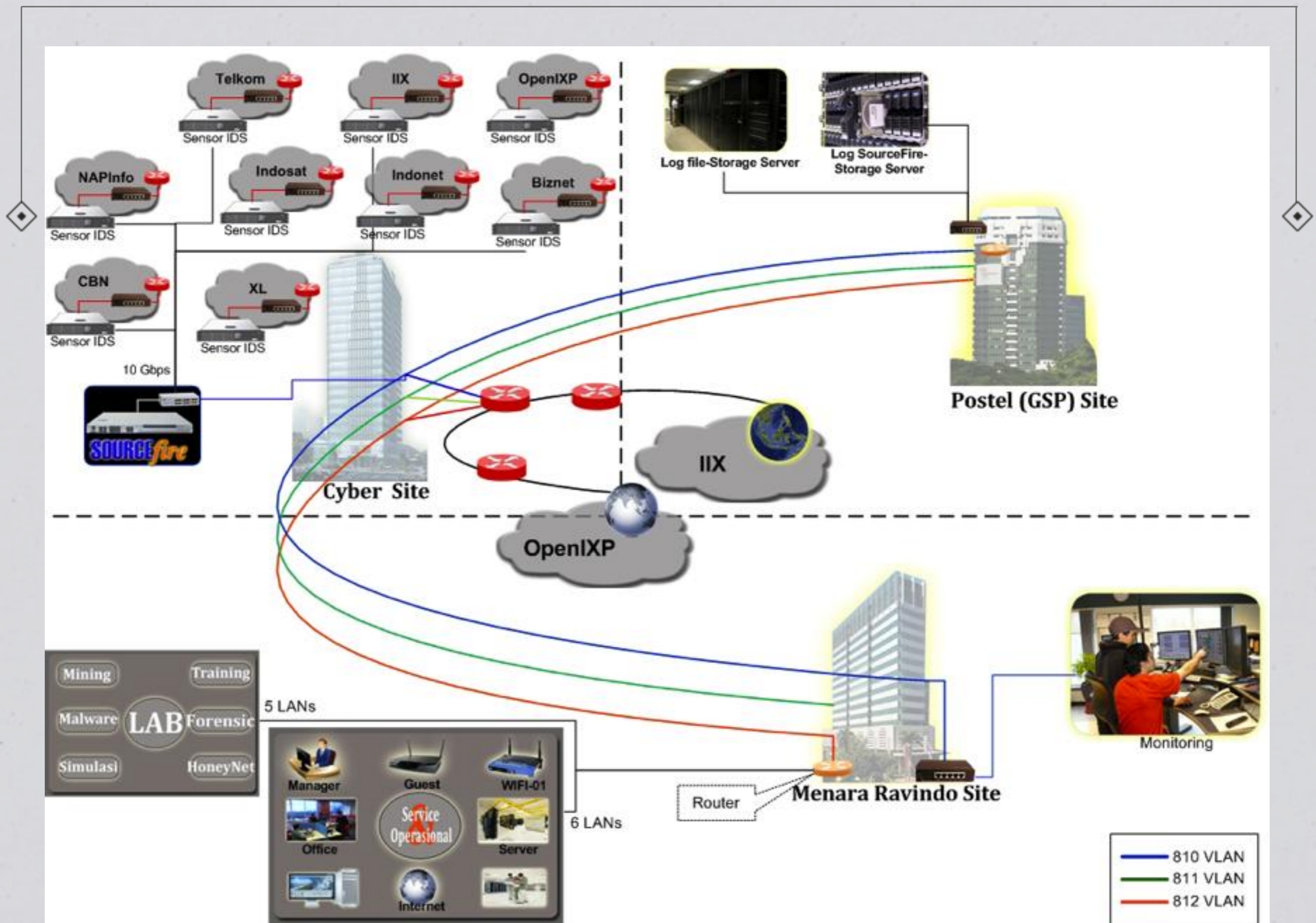
- \* Initiating by stakeholders: police, attorney general, ICT society, IT association (ISP, Internet Cafe), academicians and government
- \* Steering Committee Board founded in 2006 by Ministry Decree No. 27/2006, Executive board founded in 2007 by Ministry Decree No. 26/2007. Proposed new ministerial decree (June 2010)
- \* ID-SIRTII is a National's CSIRT/CC under the government agency Directorate General of Post and Telecommunication, Ministry of Communication and Information Technology
- \* General Member of APCERT (June 2009), promoting into a Full Membership (June 2010). Proposed membership to FIRST (2010)

