



الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
يونسُ رَسِيْتِي: اِسْلَامُهُ اَنْبَارٌ اَجْسِبًا مِلْدَسِيًّا

Garden of Knowledge and Virtue

LEADING THE WAY

KHALĪFAH • AMĀNAH • IQRA' • RAḤMATAN LIL-ĀLAMĪN

OFFICIAL IIUM

DIGITAL ECONOMY AND THE PROBLEMS OF CYBER CRIMES: LEGAL LANDSCAPE AND CHALLENGES

FAKULTAS HUKUM
Garden of Knowledge and Virtue

INTERNATIONAL GUEST LECTURE
DIGITAL ECONOMY AND THE PROBLEMS OF CYBER CRIME

12 JUNE 2026 | 08:00 AM (WIB)
Online via Zoom Cloud Meeting

BENEFITS FOR PARTICIPANTS:

- ✓ Gain new insights on Digital Economy & Cyber Crime Law
- ✓ E-Certificate for all active participants
- ✓ Enrich your academic and professional knowledge from an international expert

Assoc. Prof. Dr. Sonny Zulhuda
Associate Professor at Ahmad Ibrahim
Kulliyah of Laws (AIKOLU)
International Islamic University Malaysia (IIUM)

Scan QR Code to Register

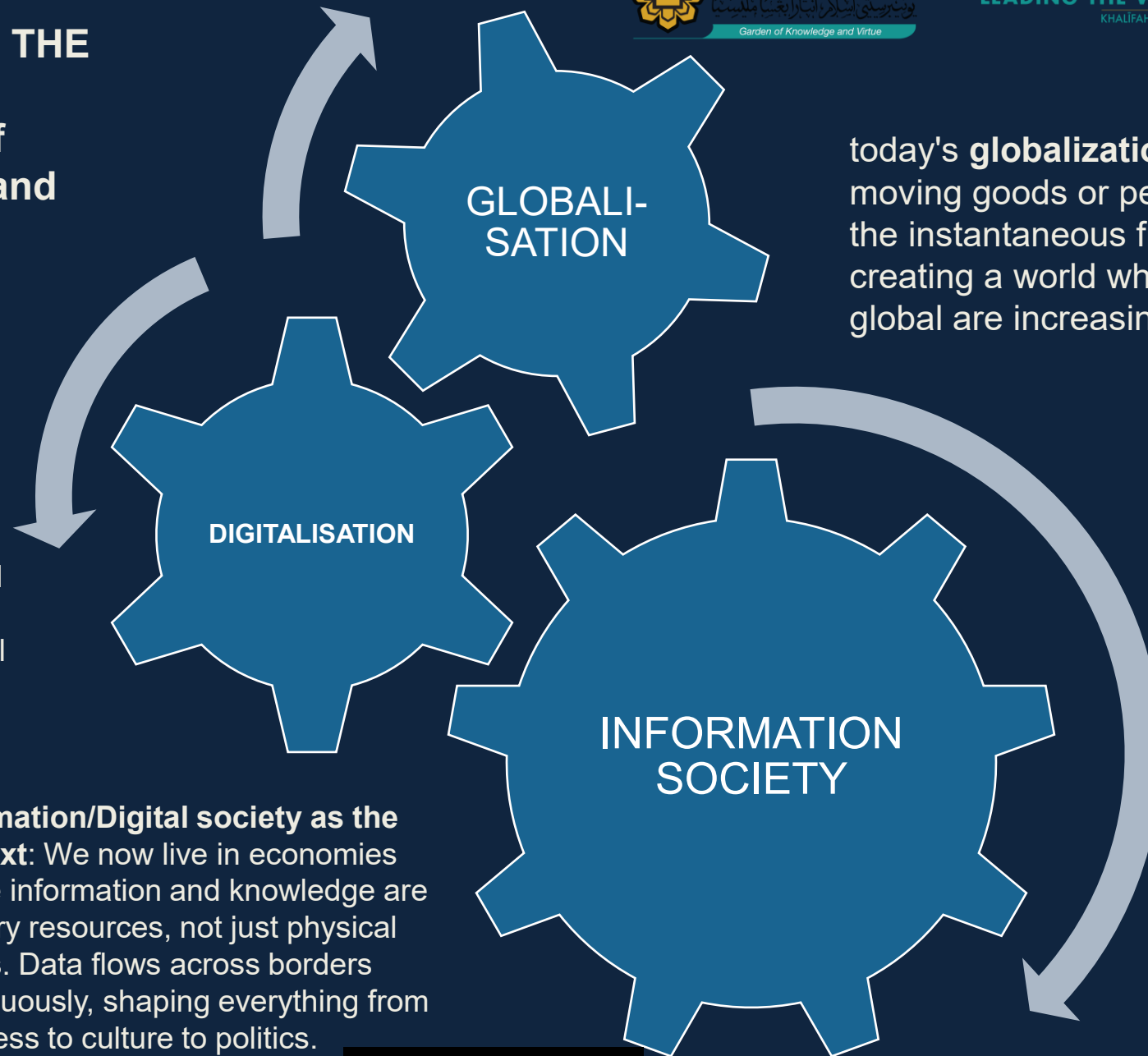
DR. SONNY ZULHUDA
International Islamic University Malaysia

INTERNATIONAL GUEST LECTURE
Faculty of Law, Universitas Bhayangkara, Surabaya
12 June 2026

3 KEY FACTORS INTO THE TOPIC – the interconnectedness of economies, cultures, and societies enabled and accelerated by digital technologies.

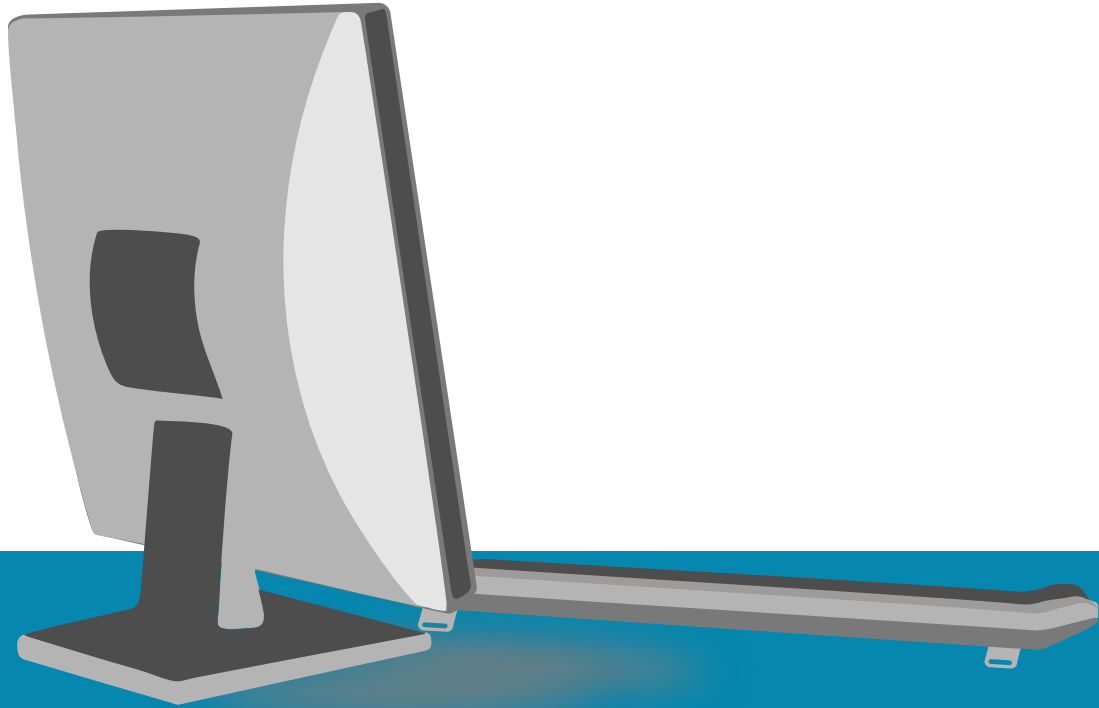
Digitalization as the enabler: Digital technologies (internet, mobile networks, cloud computing, AI) have eliminated traditional barriers of distance and time, making instant global communication and transactions possible.

