

**2019
NATIONAL
CONFERENCE**



**2019 NATIONAL
CONFERENCE**
Solo, 24 - 25 July 2019

THE ANATOMY AND EVOLUTION CYBERTHREATS IN THE WAKE OF DIGITALIZATION

Agung Nugraha, S.IP, M.Si (Han)
Plt. Deputy of Protection BSSN

EMPOWERING INTERNAL AUDITORS : EMBRACING THE 4IR



THE ANATOMY AND EVOLUTION CYBERTHREATS IN THE WAKE OF DIGITALIZATION

Agung Nugraha, S.IP, M.Si (Han)
Plt. Deputy of Protection BSSN

Solo, 25 Juli 2019

BUSINESS VS CYBER THREAT EVOLUTION



Computer era

RTGS, Online payment, Credit cards, ATM, POS, Digital Stock, Trading



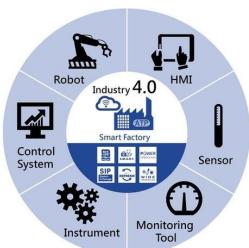
Website era

E-banking, octopus card, algo trading, P2P



Mobile and APP, social media era

Apple pay, Mobile banking, P2P, BITCOIN, 24 X 7 SERVICE



CPS, BIG DATA & AI

Robo Advisory, Crowd Funding, Digital Bank, Fortune Teller Cyber physical system (CPS), Revolusi industry 4.0

1988-2002

2002-2008

2008-2010

2010- Present

worm, virus, Malicious code, Trojan



Malicious code, Trojan, advanced worms, hacking web sites, identity theft, phishing



phone hijacking , DNS attacks, rise of botnets, sql attack, anti spam sites, competitive sabotage escalation, android hack, Social engineering,



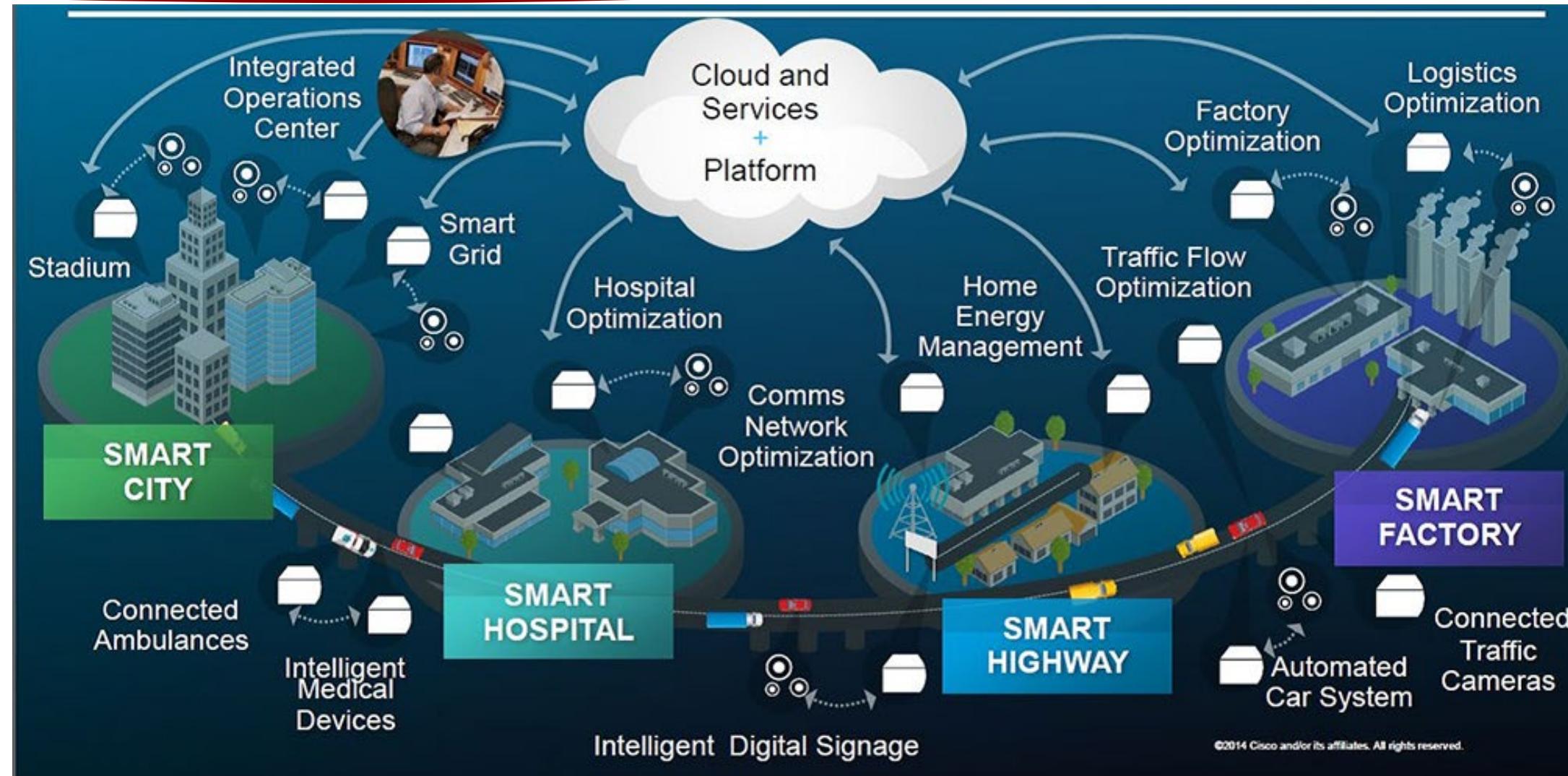
ransomware, malware, keylogger, bitcoin wallet stealer, cyberwarfare, cyber espionage, DoS, DDOS, Botnets etc