# MISSION & OBJECTIVES

- \* Internet traffic monitoring
- \* Managing log files (law enforcement)
- \* Conduct security awareness campaign
- \* Assisting how to managing security
- \* Providing security training to public
- \* Conduct R & D, labs & collaboration

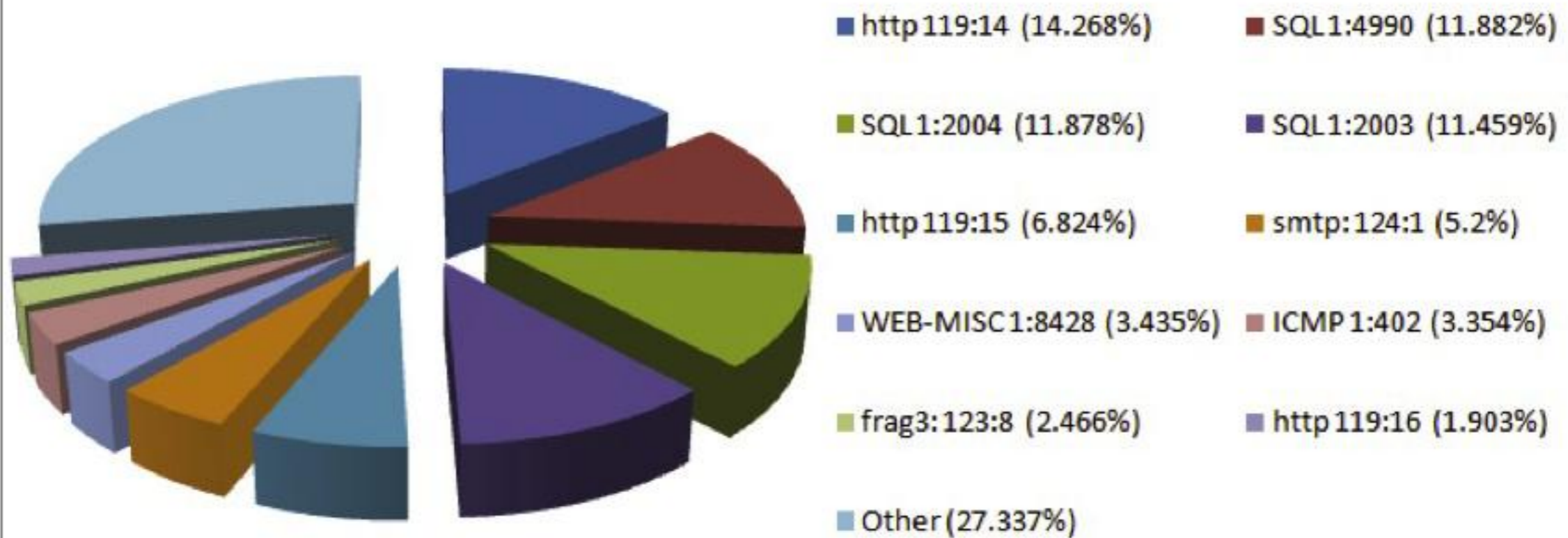
# EXISTING MONITORING

- \* 11 sensors: XL, Indosat, IM2, Telkom, Napinfo, CBN, Biznet, Indonet, Centrin, IIX (APJII), Open IXP (today, June 2010)
- \* Critical infrastructure: Government; Public Services; Defense, Military & Home Land Security; Energy & Natural Resources; Public Transportation; Stock Exchange, Finance, Investment, Bank; Education; Industry & Commerce; Public Health; Law Enforcement; Telecommunication, Media & Broadcasting; Art, Culture & Tourism; Government/State Owned Corporation
- \* Need more sensors & more interface to capture 70% traffic
- \* Future deployment (2010 – 2014) at 11 planned areas of BTIP Local Internet Data Centers & Exchanges within the country