Information/Digital society as the context: We now live in economies where information and knowledge are primary resources, not just physical goods. Data flows across borders continuously, shaping everything from business to culture to politics.



today's **globalization** isn't just about moving goods or people—it's about the instantaneous flow of information, creating a world where local and global are increasingly blurred.

STATISTICS OF DIGITAL INDONESIA





WHAT HAPPENS IN ONE MINUTE IN INTERNET*

2025

*<https://bondhighplus.com/blog/what-happens-in-an-internet-minute/>

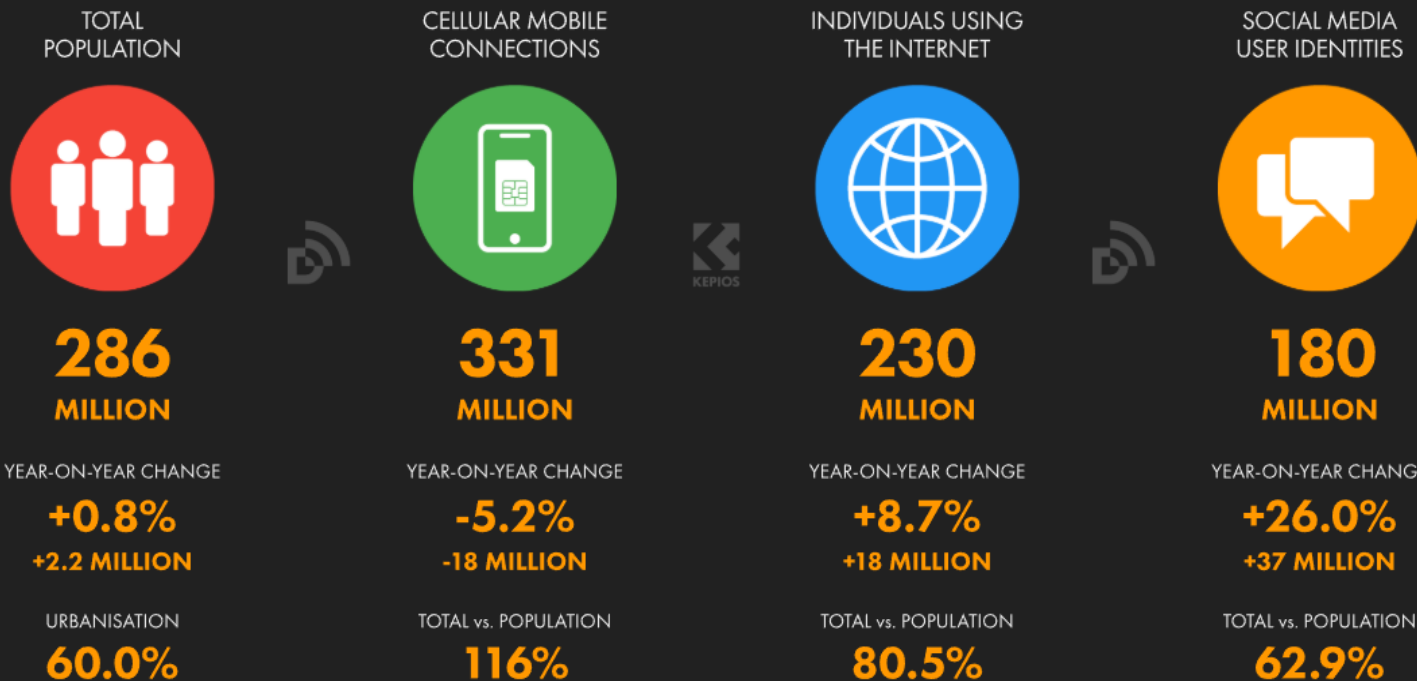
OCT 2025

INDONESIA



OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

NOTE: SIGNIFICANT REVISIONS TO SOURCE DATA MAY DISTORT VALUES FOR CHANGE OVER TIME. FIGURES SHOWN HERE ARE **NOT DIRECTLY COMPARABLE** WITH VALUES PUBLISHED IN PREVIOUS REPORTS.



14

SOURCES: UNITED NATIONS; GOVERNMENT AUTHORITIES; GSMA INTELLIGENCE; ITU; EUROSTAT; CNNIC; PLATFORM RESOURCES; OCDH; BETA RESEARCH CENTER; KEPIOS ANALYSIS **ADVISORY:** SOCIAL MEDIA USER IDENTITIES MAY **NOT** REPRESENT UNIQUE INDIVIDUALS **COMPARABILITY:** SOURCE CHANGES AND BASE REVISIONS. FIGURES ARE **NOT COMPARABLE** WITH PREVIOUS REPORTS. GLOBAL DATASETS MAY USE DIFFERENT SOURCES vs. LOCAL AND REGIONAL DATA, SO SUMS MAY NOT CORRELATE **IMPORTANT:** NEGATIVE VALUES MAY INDICATE SOURCE CORRECTIONS, AND **MAY NOT** REPRESENT DECREASES IN ACTUAL ADOPTION OR USE. WHERE YEAR-ON-YEAR CHANGE IS "[N/A]", COMPARISONS WITH HISTORICAL DATA WILL PRODUCE **INACCURATE RESULTS**. SEE [NOTES ON DATA](#).



OCT 2025

OVERVIEW OF INTERNET USE

ESSENTIAL INDICATORS OF INTERNET ADOPTION AND USE



INDONESIA

INDIVIDUALS USING THE INTERNET



230 MILLION



INDIVIDUALS USING THE INTERNET vs. POPULATION



80.5%



YEAR-ON-YEAR CHANGE IN TOTAL INTERNET USERS



+8.7% +18 MILLION



YEAR-ON-YEAR CHANGE IN INTERNET USERS vs. POPULATION



+7.8% +586 BPS

INDEXED SHARE OF GLOBAL INTERNET USERS vs. GLOBAL POPULATION SHARE



110.0



PERCENTAGE OF INTERNET USERS ACCESSING VIA MOBILE PHONES



98.0%

GWI.

PERCENTAGE OF INTERNET USERS ACCESSING VIA LAPTOPS OR DESKTOPS



51.2%

GWI.

AVERAGE WEEKLY TIME SPENT USING CONNECTED MEDIA



37H 20M

SOURCES: KEPIOS ANALYSIS, ITU, GSMA INTELLIGENCE, EUROSTAT, GOOGLE'S ADVERTISING RESOURCES, CNNIC, GOVERNMENT RESOURCES, UNITED NATIONS. TIME SPENT AND DEVICE SHARE DATA FROM GWI (Q2 2025). NOTES: PERCENTAGE CHANGE FIGURES SHOW RELATIVE YEAR-ON-YEAR CHANGE. "BPS" FIGURES REPRESENT BASIS POINTS, AND SHOW ABSOLUTE YEAR-ON-YEAR CHANGE. COMPARABILITY: SOURCE AND BASE CHANGES. ALL FIGURES USE THE LATEST AVAILABLE DATA, BUT SOME SOURCES DO NOT PUBLISH REGULAR UPDATES, SO FIGURES MAY UNDER-REPRESENT ACTUAL USE. SEE NOTES ON DATA.

