



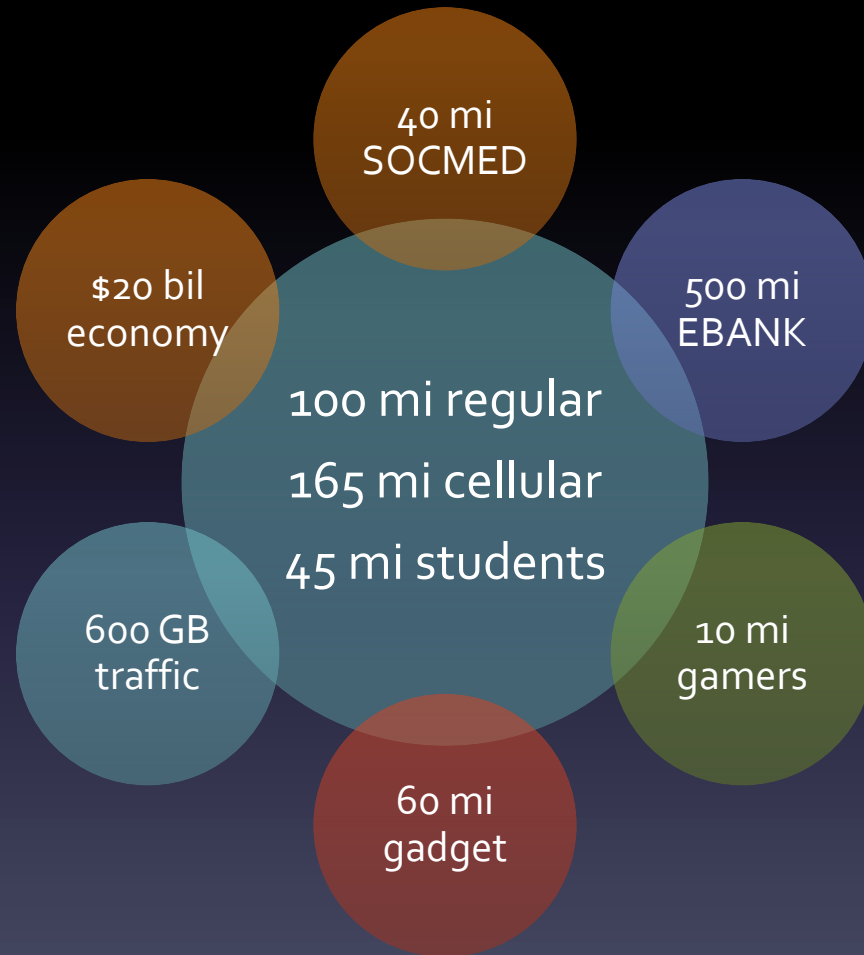
12-SIRTII

BATTLE OF THE FUTURE

Muhammad Salahuddien

Deputy of Network Operation

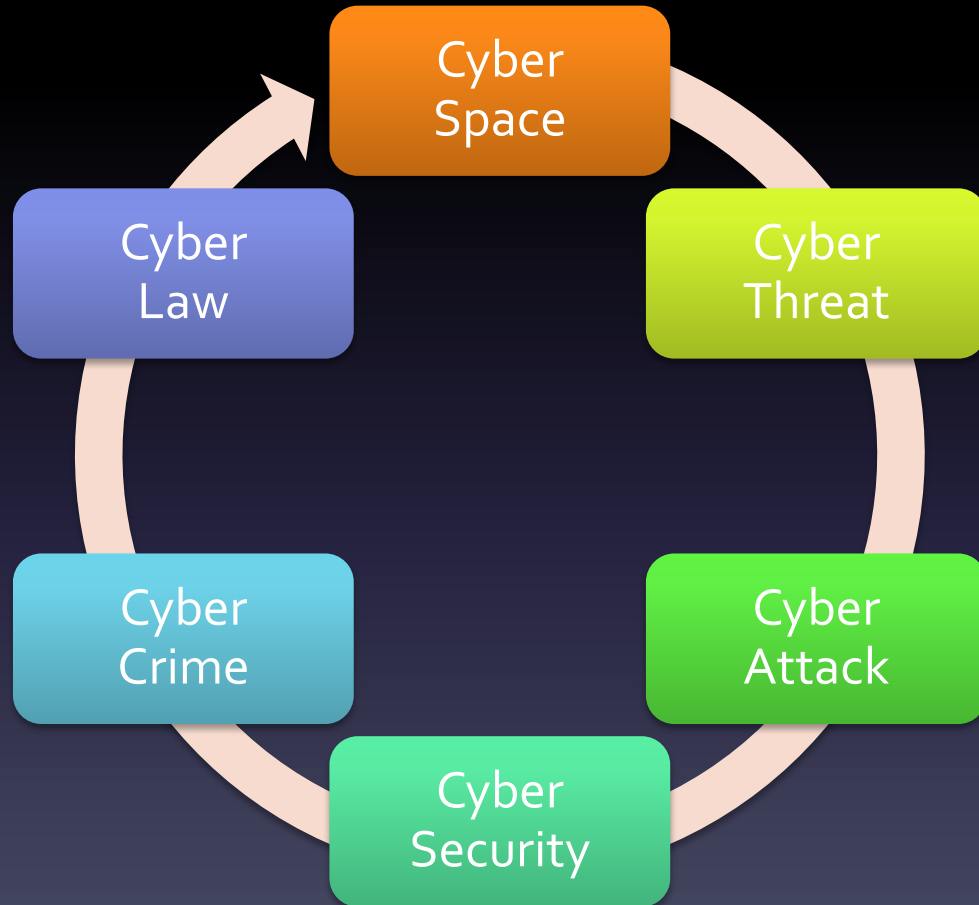
INTERNET SIZE 2014



INTERDEPENDENCY

- People interaction, workplace, lifestyle, business, art and culture heritage, military/defense, intelligence, government has more dependencies to the technology and more risk. This is the world of online society, online threat, online attack, cyber war, competition to gain information supremacy and to take over cyber resources
- How to prevent, protect, manage (critical) national ICT resources is necessary, prior action to build effective preemptive are needed
- ICT most fragile/critical internetworked infrastructure, no way to stop the attack by simply turning off the system (given situation)