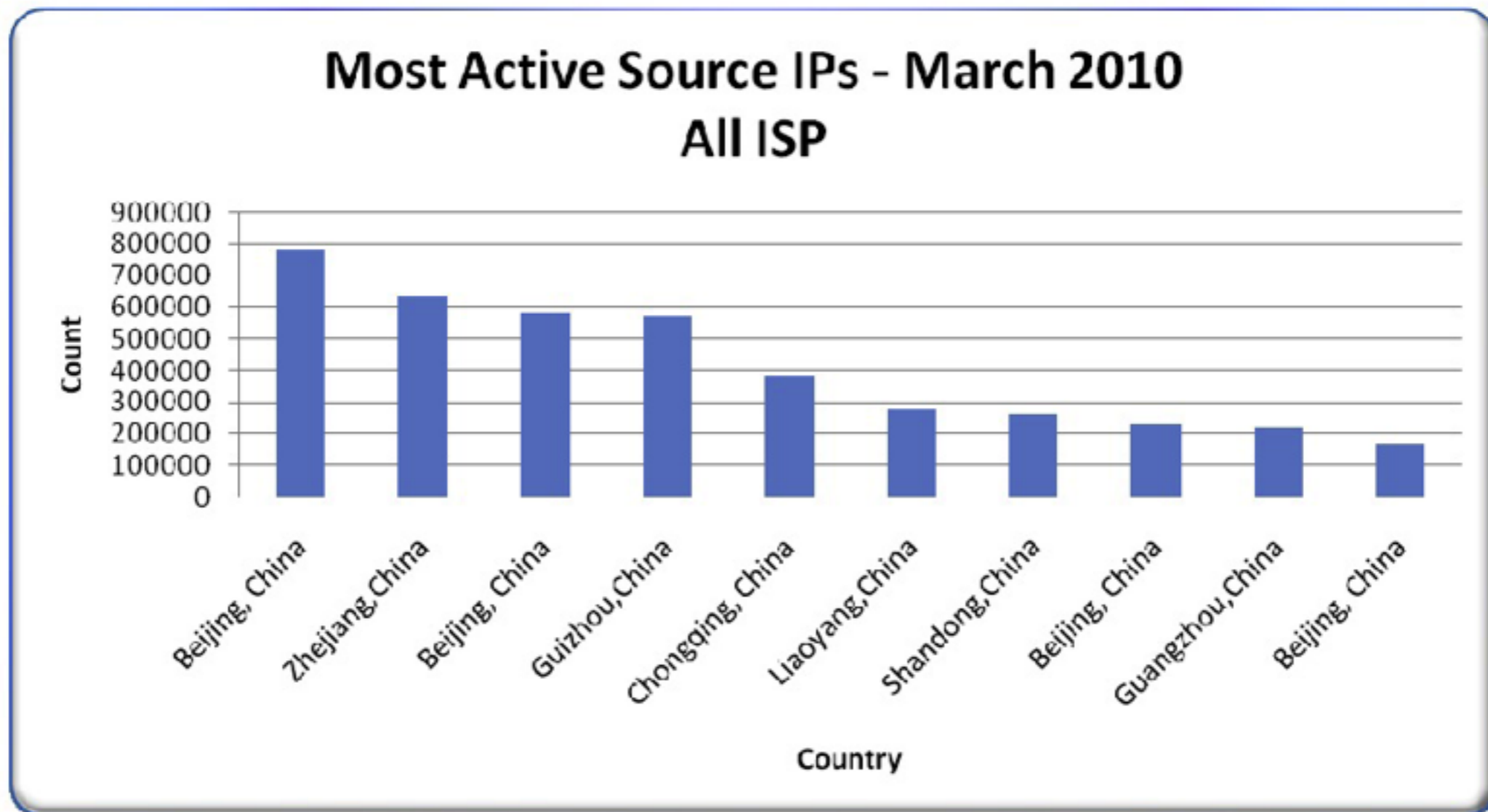


# MONTHLY TOP EVENT

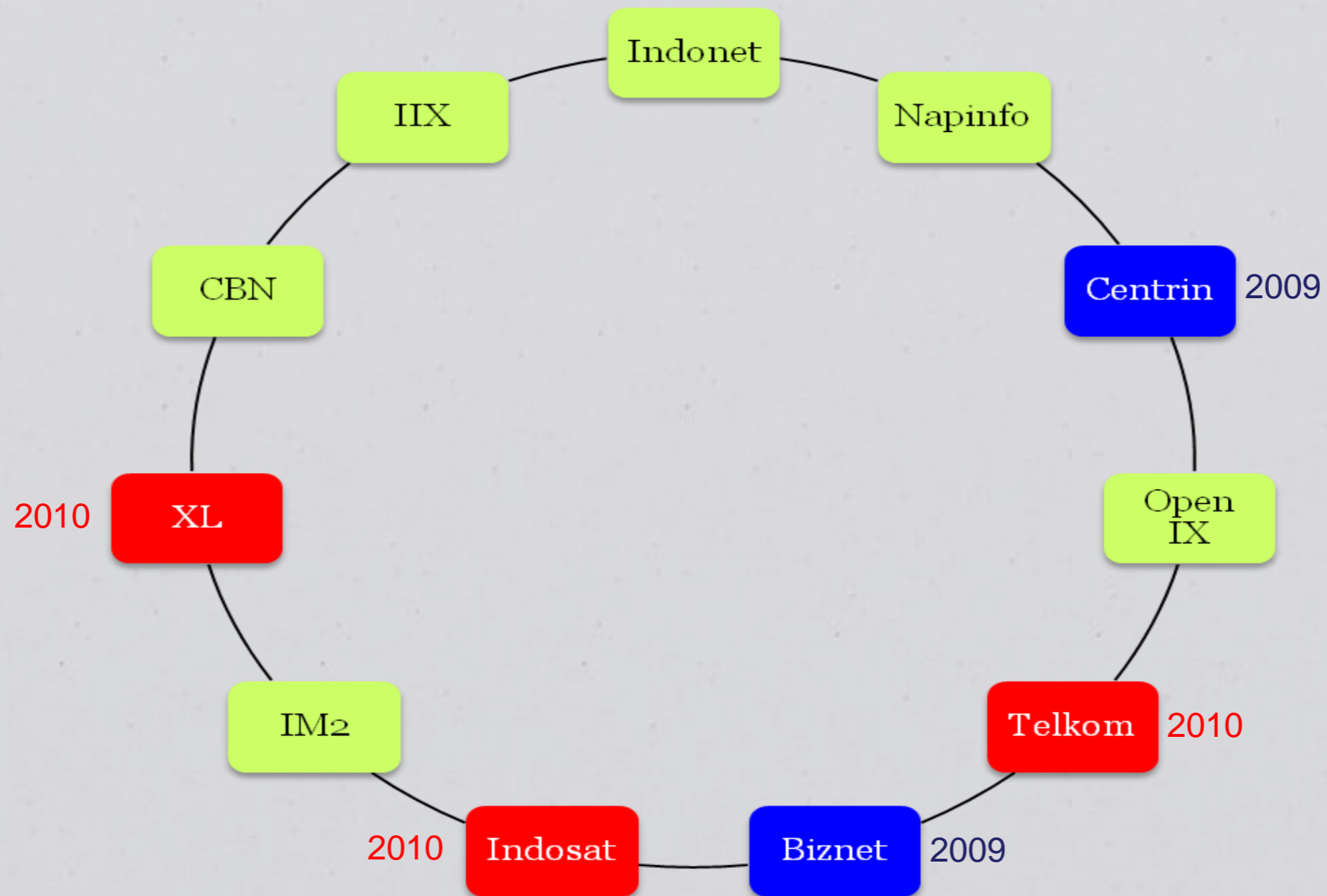
## TOP 10 EVENT - MARCH 2010



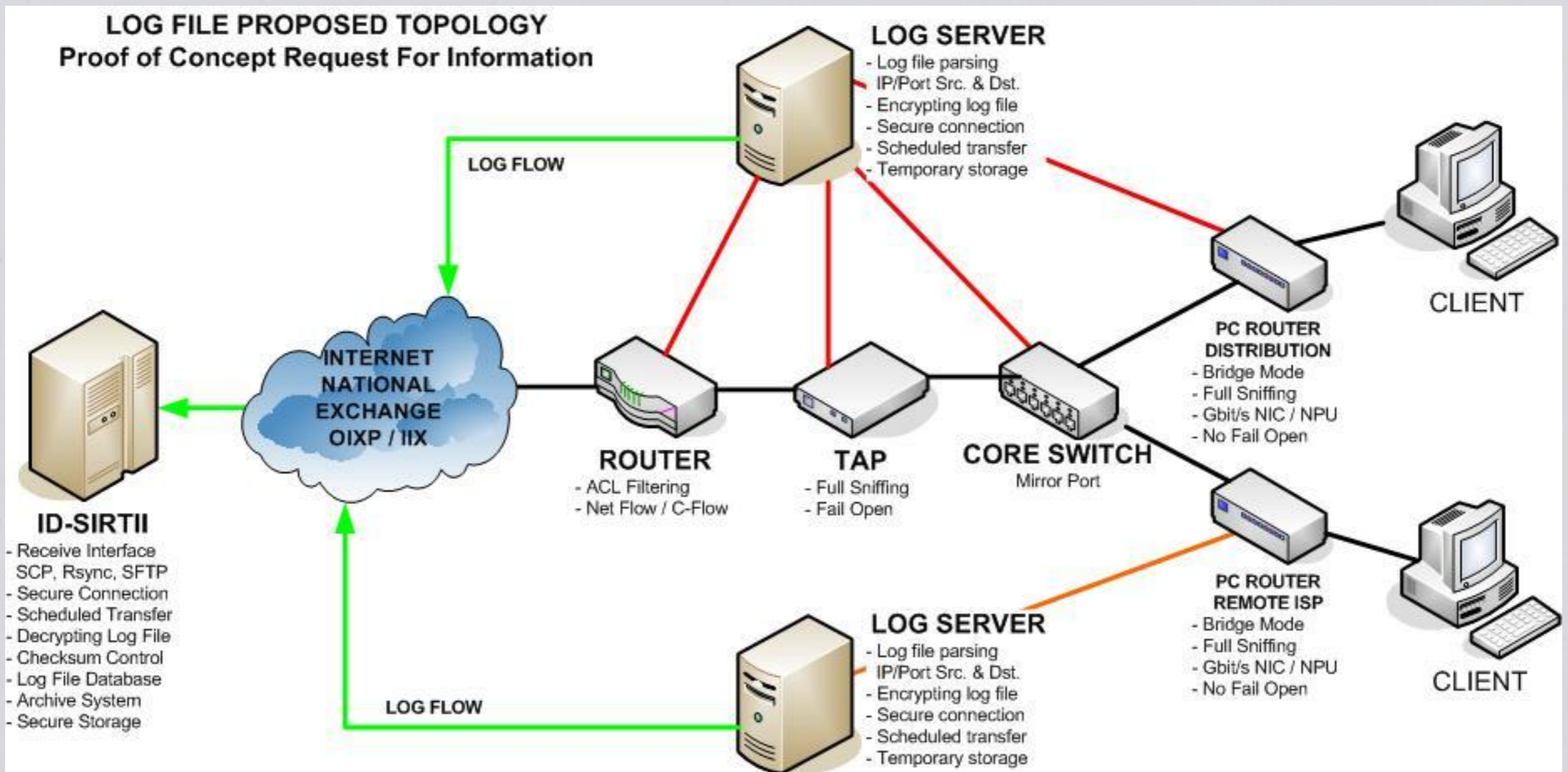
# ATTACKER SOURCE IP



# TSUBAME PROJECT



# LOG FILE TOPOLOGY



# NEXT PROGRAM (2010)

- \* Upgrading organization status into government full agency under the new cyber law act (no. 11/2008) or others future legislation
- \* Conducting security training center, simulation labs & malware analysis, digital forensic labs, national honeynet project, local DNS content filtering & resolver, anti SPAM project, children protection, OSS repository, local free mail, content delivery