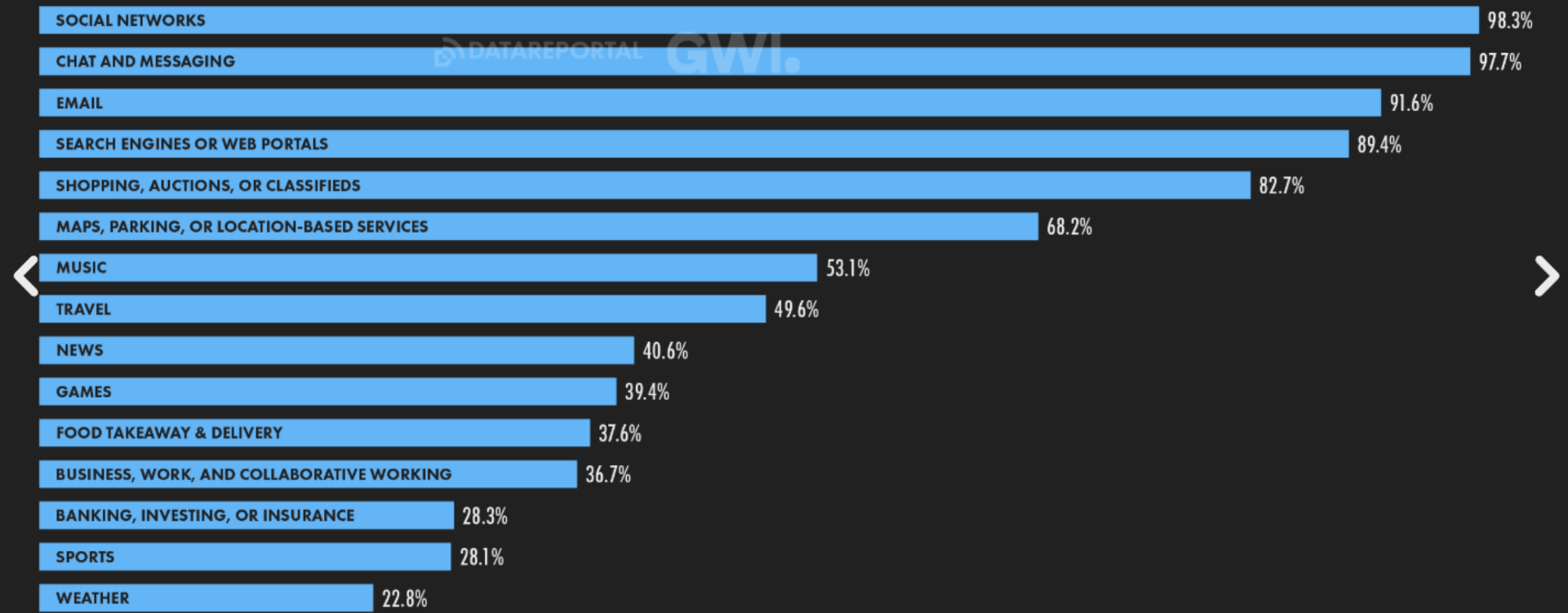
OCT 2025

TOP TYPES OF WEBSITES VISITED AND APPS USED

PERCENTAGE OF INTERNET USERS AGED 16+ WHO HAVE VISITED OR USED EACH KIND OF DIGITAL PROPERTY IN THE PAST MONTH



INDONESIA



47

SOURCE: GWI (Q2 2025) COMPARABILITY: CHANGES IN AUDIENCE COMPOSITION AND SURVEY METHODOLOGY. SEE [NOTES ON DATA](#).



**OCT
2025**

TOP WEBSITES: SIMILARWEB RANKING

SIMILARWEB'S RANKING OF THE MOST VISITED WEBSITES, BASED ON WEBSITE TRAFFIC BETWEEN 01 JUNE AND 31 AUGUST 2025



INDONESIA

#	WEBSITE	TOTAL VISITS (MONTHLY AVE.)	UNIQUE VISITORS (MONTHLY AVE.)	AVERAGE TIME PER VISIT	AVERAGE PAGES PER VISIT
01	GOOGLE.COM	2.31 B	148 M	8M 05S	8.56
02	YOUTUBE.COM	620 M	38.3 M	23M 34S	13.37
03	WHATSAPP.COM	243 M	24.1 M	12M 31S	3.95
04	CHATGPT.COM	213 M	17.6 M	10M 28S	5.84
05	INSTAGRAM.COM	150 M	23.1 M	8M 20S	13.43
06	DETIK.COM	144 M	30.4 M	1M 45S	2.56
07	X.COM	140 M	10.9 M	15M 14S	18.88
08	SHOPEE.CO.ID	119 M	30.6 M	8M 13S	8.28
09	TIKTOK.COM	108 M	37.0 M	4M 01S	7.56
10	FACEBOOK.COM	107 M	12.4 M	9M 31S	11.68

#	WEBSITE	TOTAL VISITS (MONTHLY AVE.)	UNIQUE VISITORS (MONTHLY AVE.)	AVERAGE TIME PER VISIT	AVERAGE PAGES PER VISIT
11	SSSTIK.IO	72.1 M	16.6 M	2M 55S	3.09
12	VIDEY.CO	71.3 M	15.6 M	10M 39S	28.29
13	CANVA.COM	66.9 M	17.4 M	4M 54S	5.57
14	KOMPAS.COM	58.8 M	15.2 M	4M 16S	2.37
15	GOOGLE.CO.ID	57.4 M	20.0 M	3M 02S	5.49
16	TRIBUNNEWS.COM	56.3 M	13.0 M	4M 05S	3.08
17	TOKOPEDIA.COM	56.2 M	14.5 M	6M 52S	8.59
18	LINKLIST.BIO	53.2 M	8.16 M	2M 29S	2.49
19	CROXYPROXY.COM	49.3 M	9.50 M	1M 08S	4.22
20	XNXX.COM	46.0 M	9.94 M	7M 53S	12.58

48

SOURCE: SIMILARWEB. RANKING AND VALUES BASED ON TRAFFIC BETWEEN 01 JUNE AND 31 AUGUST 2025. **NOTES:** VALUES IN THE "UNIQUE VISITORS" COLUMN REPRESENT THE NUMBER OF DISTINCT "IDENTITIES" ACCESSING EACH SITE, BUT MAY NOT REPRESENT UNIQUE INDIVIDUALS, AS SOME PEOPLE MAY USE MULTIPLE DEVICES OR BROWSERS. VALUES FOR "TOTAL VISITS" AND "UNIQUE VISITORS" REPRESENT MONTHLY AVERAGES. FIGURES ENDING IN "B" ARE IN BILLIONS; FIGURES ENDING IN "M" ARE IN MILLIONS; FIGURES ENDING IN "K" ARE IN THOUSANDS. TIME SHOWN IN MINUTES AND SECONDS. **ADVISORY:** SOME SITES FEATURED IN THIS RANKING MAY CONTAIN ADULT CONTENT, VIRUSES, MALWARE, OR OFFENSIVE CONTENT. READERS SHOULD **AVOID VISITING UNKNOWN DOMAINS.**

**OCT
2025**

ECOMMERCE: CONSUMER GOODS CATEGORIES

ESTIMATED ANNUAL SPEND IN EACH CONSUMER GOODS ECOMMERCE CATEGORY (B2C ONLY, U.S. DOLLARS, FULL-YEAR 2025)



INDONESIA



60

SOURCE: STATISTA MARKET INSIGHTS. **NOTES:** WHERE LETTERS ARE SHOWN NEXT TO FIGURES, "K" DENOTES THOUSANDS (E.G. "123 K" = 123,000), "M" DENOTES MILLIONS (E.G. "1.23 M" = 1,230,000), AND "B" DENOTES BILLIONS (E.G. "1.23 B" = 1,230,000,000). WHERE NO LETTER IS PRESENT, VALUES ARE SHOWN AS IS. FIGURES REPRESENT ESTIMATES AND PROJECTIONS OF FULL-YEAR REVENUES FOR 2025 IN U.S. DOLLARS. THE "PHYSICAL MEDIA" CATEGORY DOES NOT INCLUDE DIGITAL DOWNLOADS OR STREAMING. **COMPARABILITY:** SIGNIFICANT BASE REVISIONS AND MAJOR CATEGORY DEFINITION CHANGES. FIGURES ARE **NOT COMPARABLE** WITH PREVIOUS REPORTS.



