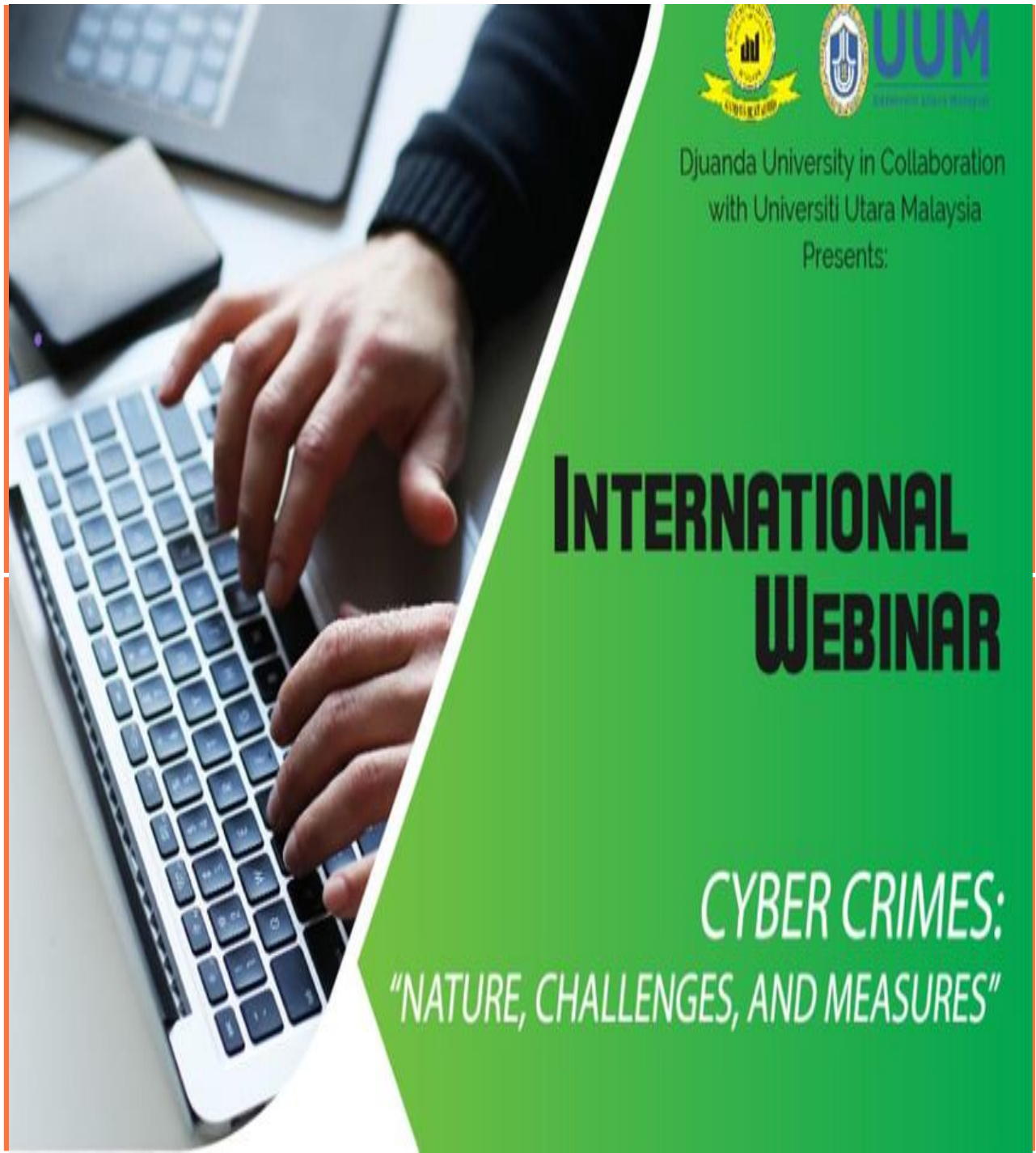
CURRENT CONDITION OF CYBER-CRIME IN INDONESIA

Dr. Bambang Widjojanto
Djuanda University

TUESDAY, OCTOBER 26TH 2021
08.30am (GMT+7)