- \* Joining international project i.e. Tsubame Project (JPCERT), drill test and research collaboration with vendors
- \* Participating international events (workshop, research, seminar, exhibitions, convention, including drill test etc.)

# ACTION PLAN 2010

- \* Installing More Tsubame Sensors (3 more units)
- \* Conducting Malware Analysis & Data Mining Program
- \* Conducting Nation Wide Honey Net Program
- \* Continue Anti SPAM & DNS Filtering Program
- \* Enhancing Threat Information Coordination
- \* Improving Security Technical Training

# ACTION PLAN 2010 (Cont.)

- \* Revising National Information Security Policies
- \* Developing National Internet Child Protection Program
- \* Developing Digital Forensics Laboratory
- \* Boosting Public Awareness Efforts
- \* Increasing Collaboration with Asian CSIRTs/CERTs
- \* Joining FIRST as General Member

# ID-SIRTII

- \* Ravindo Tower 17th Floor
- \* Kebon Sirih Raya, Kav. 75
- \* Central Jakarta, 10340
- \* Phone +62 21 3192 5551 ; Fax +62 21 3193 5556
- \* [office@idsirtii.or.id](mailto:office@idsirtii.or.id) ; [www.idsirtii.or.id](http://www.idsirtii.or.id)
- \* We look forward for future cooperation with you all. Thank you.