OCT 2025

PAYMENT METHODS USED FOR ECOMMERCE

SHARE OF 2024 B2C ECOMMERCE TRANSACTION VALUE ATTRIBUTABLE TO EACH TYPE OF PAYMENT METHOD



INDONESIA

MOBILE AND DIGITAL WALLETS



42%

DEBIT AND CREDIT CARDS



12%

ACCOUNT-TO-ACCOUNT TRANSFERS (A2A)



32%

"BUY NOW, PAY LATER" SERVICES



3%

OTHER PAYMENT METHODS



11%

Digitalisation and Data Centrality

Malaysia: 8th

Malaysia is ranked eight with the highest penetration of social media (83%)

Indonesia: Top 4

Indonesians among the highest social media audience:

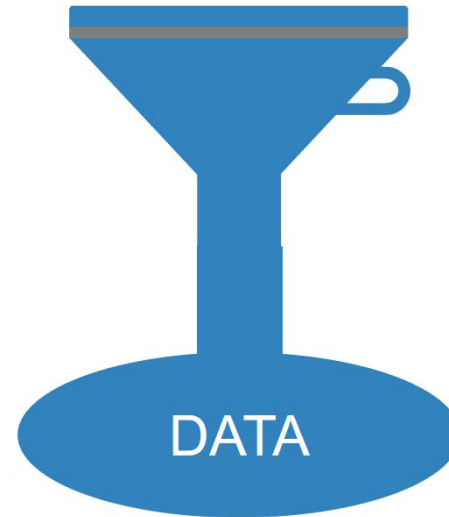
2nd on Tiktok (after the US)

3rd on FB (after India and the US)

4th on Youtube, Instagram, Twitter and WhatsApp



```
101001101001000010101
0011110111011011011010
101000011100101011001
010100111010100010101
0001011010110110110100
010101110001010100010
1000101110101100010011
010011010010000101010
0111101110110110110101
010000111001010110010
101001110101000101010
0010110101101101101001
```



Transformation to the Digital Society

1. Increasing Use of the Digital Technology:

- Data processing: Computers, wearables
- Data storage: Cloud, Blockchain
- Connectivity: Internet, mobile, wireless, Metaverse, etc.
- Analytic: Machine learning, AI, etc.
- Media: Web 2.0, Social media, etc.
- Transaction: E-money, cryptocurrency, e-wallet, etc.

2. Phases of digital transformation:

Digitalisation → Datafication → Automatisations

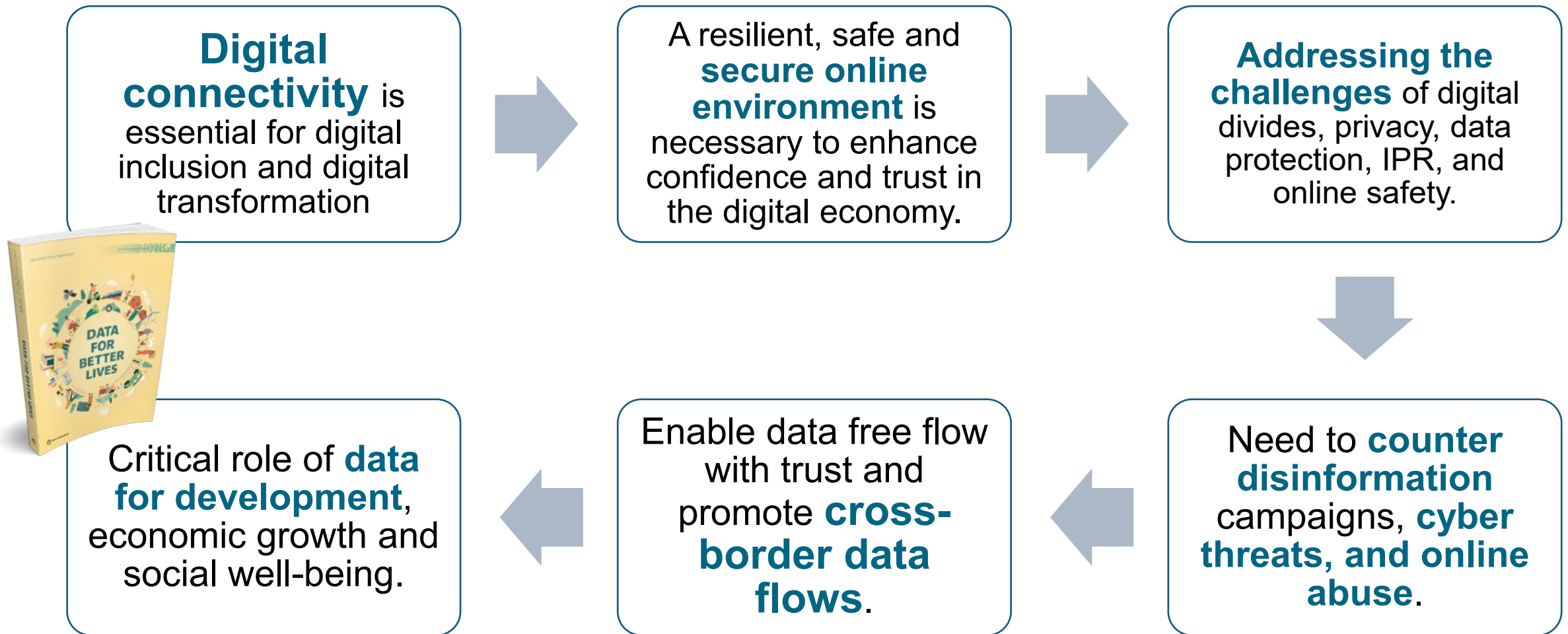
3. Data-driven decision making in private and public.

4. Emerging threats to the fundamental right of privacy.



The G20 Digital Economy Transformation Framework

G20 Bali Declaration, 2022

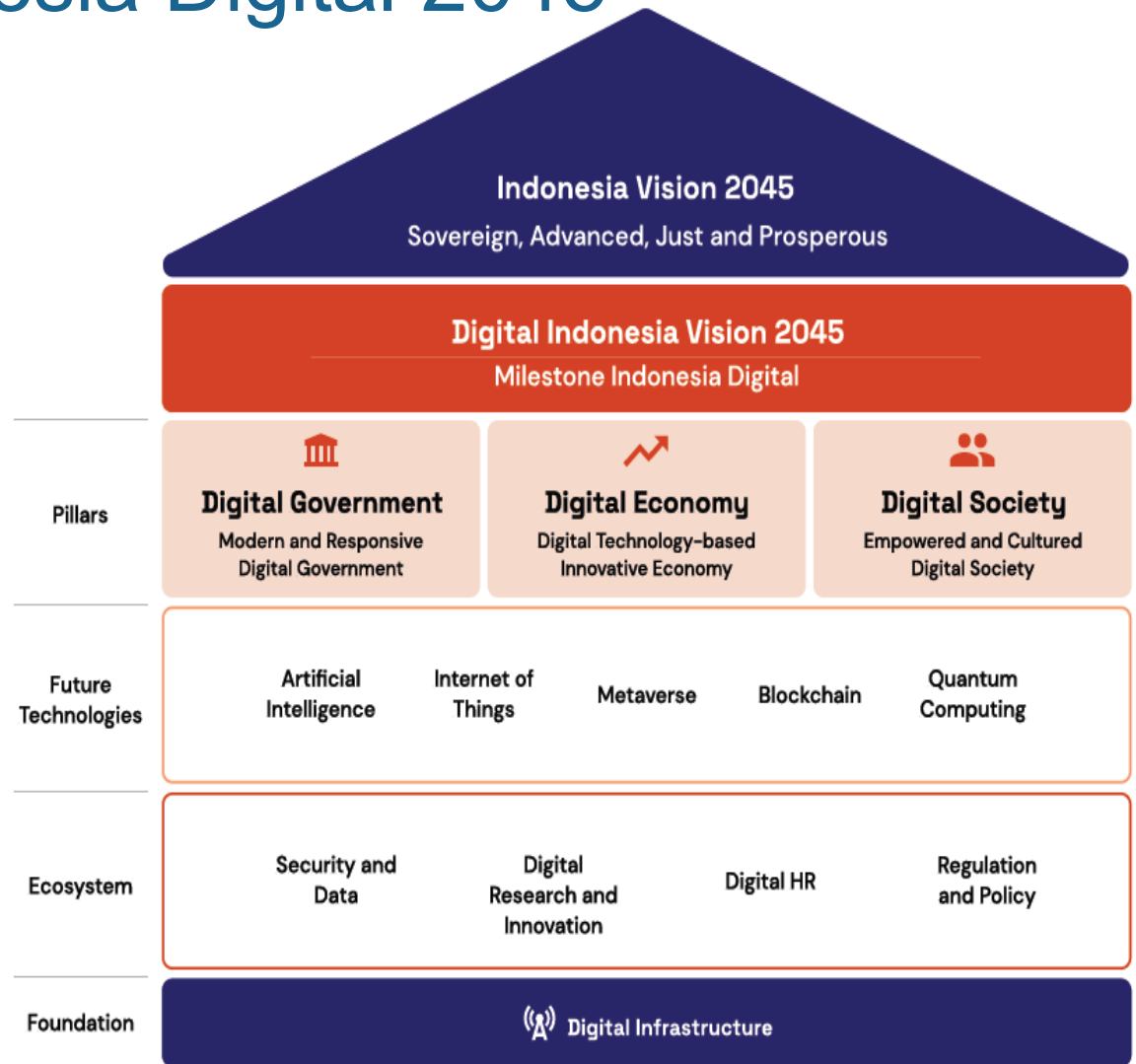


The Vision of Indonesia Digital 2045



THE VISION OF INDONESIA DIGITAL 2045:

"ACHIEVING AN INCLUSIVE AND COLLABORATIVE DIGITAL ECOSYSTEM BASED ON INNOVATION, TO SUPPORT ADVANCED, SOVEREIGN AND SUSTAINABLE INDONESIA"



▲ Figure 3.1 Framework for Visi Indonesia Digital 2045

Global Risks Severity: AI-related Risks Top 5 (World Economic Forum 2025)

FIGURE C Global risks ranked by severity over the short and long term

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period."