LIFE AND CYBERSPACE

- The Daily Life & Cyber Space like two sides of the coin;
- In each activities → interact with network technology as much more than a computational device.
- Networks → penetrate the spaces of life at a fundamental level.
- The daily life and businesses: depend on electronic data and computer networks to conduct their daily operations;

(communication, education, working, shopping, eating, banking, date, check the weather, and public discourse, seminars).

https://www.europeanfiles.eu/industry/cybersecurity-four-steps-in-the-cyber-space

THE ADVANTAGE CYBERSPACE

a. **CONNECTIVITY, COMMUNICATION & SHARING**

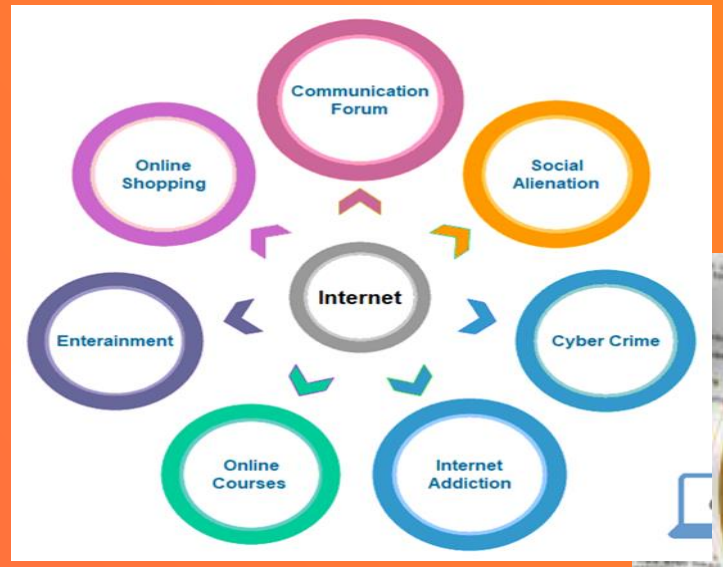
b. **INFORMATION, KNOWLEDGE, & LEARNING**

- **informational resources →**
  it is a virtual life library of information.
- **social networking also plays a major role in cyberspace**

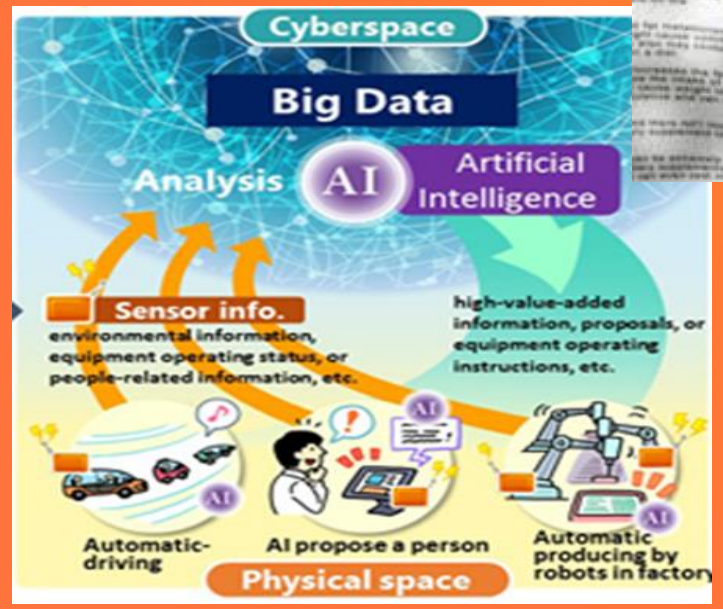
c. **E-COMMERCE→**
Selling And Making Money; Banking, Bills, And Shopping

d. **WORKCOLLACT →**
Work from home, collaboration, and access to a global workforce;

e. **ENTERTAINMENT →**
The Internet & CS provides people to access endless entertainment