CYBER CYCLE



CYBER SIX

- Cyber Space “higher the value, greater the risk”
- Cyber Threat “exploitation of vulnerability”
- Cyber Attack “to take over the resources”
- Cyber Security “defending information assets”
- Cyber Crime “when reality bites”
- Cyber Law “bring justice into the future”

CRITICAL SYSTEM



NATIONAL INTEREST



ATTACKER PERSPECTIVE

- Everybody and everything is the TARGET
- Individual computer experts ("hackers")
- Political issues, ICT supremacy, just for fun
- Intelligence agencies including cyber spy
- Criminals, cyber mafia, underground economy
- Businesses rivalry, trade secrets stealing
- Disgruntled employees, retired personnel
- Other parties may all seek to breach information security

VULNERABILITY

Natural Disaster
(earthquake, flood)

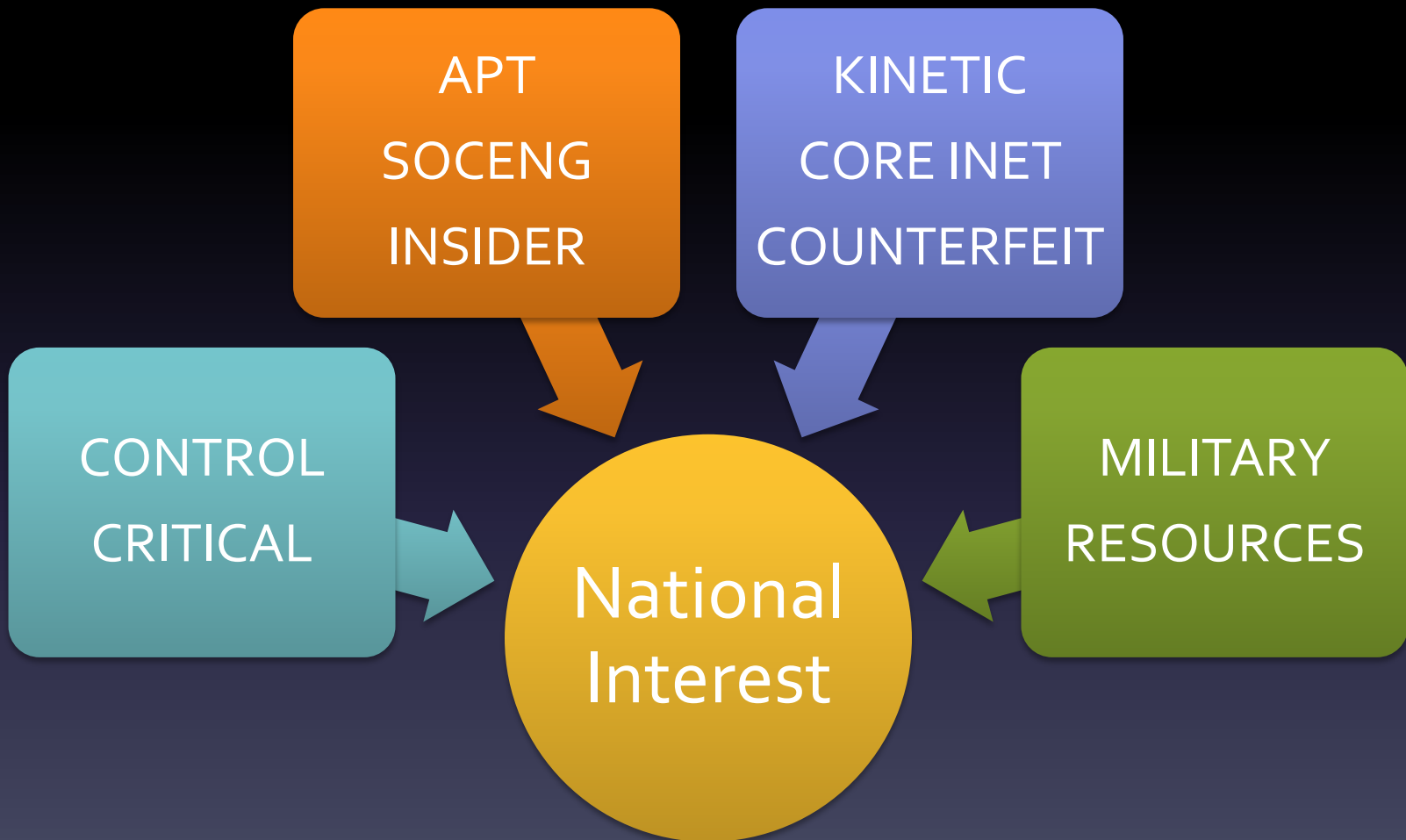
Social Unrest
(riot, chaos, war)

THREAT

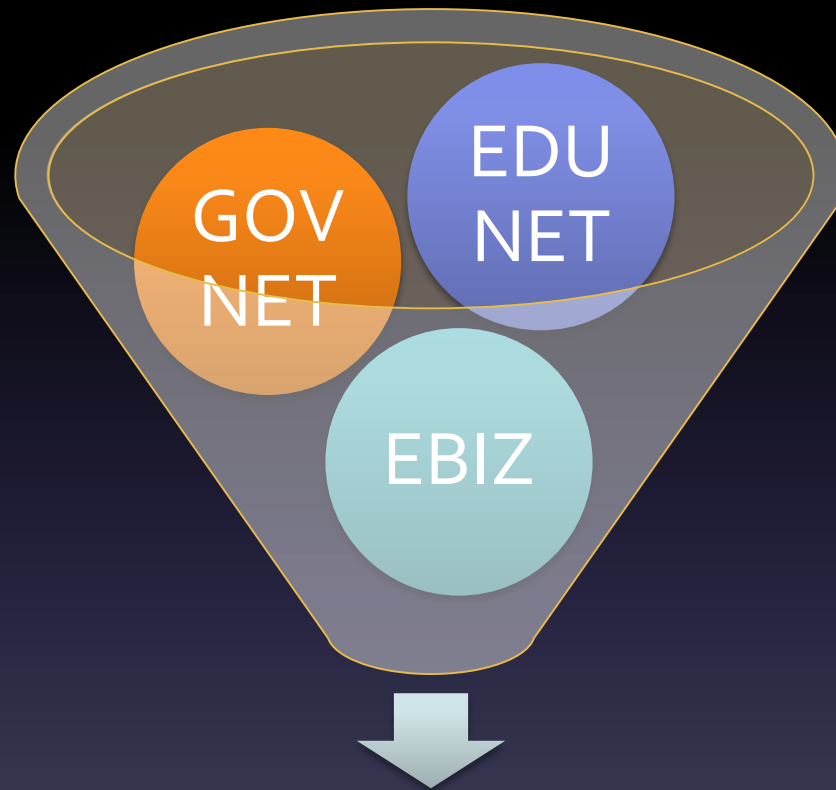
Lack of System
(policy, procedures)