IoT Business Complexity



BADAN SIBER DAN
SANDI NEGARA



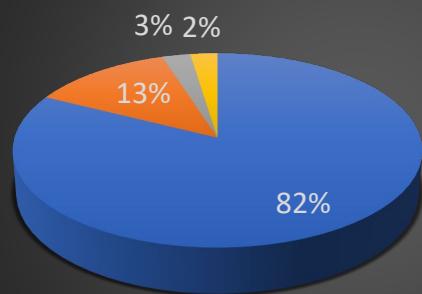
Profile of Attack Target Distribution 2018



BADAN SIBER DAN
SANDI NEGARA

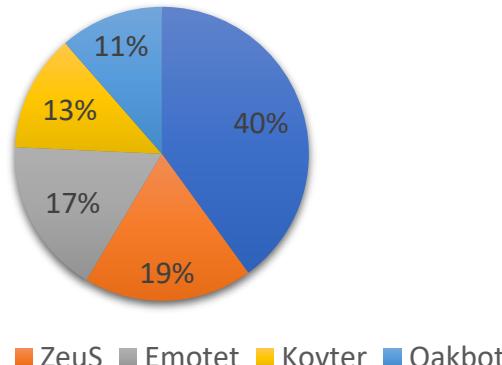
ENISA Threat Landscape Report 2018

Motivation

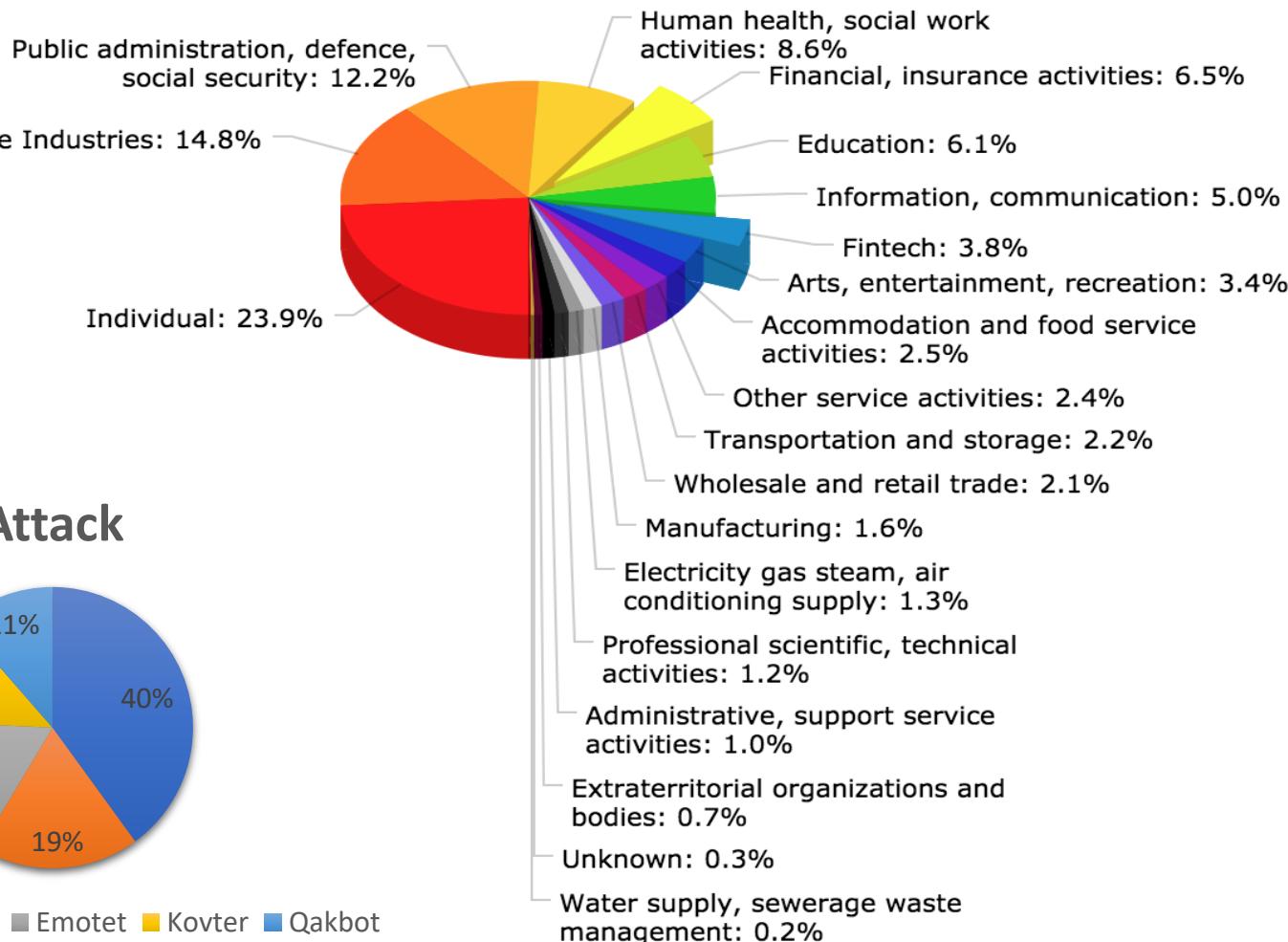


- Cyber Crime
- Cyber Espionage
- Hacktivism
- Cyber Warfare

Attack



<https://www.cisecurity.org>



PROFESIONAL



INTEGRITAS



ADAPTABILITAS TEKNOLOGI



TEPERCAYA

HIGHLIGHT – THE BIGGEST CYBERSECURITY CRISES OF 2019 SO FAR



BADAN SIBER DAN
SANDI NEGARA

AMERICAN MEDICAL COLLECTION AGENCY (AMCA) DATA BREACH

Sebanyak 7,7 Juta data pelanggan bocor dari database AMCA pada Bulan Juni 2019. data tersebut berisi biodata pasien, nomor asuransi kesehatan, dan saldo jatuh tempo dari asuransi milik pasien.

FIRST AMERICAN

First American, sebuah perusahaan properti besar di Amerika menampilkan informasi Jutaan pelanggannya di Halaman Website mereka. Informasi yang ditampilkan berisi bioadata pelanggan, nomor jaminan sosial, akun bank, dan dokumen pajak. Kejadian tersebut ditemukan pada Bulan Mei oleh Jurnalis Keamanan Informasi Brian Krebs.

CYBERWAR PLAN AGAINST IRAN

Dampak dari serangan terhadap dua kapal tanker milik US, Presiden Trump menuduh Iran menjadi dalang penyerangan tersebut. Alih-alih melakukan serangan fisik, Presiden Trump menyetujui untuk melakukan serangan siber kepada fasilitas nuklir milik Iran.