https://atozupload.com/advantages-and-disadvantages-of-internet-technology/



https://www8.cao.go.jp/cstp/english/society5_0/index.html

elearning brothers

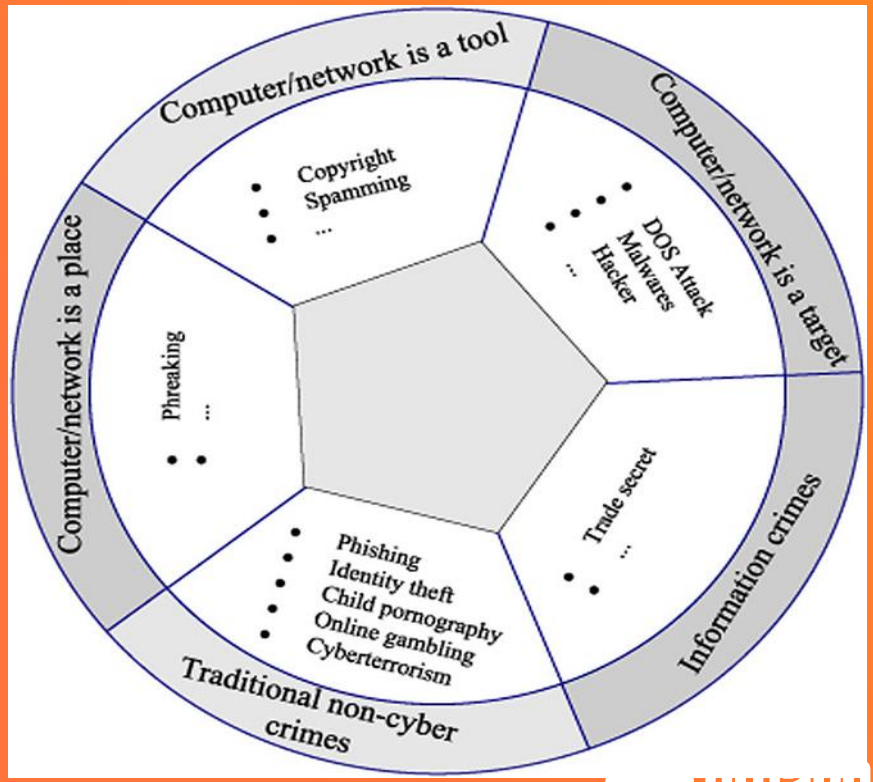
CYBER-CRIME & ATTACKS

As the Internet, computers & cyber space has become central to daily life & almost every aspect of human existence→ CYBER-CRIME ATTACKS have grown more frequent and destructive

The Threat → CYBER-CRIME ATTACKS:

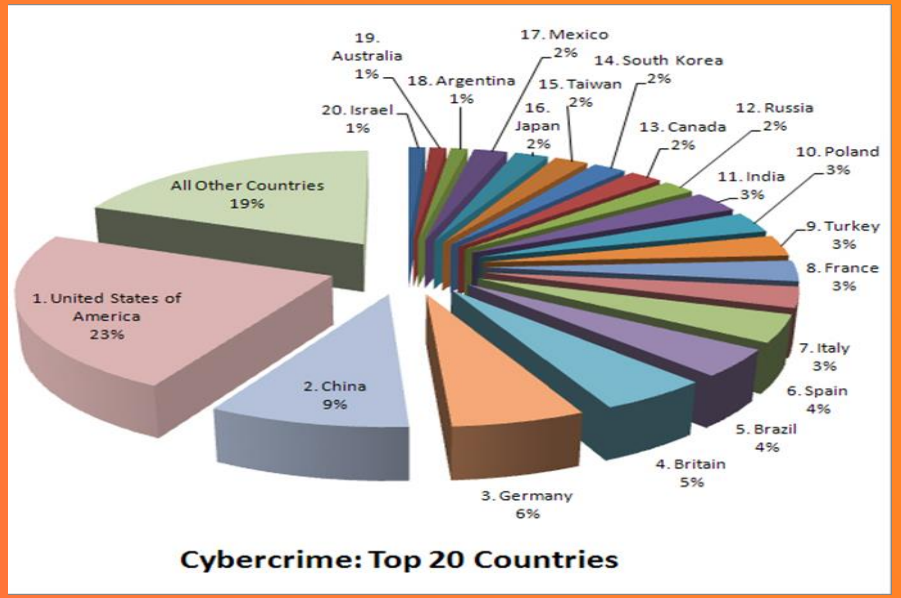
- Threaten individuals and critical infrastructure with increasing frequency and sophistication.
- The threaten → have serious effects on N&I security, democratic processes, the national & global economy, the free flow of ideas and information, and the safety, security and privacy of individuals.