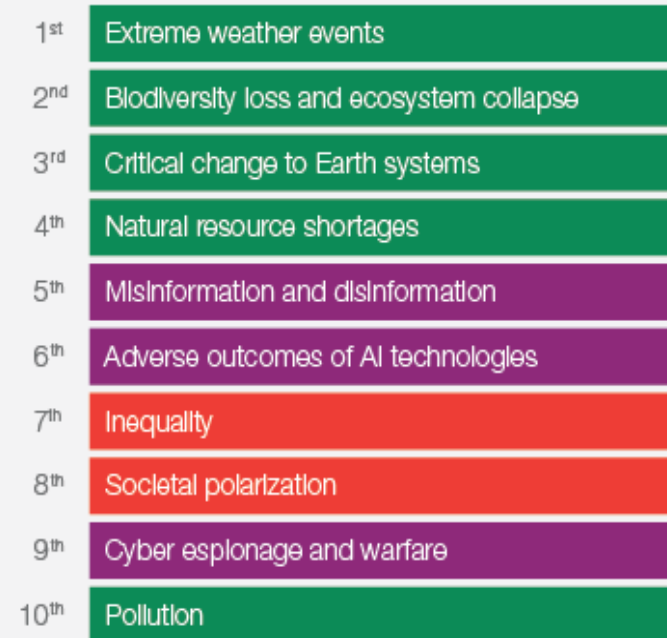
Risk categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

2 years



10 years



Source

World Economic Forum Global Risks Perception Survey 2024-2025.

Learning from the Recent Data Breaches....



- In 2025, **critical infrastructure organizations** around the world have faced a wave of cyber threats driven by **espionage**- or **sabotage**-motivated threat actors, **financially motivated ransomware** groups, and **ideologically driven hacktivists**.
- The cyber operations are often connected to real-world geopolitical and ideological conflicts.
- Adversaries increasingly **“log in”** rather than **“break in,”** so they exploit legitimate accounts and authentication processes to gain access.

Morgan Adamski, PwC US (2025)

Cyber Risks in the Financial Institutions

Data breaches still haunt Indonesia as BSI becomes latest victim

The hacker group, which uses malicious software LockBit 3.0 that blocks user access to computer systems, claimed to hold BSI's data, including its customers' and employees' contact details, financial documents, card details and passwords of the customers.



StarPlus News Asean+ Business Sport Metro Lifestyle Food Tech Education

TOPICS : StarExtra Flood Alert StarESG Urban Biodiversity True or Not SOBA 2023 Co

Potential data breach at iPay88 still under probe, says Bank Negara

THE STRAITS TIMES

8,500 phishing cases in Singapore in 2022; more than 80% spoofed a bank or financial service

Maybank warns of new fake banking website created to steal customer details

By ANGELIN YEOH

Singapore bank faces regulatory action over 'unacceptable' digital service outage

Hours-long disruption to DBS' online banking services is the second such incident in just over a year, notes Singapore's industry regulator, which says the bank has "fallen short" in ensuring system availability and quick recovery.



Search News

TEMPO EXCLUSIVE

Home Popular News News Asean & Beyond Sport Environment

Police Arrest EDCCash CEO over Cryptocurrency Fraud

Translator Editor



INDONESIA ELECTION 2024 BUSINESS WORLD OPINION CULTURE DEEPDIVE FRONT ROW

LIFE • LIFESTYLE

The 'pinjol' trap: The horrors of payday loans in pandemic-stricken Indonesia

Many Indonesians are drowning in overbearing loans and intimidation attacks after taking out on loans to survive.

JP Staff (The Jakarta Post)

PREMIUM Jakarta • Fri, September 17, 2021

Dugaan Kebocoran Data, Bank Jatim: Data Penting Nasabah Dipastikan Aman

Kompas.com - 29/10/2021, 18:38 WIB

Recent Data Breach Incidents in Indonesia



BPJS Kesehatan
Badan Penyelenggara Jaminan Sosial



**komisi
pemilihan
umum**



eHAC Indonesia
Health Quarantine MoH Indonesia



Lazada

facebook
Indonesia

BRIlife

kreditplus
PT. KB FINANSIA MULTI FINANCE



tokopedia

bukalapak

RedDoorz

NPWP
Nomor Pokok Wajib Pajak

PUSAT DATA NASIONAL
KOMINFO

BSI
BANK SYARIAH
INDONESIA

<https://inet.detik.com/security/d-7549825/data-npwp-bocor-tambah-daftar-panjang-kasus-kebocoran-publik-di-ri>

<https://nasional.kompas.com/read/2021/09/03/18445501/deretan-kasus-kebocoran-data-pribadi-dalam-dua-tahun-terakhir>

<https://www.liputan6.com/teknologi/read/5285458/kronologi-bsi-jadi-sasaran-ransomware-lockbit-aksi-peretasan-diduga-saat-libur-lebaran>

BAHAYA BOBOLNYA PUSAT DATA NASIONAL

Pusat Data Nasional (PDN) lumpuh akibat *ransomware* Brain Cipher pada Kamis 20 Juni lalu. Akibatnya, aktivitas layanan publik di sejumlah kementerian/ lembaga terhambat.

Ransomware Menyerang PDN



Dampak

- ▶ 24 kementerian
- ▶ 32 lembaga
- ▶ 210 layanan publik pusat & daerah



Jenis ransomware

Brain Cipher (varian *Lockbit 3.0*)

- ▶ Ekstraksi Data
- ▶ Enkripsi Data
- ▶ Mengirim ID enkripsi dijual di *dark web*
- ▶ Mirip *ransomware* yang menyerang BSI pada 2023

Dkatadata.co.id

#KalauBicaraPakaiData

Ekonografik

Tebusan yang diminta peretas
US\$8 juta
(Rp131 miliar)



Data yang Bocor di *Dark Web*

Sejak bocornya Pusat Data Nasional, beragam data pribadi penduduk Indonesia diperdagangkan di BreachForums*

*) Data diambil pada 25 Juni 2024, pukul 14.37 WIB

- ▶ Anggota DPR
- ▶ Anggota Badan Intelijen Strategis (BAIS) TNI
- ▶ Anggota INAFIS Kepolisian
- ▶ Anggota Kepolisian RI
- ▶ Pekerja di SatuData.go.id
- ▶ Data guru Yogyakarta dari Ditjen Guru dan Tenaga Kependidikan
- ▶ Karyawan Astra Indonesia
- ▶ Karyawan PT Berca Kawan Sejati
- ▶ Lebih 15 ribu KTP, SIM, & paspor penduduk Indonesia

SUMBER: KOMINFO, BREACHFORUMS, BROADCOM, KATADATA, KOMPAS | NASKAH: PUJA PRATAMA | ILUSTRASI: FREEPIK, A.I | DESAIN: AMOSELLA | PRODUKSI: JUNI 2024

“Apakah ada kaitan judi online atau tidak, itu nanti dalam tahap investigasi selanjutnya.”

Nezar Patria, Wakil Menkominfo



KATADATAcoid

Katadata Indonesia

katadatacoid www.katadata.co.id



AI and Misinformation

Europe Invasion @EuropeInvasionn
BREAKING
A man attacked a nursery in Southport and stabbed 6 children. Multiple ambulances attended the scene. 1 child died. The attacker is alleged to be a Muslim immigrant.