Human Weakness
(social engineering)

VECTOR OF THREAT



RECENT INCIDENT



MOST VULNERABLE

INSIDER THREAT

Sophistication/targeted attack

Personal information stealing

Account hijacking and fraud crime

Lack of awareness, user behavior

Caused by data over exposure

Social engineering techniques

Phishing, malicious code as tools

Human, the weakest security link

Trojans and backdoor

Unsecure programming

Counterfeit equipment

Data/information misuse

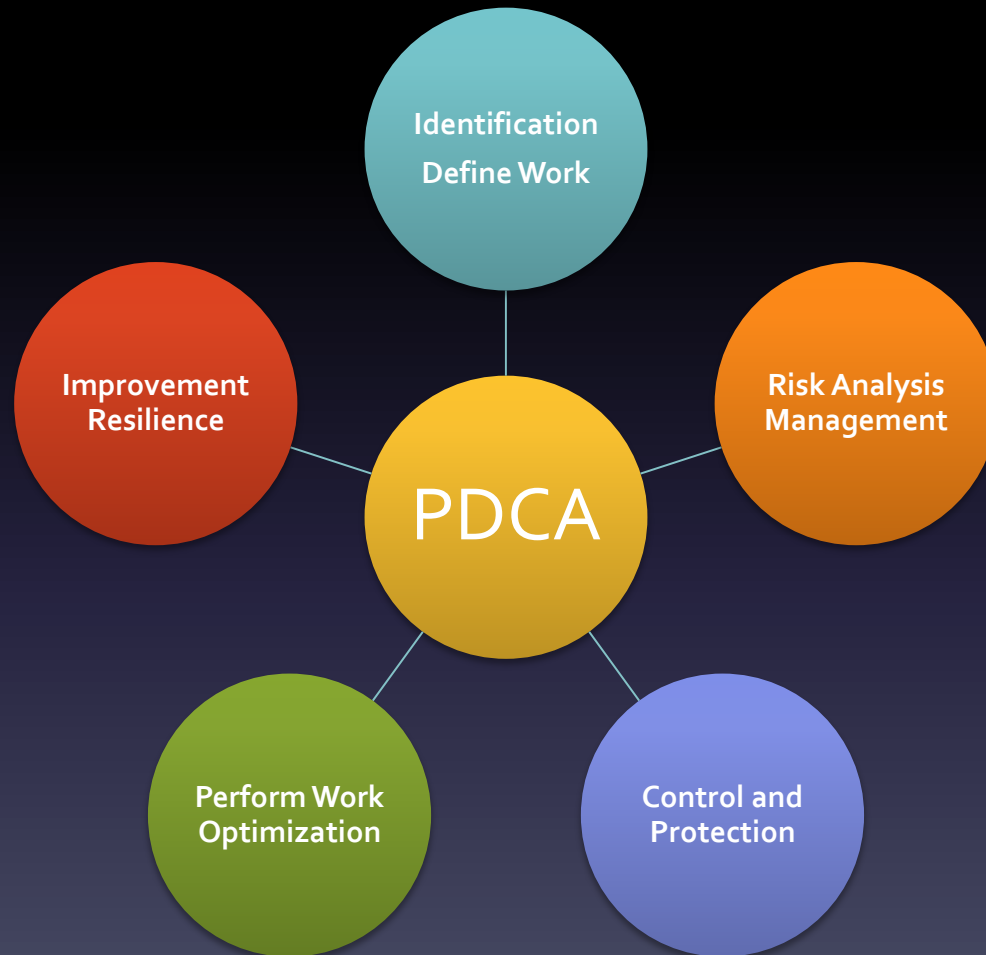
Level of access policy breach

Physical security perimeter breach

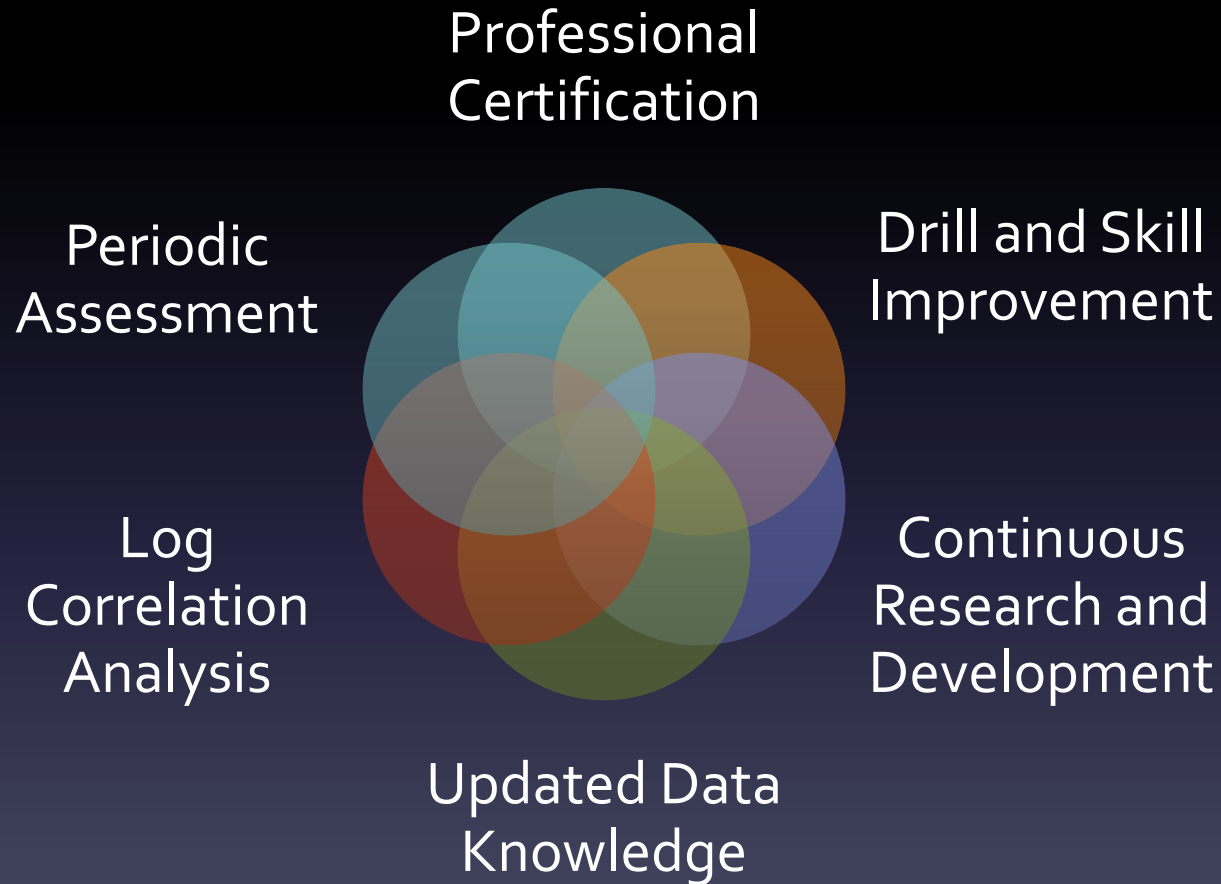
Inappropriate disposal procedures

Weak NDA and retirement program

ISMS



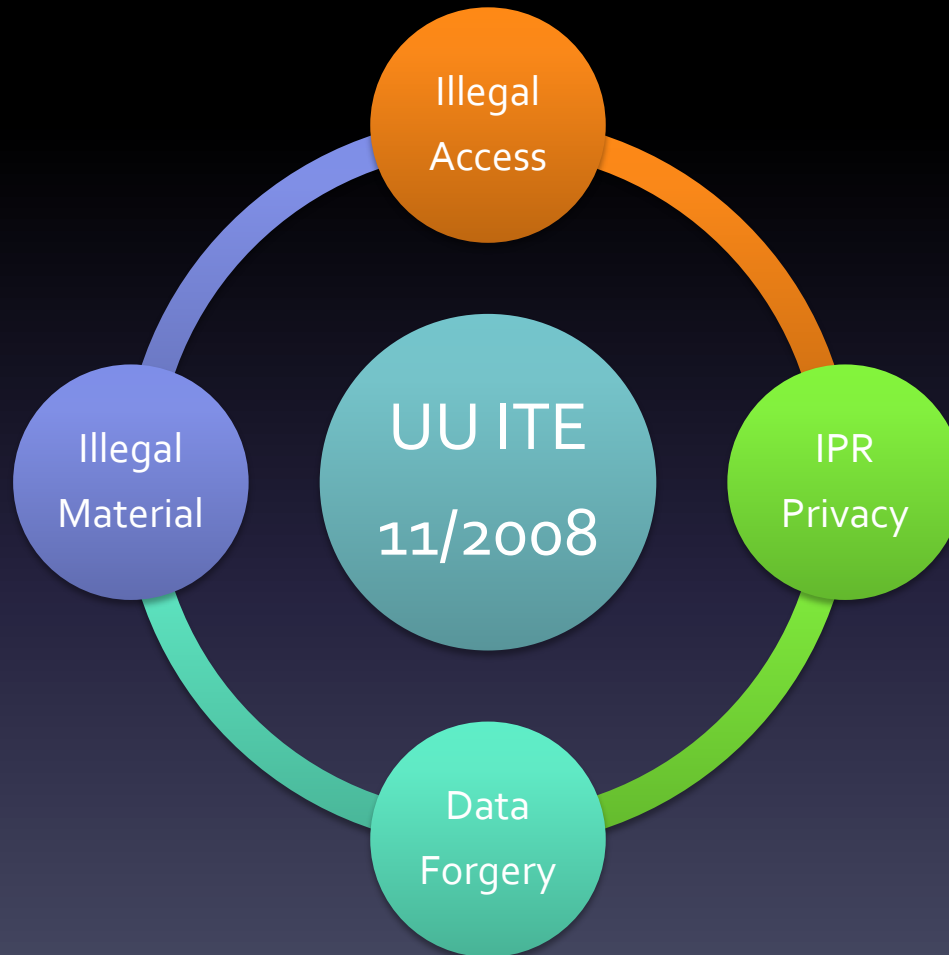
STRENGTHEN



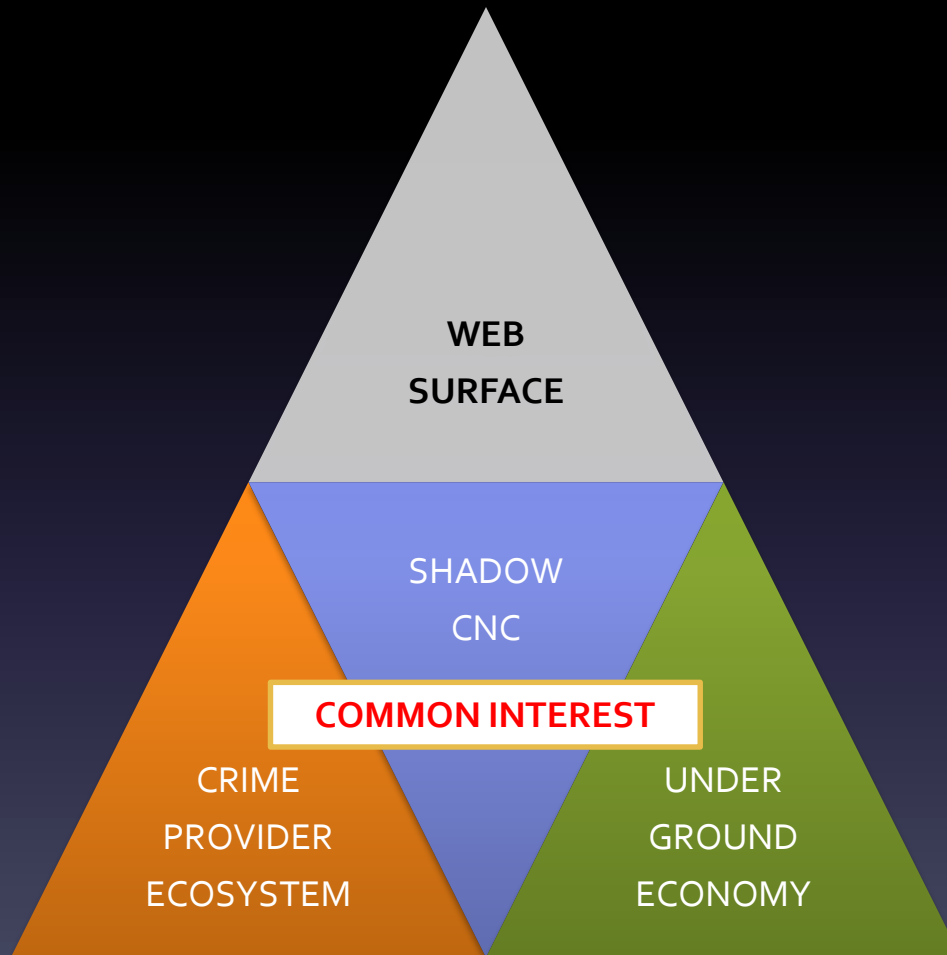
THREAT DETECTION



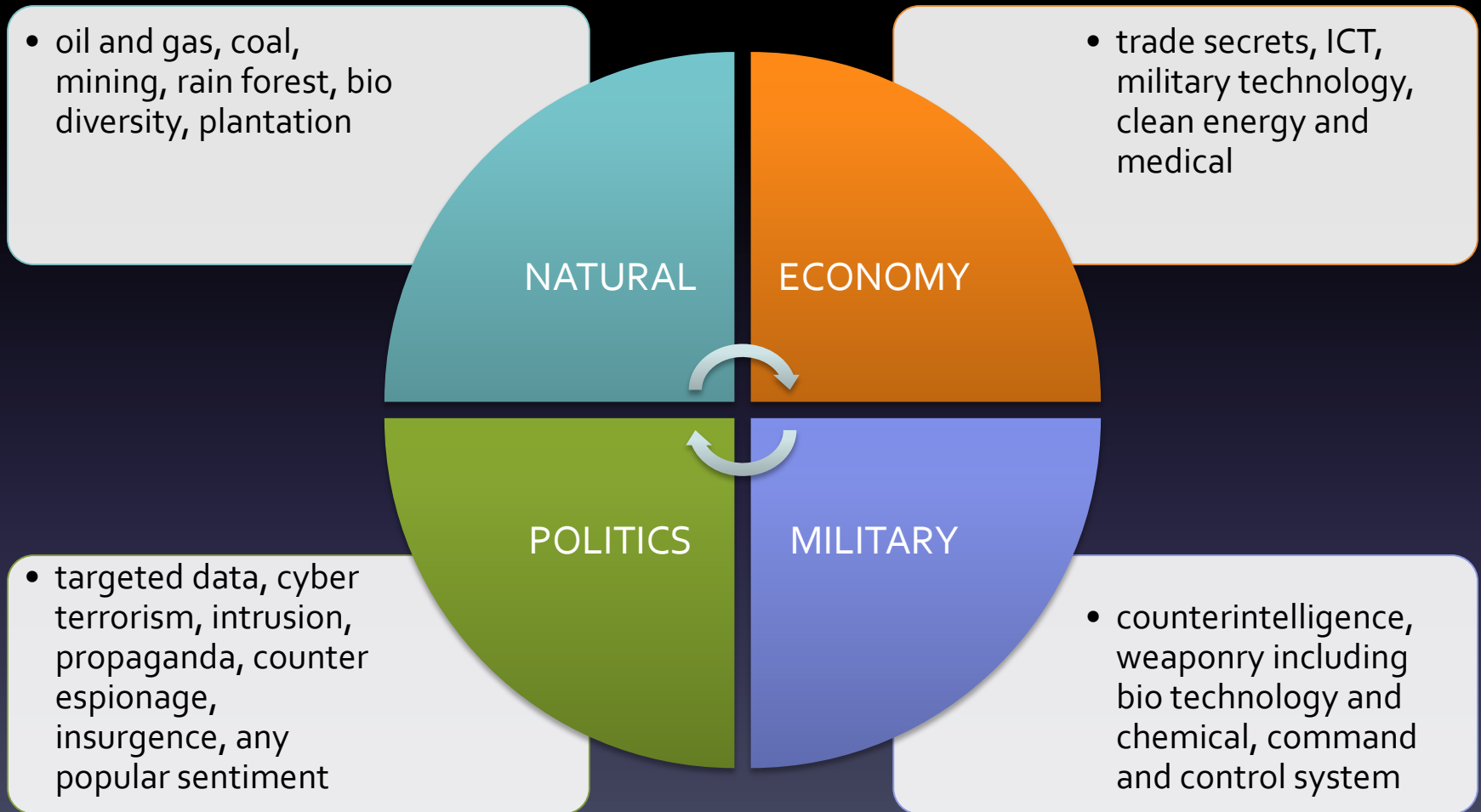
CYBER CRIME



DEEP WEB



CYBER ESPIONAGE



CYBER WAR

- An attack with politically motivated and or nation-state sponsored with intelligence style operation or an insurgence involving and or targeting computer system, networks, especially IP based (internet) to infiltrate, disrupt and or causing damage and or to sabotage/neutralize existing services including its content, this is definition of cyber warfare.