https://www.digitalnewsasia.com/digital-economy/kaspersky-invites-msian-students-to-participate-in-cybercrime-research-competition

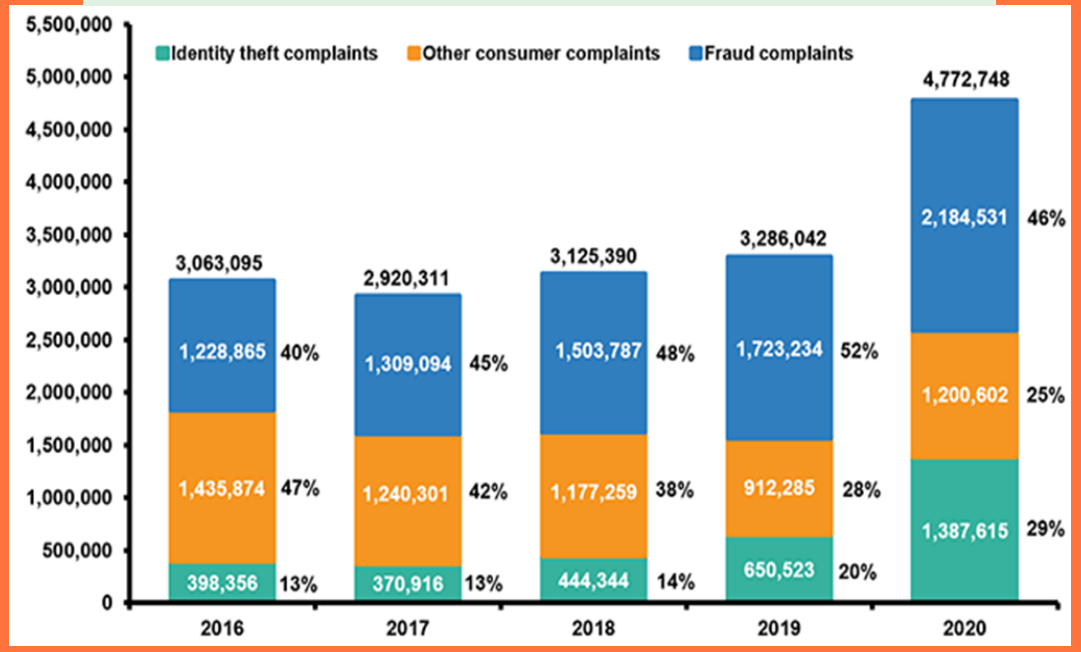


Categorization Of Cyber Crime
Survey Of Cyber Crimes: Yanping Zhang1, Yang Xiao1*, Kaveh Ghaboosi2, Jingyuan Zhang1and Hongmei Deng
Security Comm. Networks 2012; 5:422–437