SOUTHPORT - If this is true, then all hell is about to break loose.

Southport Stabbings suspect, **Ali-Al-Shakati**, was on MI6 watch list and was known to Liverpool mental health services. He was an asylum seeker who came to UK by boat last year.

BBC

BITESIZE

Timeline of how online misinformation fuelled UK riots

Part of [Other Side of the Story](#)

[Save to My Bitesize](#)

Just hours after an attack at a dance class in Southport, which resulted in the death of three girls, a surge of misinformation spread online fuelling protests and riots across the country.

INDEPENDENT [Subscribe](#) [Menu](#)

NEWS SPORT VOICES CULTURE LIFESTYLE INDYBEST DEALS

News > World > Americas > US politics

Fake videos and AI chatbots drive disinformation about LA protests

As protests against Trump's immigration raids spread across the country, machine-generated deepfakes spread by partisan outrage merchants are pouring fuel on the fire

Io Dodds in San Francisco • Friday 13 June 2025 05:42 BST

[9 Comments](#)

[Bookmarks](#) [Facebook](#) [Twitter](#) [WhatsApp](#) [Email](#)

VOICES CULTURE **LIFESTYLE** INDYBEST DEALS TRAVEL MORE **INDEPENDENT tv**

Tech

Indonesia blocks Facebook and WhatsApp features after 'fake news-inspired' riots and deaths

One hoax story that went viral on social media claimed secret Chinese soldiers were posing as riot police

BY MATT BURGESS SECURITY JUL 14, 2025 7:00 AM

AI 'Nudify' Websites Are Raking in Millions of Dollars

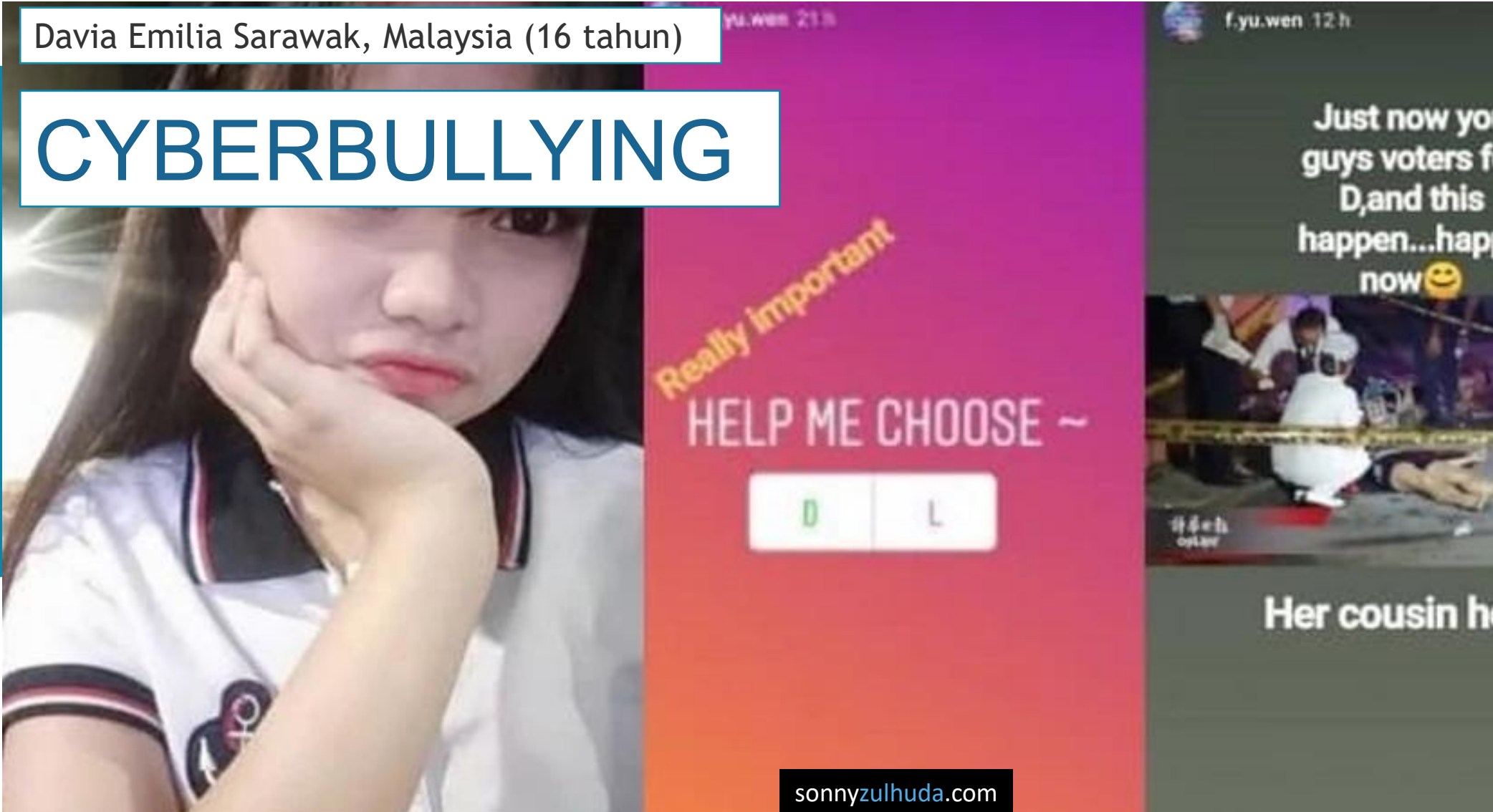
Millions of people are accessing harmful AI "nudify" websites. New analysis says the sites are making millions and rely on tech from US companies.



Remaja Bunuh Diri Setelah Bikin Poling Instagram dan 69 Persen Memilih 'Mati'

Davia Emilia Sarawak, Malaysia (16 tahun)

CYBERBULLYING

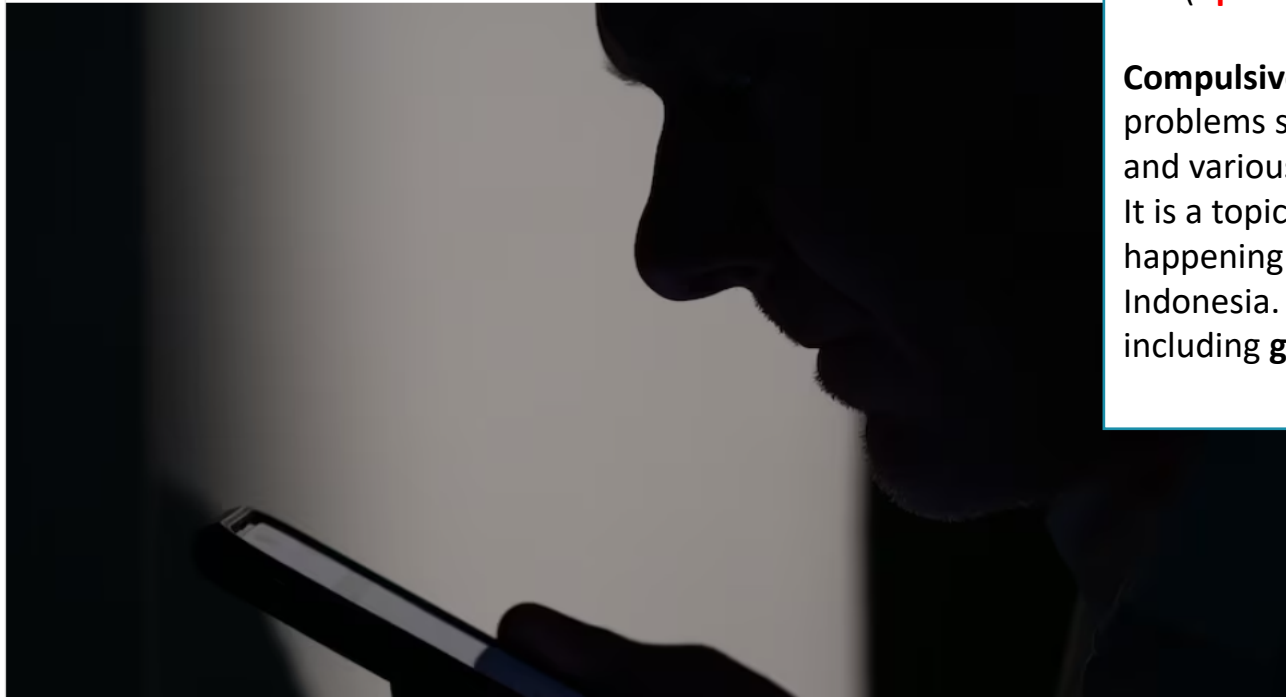


ANALYSIS

Indonesia has to hold or fold on online gambling ban

360info / By Bambang Pratama

Posted 20 Aug 2024, updated 20 Aug 2024



Indonesia's online gambling problem is **huge**.