ASYMMETRIC

- ICT offenses to prevail/take over, dominate, control targeted resources to gain supremacy, build propaganda (public opinion, intl. perception)
- Political issues causing uncontrolled widespread cyber warfare involving many group of interest that could be very difficult to identify who they really are and how to detect their presence

ASYMMETRIC

- Not an open direct attack. Silent, anonymous, random, distributed, undercover, untraceable and continuous using widespread any unrelated resources, internetworked, cross borders and beyond any jurisdictions
- Nobody's know the real enemy and who is attacking who. Using complex strategy involving many different parties, amateur, professionals, military and civilians, organization

OFFENSIVE CAPABILITY

- Series of capabilities to launch massive tabletop targeted counter attack
- Set of scenario to exercise cyber deterrence and prepare battlefield
- Faster is better. Cyber war moves faster than any other type of warfare
- Focus on escalatory control, crisis instability and to collateral damage
- Civilians high impact preparation, it could harm power/financial systems
- Attribution, extremely difficult to track down who is really the cause of the attack. Unsuspecting countries and or parties can be used as a launching point for other countries attacks and they can easily and accidentally involved into the war strong offense/defense needed

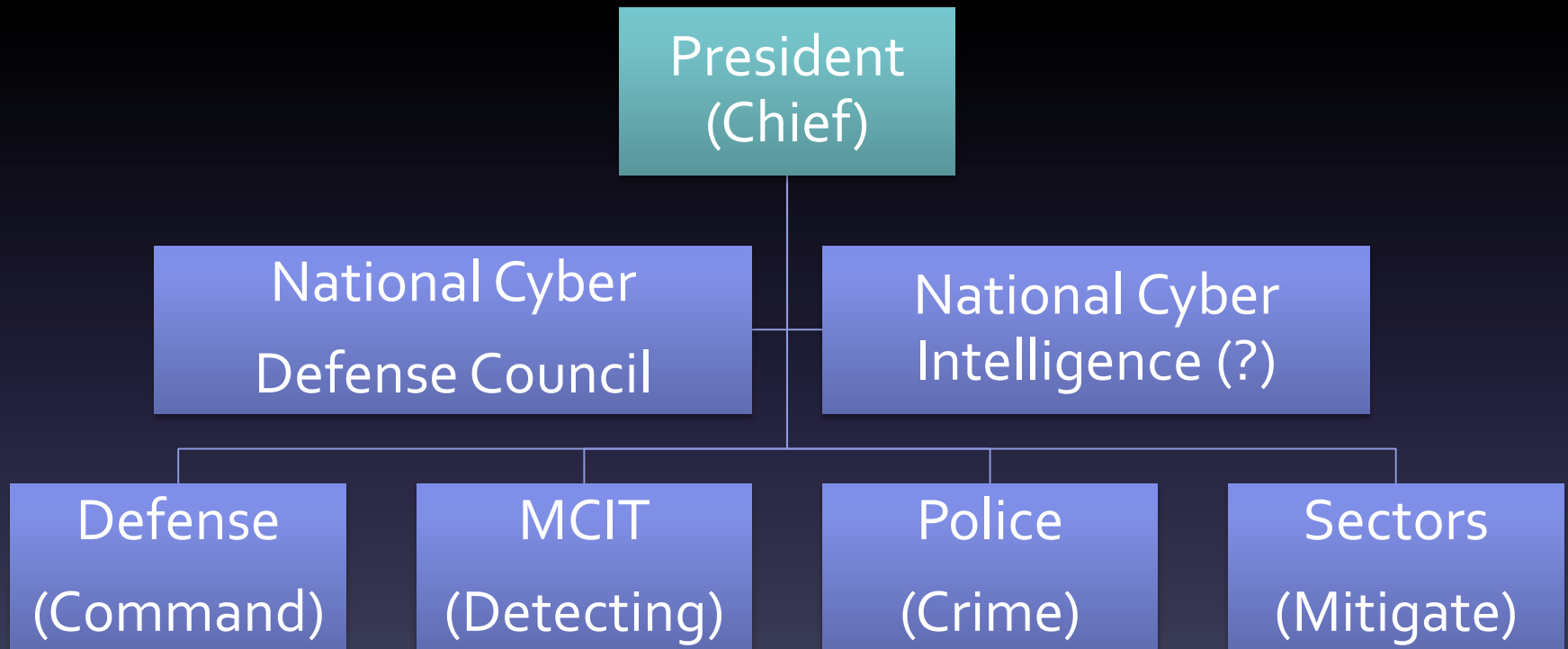
STRATEGIC SOLUTIONS

- Using any common technology and application – easy to use not easy to break, practical and it is cheap but reliable
- Rely on human resource: discipline, procedures and logic
- Instantly leverage the lack of secure private infrastructure and it's adequate quality of services with affordable cost
- Expanding collaboration with any other related potential local trusted agency, expert, academia, community etc.
- Focus on cyber priority target, capacity building, monitor and surveillance to detect/prevent possible threat/attack
- New structure needed: national cyber intelligence service