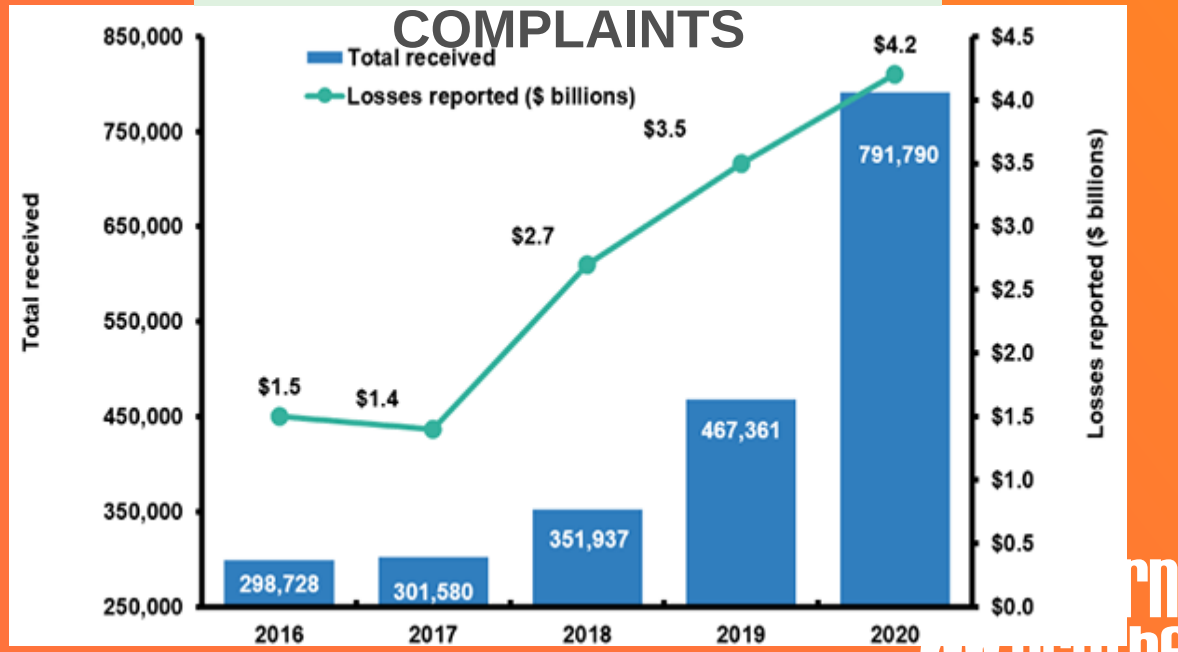
- Almost all countries in the world have problems with cybercrime;
- Not only developed countries are getting cybercrime attacks
- Complaints against cybercrime attacks have a tendency to increase



IDENTITY THEFT AND FRAUD REPORTS



CYBERCRIME COMPLAINTS



https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

- The Cybercrime — which is predicted to inflict damages totaling $6 trillion USD globally in 2021
- The costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025;
- This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

(Cybercrime To Cost The World, Special Report: Cyberwarfare In The C-Suite.
– Steve Morgan, Editor-in-Chief; Sausalito, Calif. – Nov. 13, 2020)

INDONESIA EXPERIENCES: E-COMMERSE & IT CRIMES

1. The Information & Transaction Law (ITE) Law No. 11/2008 was promulgated in 2008 and revised into Law No. 19/2016;
2. The formulation process has been carried out since 2003 and submitted to the parliament in 2005;
3. All of these are based on responding to technological developments that invade people's lives in Indonesia and the world;
4. The galis to ensure that electronic or e-commerce transactions run well and consumer rights are protected
5. In 2005, The Government established the Ministry of Communication and Information Department;

1. 2017 → Indonesian Government developed “State Cyber and Signal Agency“ (BSSN).
2. One of BSSN duties is to carry out cyber security to maintain the sovereignty of Indonesia's IT infrastructure.

1. The ITE Law regulates e-commerce issues and information technology crimes.
2. Important things that are regulated in information technology crimes, namely:
   a. Illegal content, such as: SARA information, hate speech, false/hoax information, online fraud, pornography cases, online gambling, and defamation;
   b. hacking, illegal interception such as wiretapping and data interference such as interference or illegal system destruction.
3. Since then, electronic information or documents have become valid legal evidence

CONTINUE .....