- Indonesians lost an estimated \$30.7 billion (**Rp327 trillion**) gambling online in 2023.
- More than 10% (440,000) online gamblers are **11-20 yrs**.
- A staggering 80,000 more are **under 10**.
- The past 5 yrs, cash flow is estimated at \$56.36 billion (**Rp600T**).

Compulsive online gambling plays a role in detrimental social problems such as addiction, loan shark debts, murders, divorce and various mental health problems.

It is a topic of national concern in the media. This is all happening despite gambling, for the most part, being illegal in Indonesia. That has not stopped millions from indulging in it, including **government officials**.

<https://www.abc.net.au/asia/indonesia-has-a-huge-online-gambling-problem/104179856>



In Indonesia, online fraud is the second largest kind of crime

Approximately 25% of all Indonesians become victim of online fraud

In Indonesia, online fraud makes up the second largest category of cases filed in police reports. It contributes to more than a quarter of all cybercrime cases, according to data from the [National Police's Criminal Investigation Agency](#).

The National Cyber and Crypto Agency (BSSN) noted that in 2021 there will be more than 90,000 criminal acts in the Indonesian Internet world. In addition, the 2021 cyber security monitoring report issued by BSSN also detected 1.6 billion suspicious attempts to infect cyber security systems or internet traffic anomalies in Indonesia. That number has tripled compared to 2020.

Especially investment scams are a concern. The number of consumers investing has tripled since 2019. More than 3,000 online trading and investment platforms have been shut down as scams.

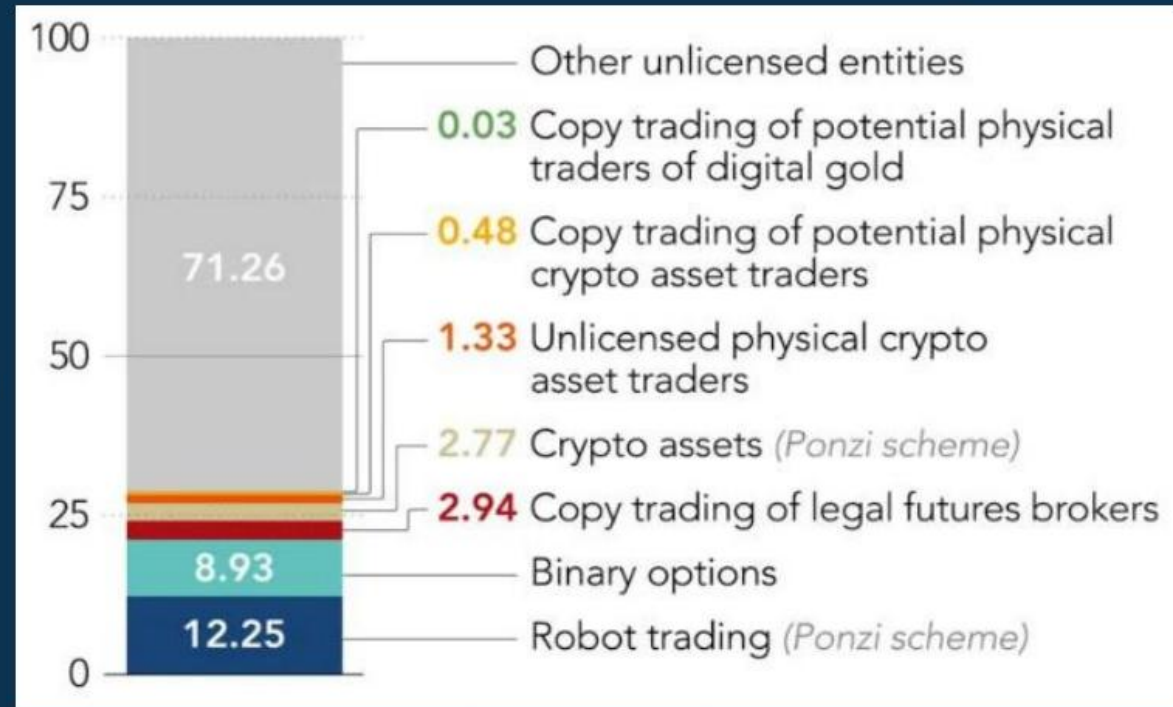
Several studies by Kaspersky and Experian state that 25% of the consumers have fallen for scams. Most of these scams (51%) happen on social media.

Indonesians are directed to several organizations to report online scams. For suspicious investment schemes, the Enforcement and Investor Protection Department of the SEC can be contacted via phone and email.

For malicious messages, reports can be lodged to the [National Bureau of Investigation \(NBI\) Anti-Fraud Division](#) online, via email, phone and Facebook. The NBI is investing heavily in both equipment as well as staff, hiring 200 additional cybercops in 2021 alone.

Citizens can also report incidents to the [PNP Anti-CyberCrime Group](#) online and via phone.

The Department of Finance has also opened its online channels for netizens to report any posts, advertisements, and messages containing false information.



Blocked trading platforms in Indonesia by type, 2923 sites, 2020 – July 2022
Source: Indonesia's Commodity Futures Trading Regulatory Agency.

Key Statistics:

Population:	276 million
Internet:	77%
# of Scams:	-
Scams / 1,000 :	-
Money lost:	-
Per capita:	-
Per report:	-

Key Organizations:

- [National Cyber and Crypto Agency](#)
- NBI Anti-Fraud Division
- PNP Anti-Cybercrime Group

WhoisXML API:

Domains/capita	0.003
Domains registered	886,915



Home > News > World-first "Cybercrime Index" ranks countries by cybercrime threat level

World-first "Cybercrime Index" ranks countries by cybercrime threat level

RESEARCH SOCIAL SCIENCES

Following three years of intensive research, an international team of researchers have compiled the first ever 'World Cybercrime Index', which identifies the globe's key cybercrime hotspots by ranking the most significant sources of cybercrime at a national level.

CYBERCRIME INDEX

Ranking countries by cybercrime threat level

Ranking	Country	WCI score	Ranking	Country	WCI score
1	Russia	58.39	11	Iran	4.78
2	Ukraine	36.44	12	Belarus	3.87
3	China	27.86	13	Ghana	3.58
4	United States	25.01	14	South Africa	2.58
5	Nigeria	21.28	15	Moldova	2.57
6	Romania	14.83	16	Israel	2.51
7	North Korea	10.61	17	Poland	2.22
8	United Kingdom	9.01	18	Germany	2.17
9	Brazil	8.93	19	Netherlands	1.92
10	India	6.13	20	Latvia	1.68

<https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level>

UN agency map reveals Cambodia as global scammer hub

Sign up now: Get insights on Asia's fast-moving developments



Contrary to widespread assumptions that Myanmar is the regional epicentre, Cambodia now appears as the leading hotspot for cyber fraud operations.

PHOTO: ST FILE

Disekap, disetrum, dan dipukul hingga babak belur: Pengakuan WNI yang menyelamatkan diri dari perusahaan scam di Kamboja



EPA

Our misconception about the Internet!

Many believe that cyberspace simply cannot be regulated. Behavior in cyberspace, this meme insists, is beyond government's reach. The anonymity and multi-jurisdictionality of cyberspace makes control by government in cyberspace impossible. The nature of the space makes behavior there unregulable.

This belief about cyberspace is wrong.

It is based on two wrong assumptions: that the nature of cyberspace is fixed, cannot be changed — or that government cannot take steps to change this architecture.