NATIONAL INITIATIVES



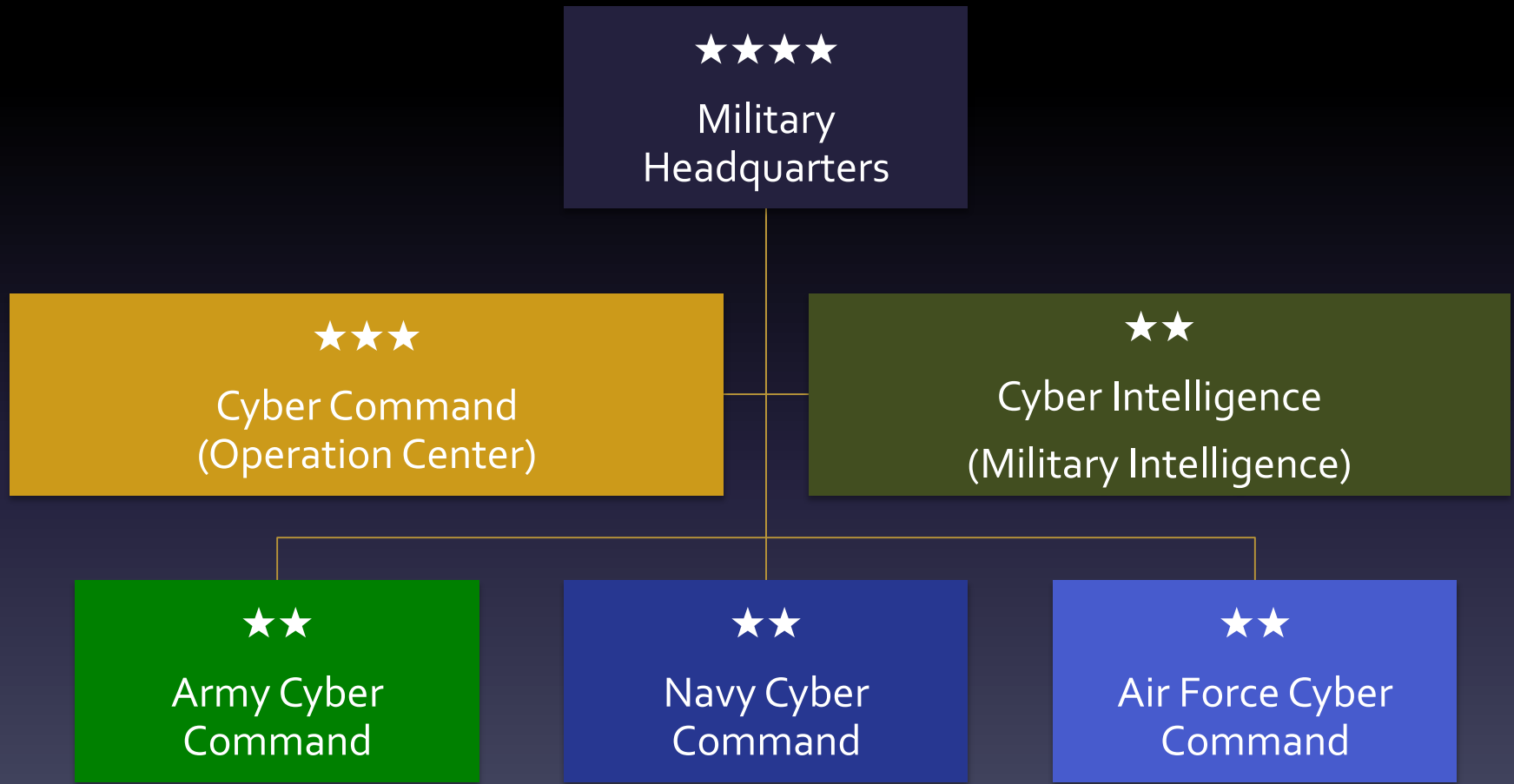
CYBER SECURITY COUNCIL



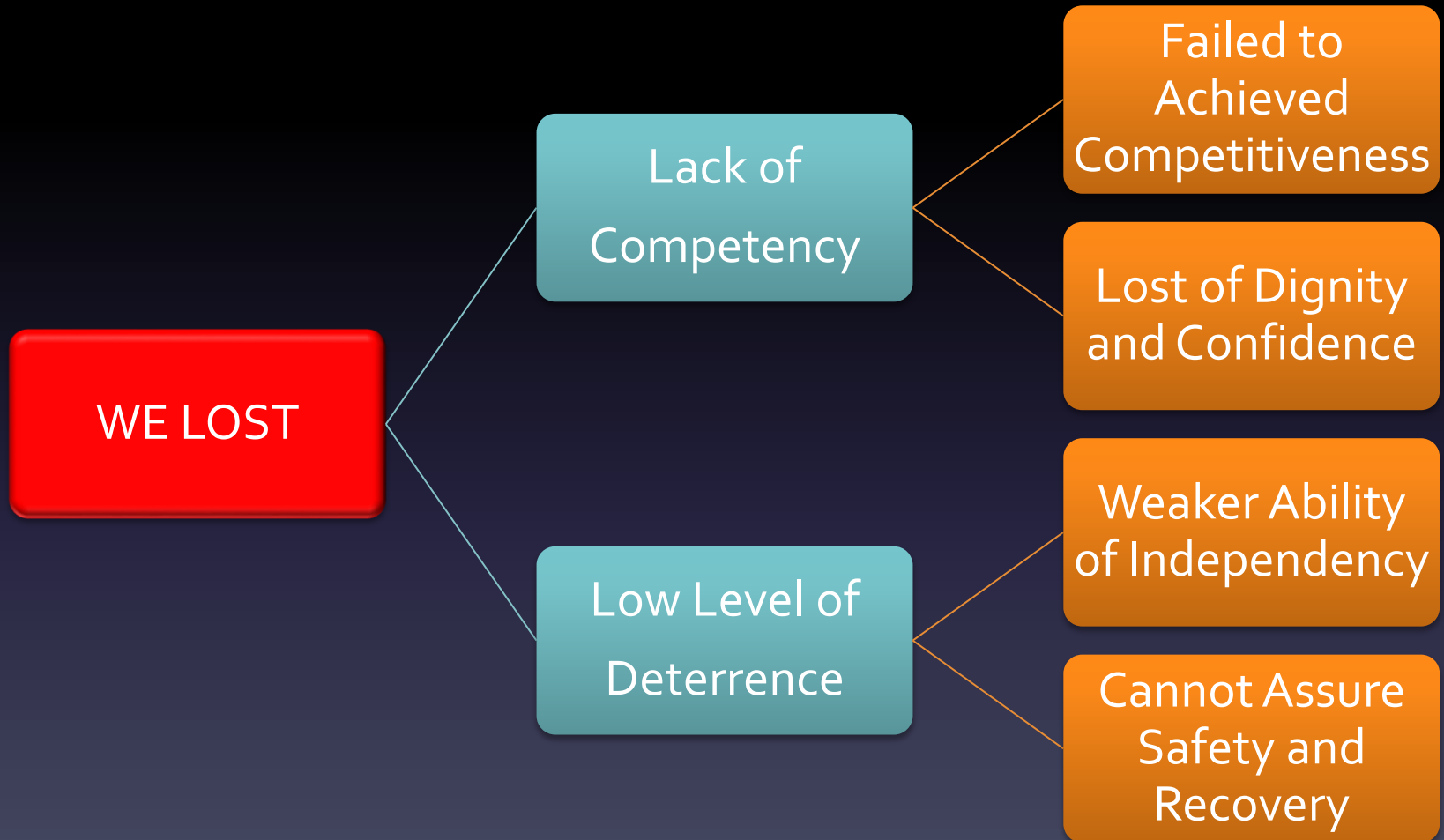
CYBER DEFENSE AGENCY



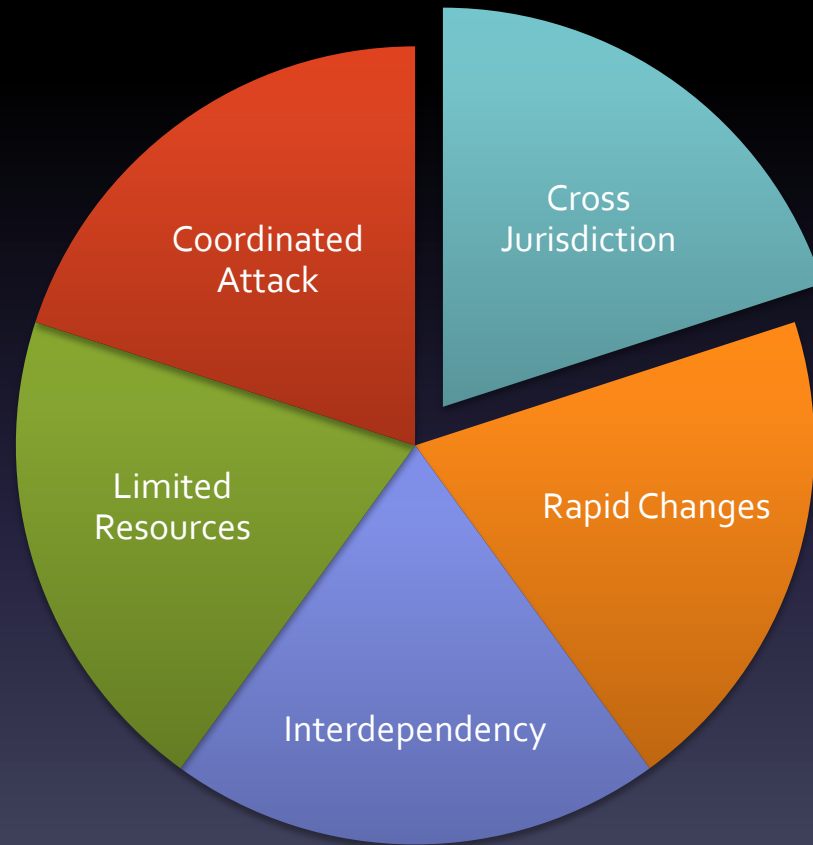
CYBER COMMAND



NO INFRASTRUCTURE



COOPERATION



ASIA PACIFIC OVERVIEW

- Every year, China recruit more than +3000 IT post graduate students, security professionals and voluntary hackers. Now estimated +100000 official Cyber Army are in services
- China and Russia has the largest underground economy i.e. “The Russian Company” and most powerful Ghost Net
- Vietnam has established 1000 Cyber Army in the year 2011
- Malaysia has prepared scenarios (drill) and resources for the “Cyber Storm” since 2005. The Cyber Security Malaysia has +300 expert in many areas: cryptography, digital forensic etc.

FOCUS: CAPABILITY

- Singapore has the largest multiple fiber optic backbone that is connecting Asia Pacific rim and Australia to Europe, known as the most concentrated exchange networks + data centers that host most regional strategic content and retain its traffic. Which means they have the most **cyber espionage capability** in the region and Indonesia is the most dependent with 90% of traffic flows
- Japan has more +500 secure and solid infrastructure of global scale data centers with DRC that are proven by numerous catastrophic event including natural and nuclear disaster. Which means they have the **most sophisticated cyber resilience** in the region

FOCUS: DETERRENT