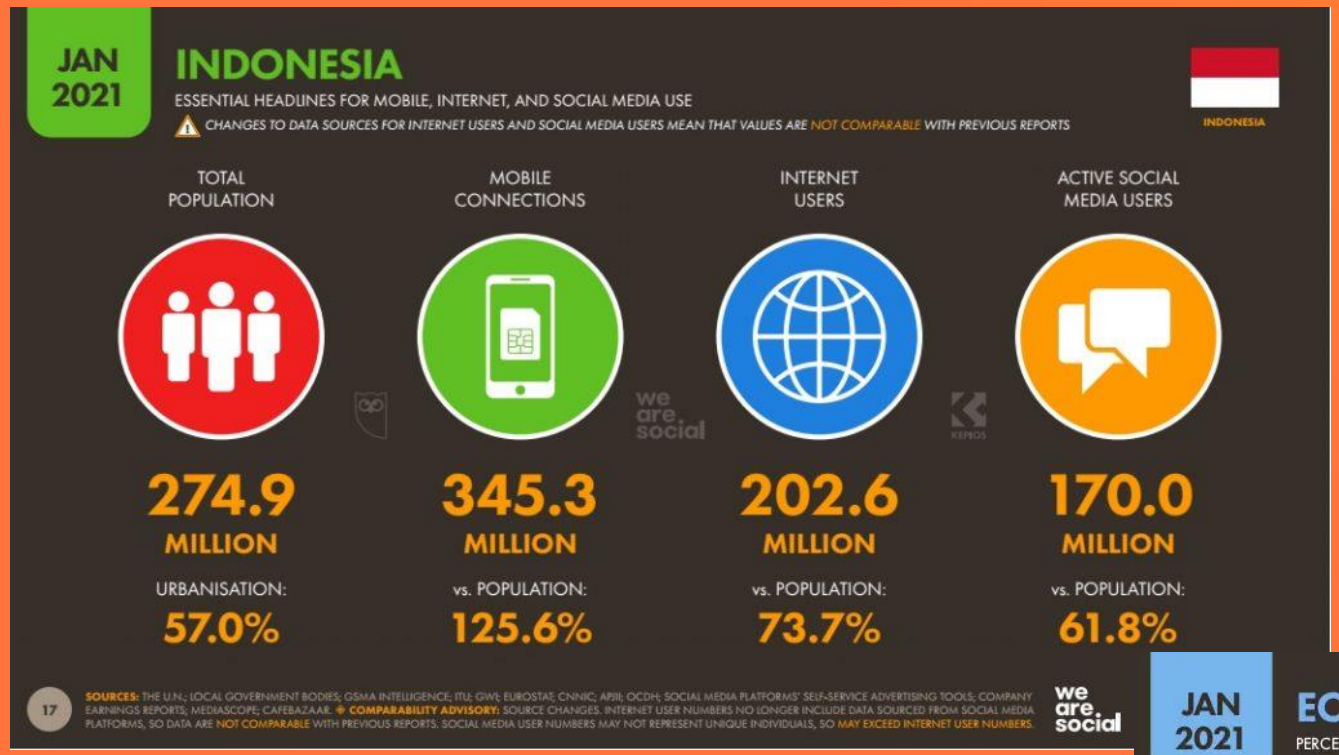
CYBERCRIME, CYBER ATTACK, AND CYBER WARFARE are three illegal activities in cyberspace that have different legal consequences

1. "**CYBER ATTACK** is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"
2. The purpose of the attack is to damage and/or destroy the cyber system which includes computer networks and the internet.

CYBER WARFARE →

The object that is attacked in cyber warfare is a cyber system that is directly related to the activities of the government within cyberspace

1. **CYBER CRIME →** Illegal Acts Of Criminals using computer network information system technology (IST) that directly attacks the victim's IST
2. The Cyber Crime Is A Crime, namely:
   - Conventional Crimes developed from real space (fraud, theft, pornography, defamation); and
   - New Crimes that can only be committed in cyberspace (cyber espionage, cyber sabotage and extortion, cracking)
3. Cyber Crime is increasingly being carried out during the Covid-19 pandemic;
4. There are 5 (five) highest cases, namely: provocative cases, hate content and hate speech, online fraud and pornographic content;