US CUSTOM & BORDER PROTECTION (CBP) CONTRACTOR DATA BREACHES

Pada Bulan Mei, Hacker mempublish 100,000 data *passport* milik penumpang yang mereka dapat dari Kontraktor yang bekerja sama dengan Bea dan Cukai Amerika Serikat bernama Perceptics. Kebocoran data ini menjadi pukulan bagi Amerika, karena kenapa data yang sifatnya terbatas dapat disimpan oleh Kontraktor

RANSOMWARE-LOCKERGOGA

Ransomware LockerGoga mengincar data-data di sektor industri dan manufaktur. LockerGoga mengganggu sistem otomatisasi Industri dan mengakibatkan berhentinya produksi.

SUPPLY CHAIN ATTACKS

Pada Bulan Maret Kaspersky melaporkan adanya celah kerawanan pada system live update komputer ASUS. Akibatnya hacker dapat menyusupkan malware pada celah tersebut dan mengancam jutaan pengguna ASUS. System live update adalah layanan purna jual dari ASUS untuk melakukan update driver perangkat (patching) secara online.

Sumber: www.wired.com/Biggest-Cybersecurity-Crises-2019-Sofar/



PROFESIONAL



INTEGRITAS



ADAPTABILITAS TEKNOLOGI



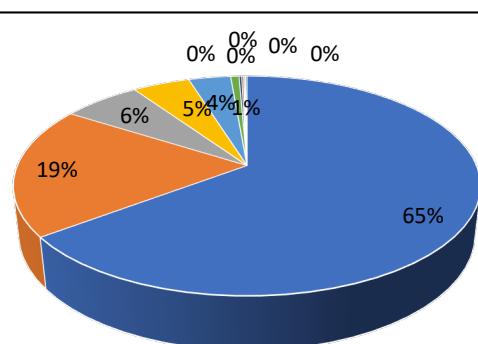
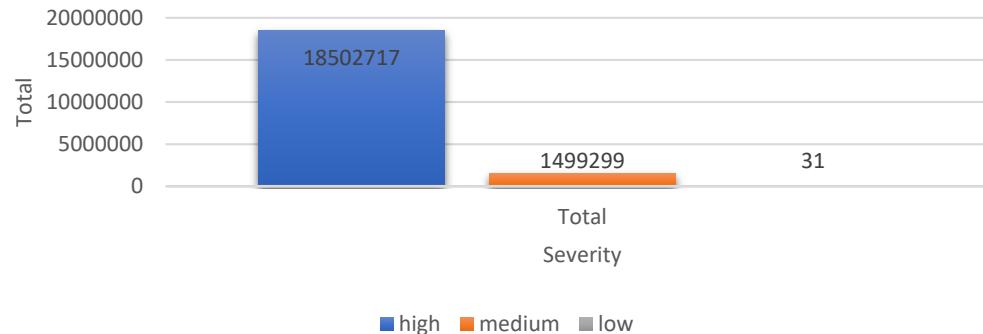
TEPERCAYA

STATISTIK – SERANGAN SIBER DI INDONESIA (Jan-Mei 2019)