- Korea has the highest cyber content density, best broadband services and top of the world cyber penetration. Which means they have the most **cyber deterrence** in the region
- China has the largest independent network with incomparable internet users and business scale. Which means **nobody could control** China. They have the **most significant cyber enforcement** with any kind of measures (power) including cyber military
- Russia has the largest underground network, cyber crime providers, black market, mercenaries. Which means **they have unlimited resources** to promote **any kind of cyber chaos**

FOCUS: POWER GAME

- Ideology is no longer perceived as major threat, the main reason now is to make **more money**, winning **competition**, to **dominate** others and control as much as cyber resources available on the net
- China and Russia has the most leading, sophisticated, very well organized attack activity aimed for information espionage, piracy, fraud, business data information leakage, identity theft, around the globe – mostly targeting US ICT resources (technology etc.) and hosting the largest underground economy: billions \$/year

CONCLUSION

- Global cyber subjection will be determined with the power of knowledge, new invention of technology or innovation, cyber resources domination and common interest: **money**

THANK YOU

- Ravindo Tower 17th Floor
- KEBON SIRIH RAYA 75
- Central Jakarta, 10340
- Phone +62 21 3192 5551 ; Fax +62 21 3193 5556
- Web: www.idsirtii.or.id ; Email: info@idsirtii.or.id