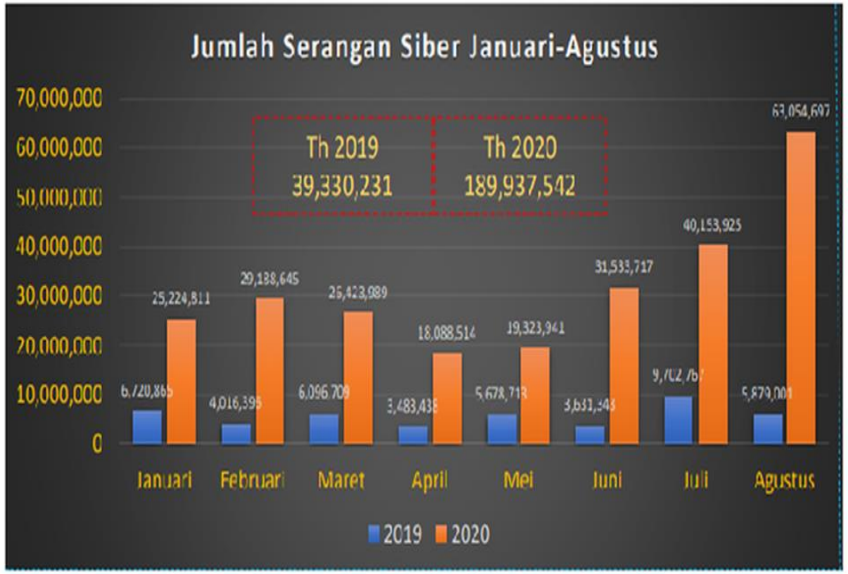
ISSUES & CHALLENGES

1. Indonesia Need to Anticipating the Cyber Attack
2. The Increase of Digitalization has Increased the Number of Cyberattacks

3. Indonesian cybersecurity laws and regulations created fragmented responsibilities across different ministries and they remain ineffective in preventing cyberthreats and cybercrime. A comprehensive regulation on cybersecurity is urgently needed in Indonesia.

4. Indonesia should be developed Infrastructure of Syber Security to minimizing potential impact from Cyberattacks

1. The National Cyber and Crypto Agency (BSSN) reported 290 million cases of cyberattacks in 2019;
2. This amount is 25% more than the previous year & caused a loss of US$ 34.2 billion in Indonesia (https://id.cips-indonesia.org/post/ ringkasan-kebijakan-perlindungan-keamanan-siber-di-Indonesia
3. "BSSN detected more than 495 million cyberattacks last year. This number has doubled compared to 2019" (https://portalsulut.pikiran-rakyat.com/nasional/pr-852024125/kejahatan-siber-di-indonesia-terus-naik-bssn-tahun-2020-terjadi-495-juta-cyber-attack
4. Head of the National Cyber and Crypto Agency (BSSN) Hinsa Siburian said that during 2021 there were 888,711,736 cyber attacks recorded. (https://nasional.kompas.com/read/2021/09/ 14/ 10493771/bssn-hingga-agustus-2021-tercatat-888-juta-serangan-siber.



CONTINUE ISSUES & CHALLENGES ….

INCIDENT OF PERSONAL DATA LEAKAGE IN INDONESIA

PERSONAL DATA OF ELECTRONIC HEALTH ALERT CARD (eHAC) users.September 2021, there are 1.3 million eHAC user data was first discovered on a server that can be accessed by everyone. First discovered by vpnmentor researchers and reported from vpnmentor.com. As for some of the data that was leaked, including names, home addresses, ID numbers, hospitals where Covid-19 tests were carried out.

DATA LEAK OF HEALTH INSURANCE MANAGEMENT AGENCY. May 2021, Social Security Administering Body (BPJS) Participant data was sold on Raid Forums for 0.15 Bitcoin. Data sold by 'Kotz'. The total number is 279 million.