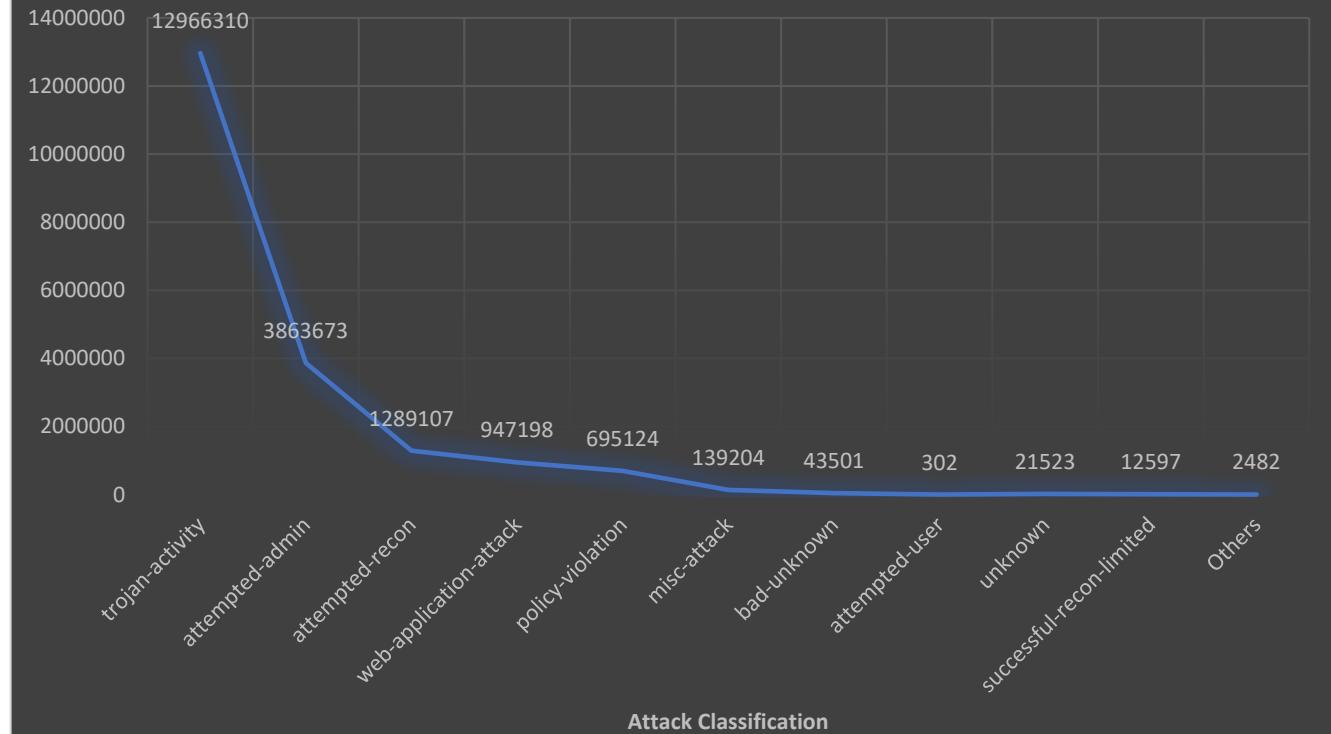
BADAN SIBER DAN
SANDI NEGARA

Severity Anomaly Jan - Mei 2019



- trojan-activity
- attempted-admin
- attempted-recon
- web-application-attack
- policy-violation
- misc-attack
- bad-unknown
- attempted-user
- unknown
- successful-recon-limited
- Others

Grafik Jumlah Serangan Berdasarkan Jenis Serangan



Source:



PUSAT OPERASI KEAMANAN SIBER NASIONAL
Id-SIRTII/CC



PROFESSIONAL



INTEGRITAS



ADAPTABILITAS TEKNOLOGI



TEPERCAYA

Peraturan Presiden Nomor 53/2017 dan 133/2017



BADAN SIBER DAN
SANDI NEGARA

PEMERINTAH

PUBLIK

INFRASTRUKTUR INFORMASI
KRITIS NASIONAL

Kerjasama Nasional, Regional, dan Internasional dalam urusan Keamanan Siber

Standarisasi
Produk

Sertifikasi
Profesi

Akreditasi
Lembaga

Penyidikan &
Digital Forensik

Monitoring

Infosec Assurance

Sec Awareness & Capacity
Building

Proteksi e-
Commerce

Persandian

Diplomasi
Siber

Penapisan

Pusat
Manajemen
Krisis

Pusat
Kontak
Siber

Dukungan
Mitigasi

Penanggulangan
Kerentanan

Penanggulangan
Insiden

Penanggulangan
Serangan

IDENTIFIKASI

DETEKSI

PROTEKSI

PENANGGULANGAN

PEMULIHAN

PEMANTAUAN

EVALUASI

PENGENDALIAN

PENYUSUNAN KEBIJAKAN

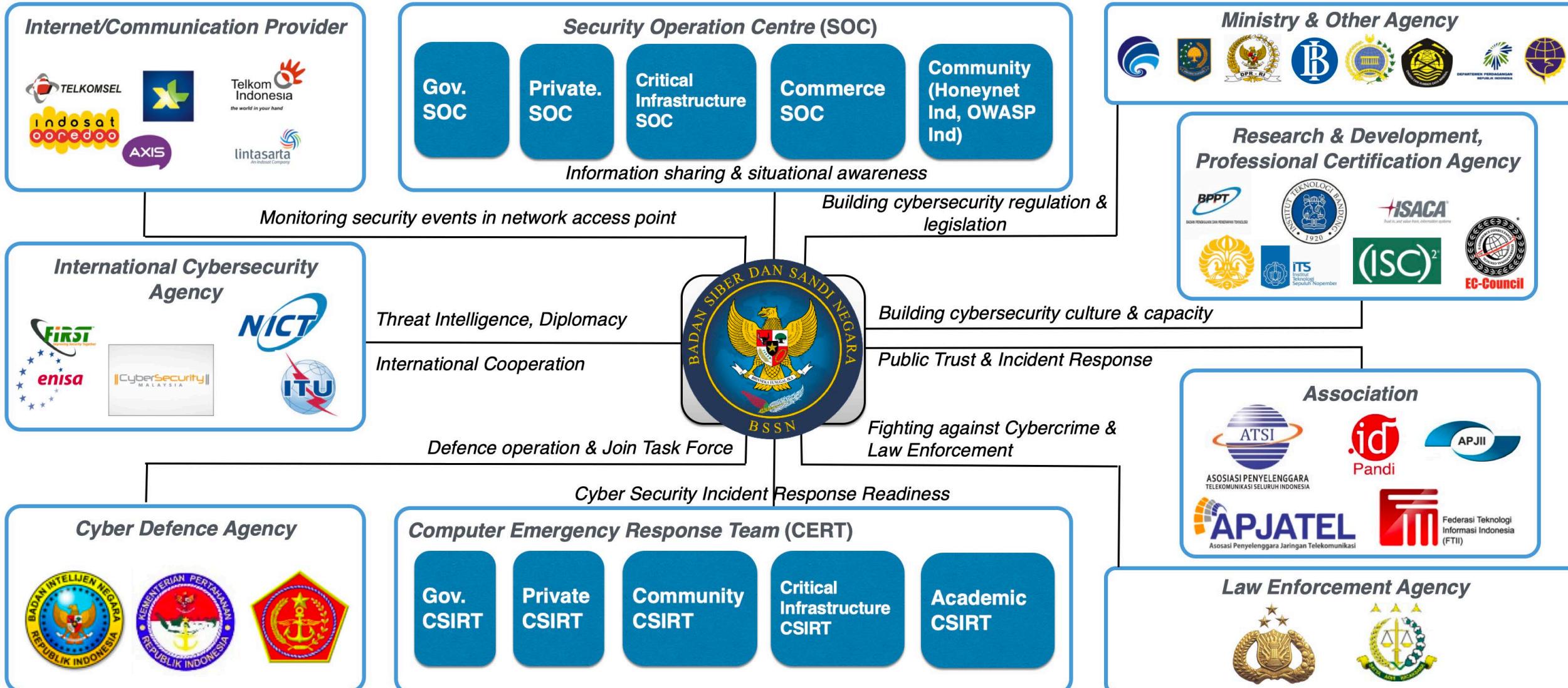
PELAKSANAAN KEBIJAKAN

PEMANTAUAN KEBIJAKAN

Collaboration in Cyber Security



BADAN SIBER DAN
SANDI NEGARA



Rancangan Peraturan BSSN tentang Audit Keamanan Informasi (AKI)



BADAN SIBER DAN
SANDI NEGARA

Tujuan

- Meningkatkan keamanan informasi Penyelengara pada Sistem Elektronik ;
- Sebagai acuan bagi Penyelenggaraan AKI;
- Memberikan kepastian hukum dalam AKI.



Ekosistem Audit Keamanan Informasi

1. Penyelenggara Sistem Elektronik
2. Lembaga Sertifikasi
3. Lembaga Sertifikasi Profesi
4. Auditor
5. Asosiasi Auditor KI
6. Lembaga Audit KI
7. Regulator
8. Penyelenggara pendidikan Auditor Keamanan Informasi

**“Kechilafan Satu Orang Sahaja
Tjukup Sudah Menjebabkan
Keruntuhan Negara”**



**Mayjen TNI Dr. Roebiono Kertopati
(1914 - 1984)**
Bapak Persandian Republik Indonesia



**BADAN SIBER DAN
SANDI NEGARA**