SALES OF BRI LIFE CUSTOMER DATA

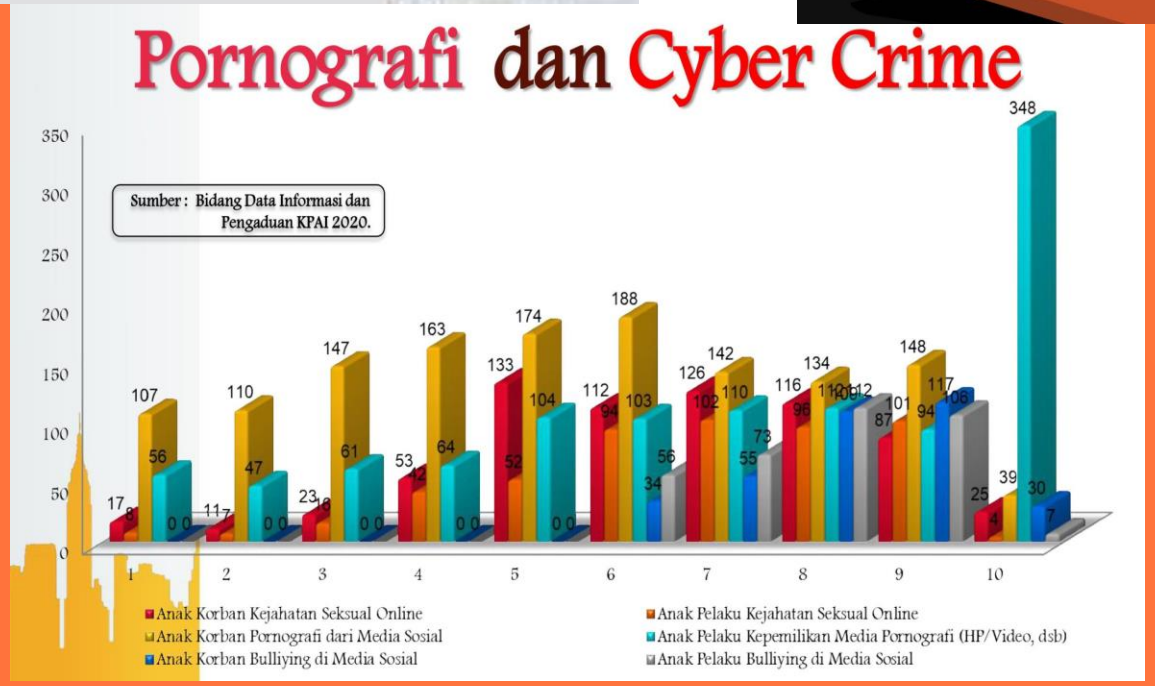
In July 2021, there is data that two million BRI Life customers were sold at a price of $7,000 or around Rp. 101.6 million. Bereda via Twitter account @HRock. The documents listed in the screenshot are photos of electronic ID cards, account numbers, taxpayer numbers, birth certificates, and medical records of BRI Life customers.

CERMATI AND LAZADA DATA LEAKS

December 2020, Customer data from 2 (two) Cemarti and Lazada companies circulated on the Raidforums website. The data traded from meticulous.com as many as 2.9 million customers were taken from the activities of 17 companies in the financial sector. Lazada data leak of 1.1 million data.

TOKOPEDIA DATA LEAK

In May 2020, millions of Tokopedia e-commerce user accounts were suspected to have been leaked. The owner of the Twitter account @underthebreach said the hacker actor had sold the Tokopedia database of 91 million accounts for US$ 5,000 on the darkweb.



LAWS, MEASURES, ACHIEVEMENT & POTENTIALS

1. Indonesia lags behind in terms of ICT security policy and regulations.
2. Malaysia, for instance, already has a Computer Crime Act, Digital Signature Act, Telemedicine Act (three of them have been enacted since 1997), Multimedia Act (1998), Payment System Act (2003) and a Personal Data Act (2010).
3. Singapore has a set of similar regulations but Indonesia's lack of policies;
4. Indonesia need **THE CYBER SECURITY AND RESILIENCE BILL & PERSONAL DATA PROTECTION BILL.**
5. The Law of The Republic of Indonesia Number 11 of 2008 concerning **ELECTRONIC INFORMATION AND TRANSACTION** (Articles 29-37), it has a limited scope.
6. Due to these limitations, criminal cases related to cyber crimes are being punished with Criminal Procedural Law Codex (UU KUHAP), Consumer Protection Law No. 8/1999, Copyright Law No. 19/2002 or the Anti-Pornography Law No. 44/2008

SUGGESTIONS & HOPE

1. Indonesia until now, have not had a cyber security policy that is lex. In fact, policies in many countries, shows that each country has particularly policy that is lex specialist in cyber security in accordance with the potential threat inherent (embededness)

2. The Cybersecurity and Cyber Resilience Bill was initiated by the Parlemen in May 2019; and was supposed to be finished by parlemen.
It would have made Indonesia the fourth ASEAN member with a cybersecurity law besides Singapore, Malaysia, and Thailand.

3. **CYBER CRIME** is a crime that crosses national boundaries.
Because crosses national borders and could involve many countries, therefore cyber crime including extraordinary crime it is important that multilateral cooperation agreement in order to overcome this problem, both at regional and international levels.

4. The threat of cyber criminality requires more effort to improve the security of the products we use, to strengthen our defenses against criminals and to promote cooperation among all stakeholders, within and across national borders

THANK YOU