**Lawrence Lessig, Lawrence Lessig. (1999).
“The Law of the Horse: What Cyberlaw might
Teach.”(1999) 113 Harvard Law Review 501.**



The False Sense of Anonymity



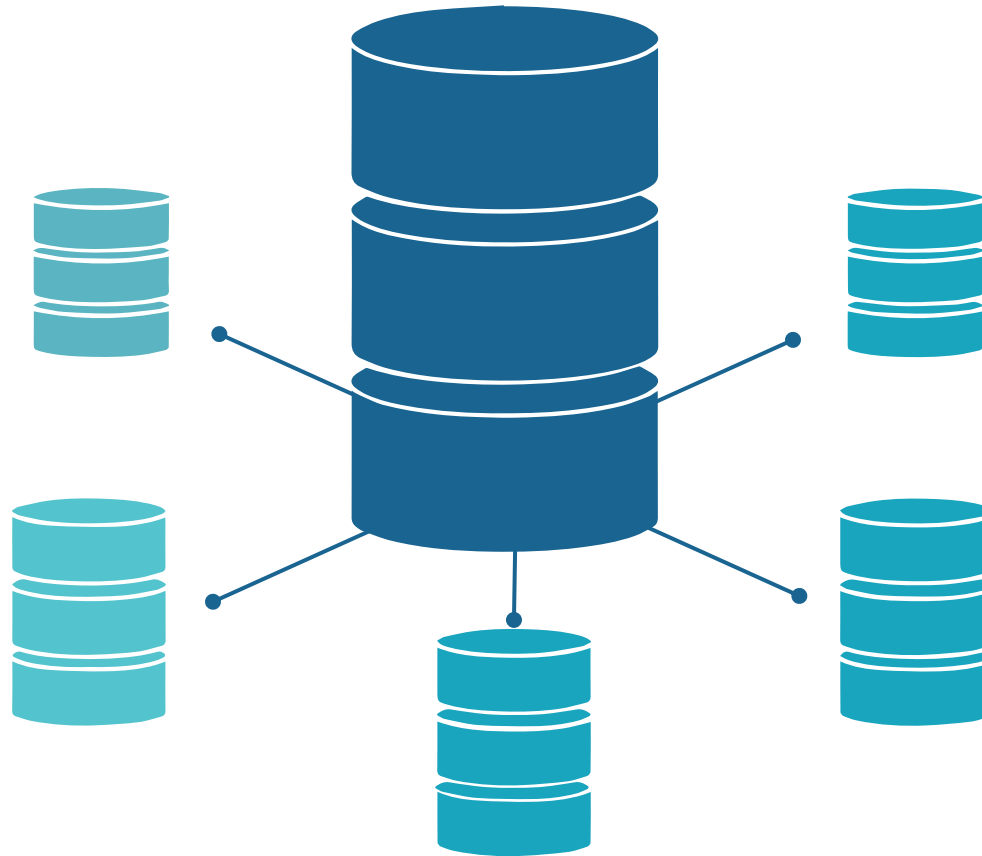
False Sense of Anonymity

Kevin Mitnick (1995) on hacking spree believing that he could beat authority.



Doing Away with Government

Edward Snowden (2013) is wanted by the US Government for an alleged leaking of secret information.



Freedom of Expression

Ross Ulbricht and the Road Silk (2015) launched a commercial portal for illicit materials in the dark web, arguing for freedom of expression



Predatory Behaviour

Takahiro Shiraishi (2020) made his Twitter account to provide help for those who want to commit suicide.

Disregard Personal Data

Facebook/Meta (2021) made a public enemy by allowing data of its users misused in the political campaign.

The False Sense of Anonymity



ROSS ULBRICHT
San Francisco, USA

Di usia 27 menciptakan platform SILK ROAD

Di usia 29: Memiliki aset Bitcoin senilai Rp 1.1 Triliun

Di usia 31 dijatuhi hukuman penjara seumur hidup tanpa peluang pengampunan



messages(0) | orders(0) | account

Shop by category:

- Drugs(752)
- Cannabis(280)
- Ecstasy(35)
- Dissociatives(11)
- Psychedelics(84)
- Opioids(62)
- Stimulants(53)
- Other(107)
- Benzos(70)
- Lab Supplies(6)
- Digital goods(98)
- Services(48)
- Money(55)
- Weaponry(15)
- Home & Garden(14)
- Food(4)
- Electronics(5)
- Books(49)
- Drug paraphernalia(28)
- XXX(30)
- Medical(3)
- Computer equipment(4)
- Apparel(4)
- Musical instruments(2)
- Tickets(1)
- Forgeries(13)



5 Marijuana Butter
Chocolate Chip...
฿8.53



4mg. TIZANIDINE
(zanaflex) x25
฿2.09



US customers only
Express...
฿2.79



4 x 20MG Original Lily
Cialis
฿7.85



(1g) High-grade Crystal
Meth
฿11.95



MindFood - Protect your
brain!...
฿3.69



to US 1/4 lb (qp) BC
Master Kush...
฿121.37

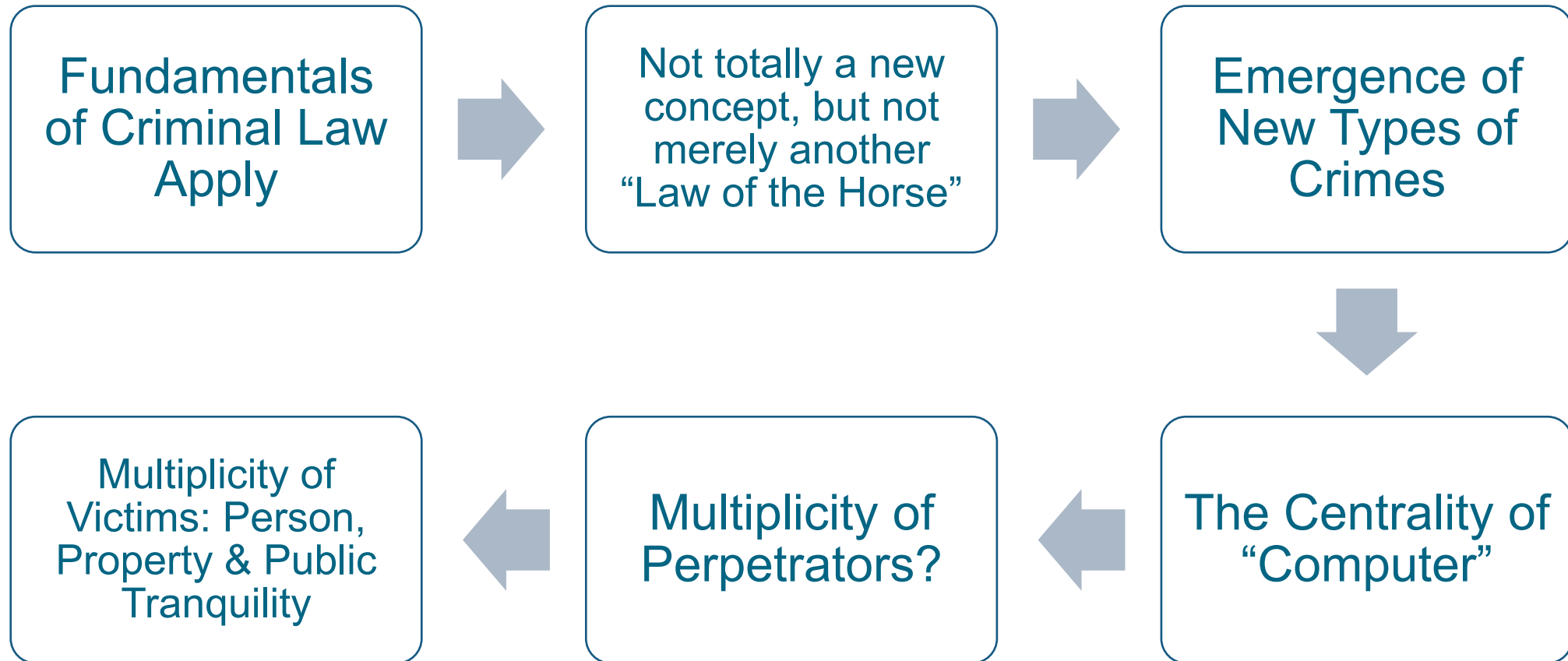


How to Grow Mushrooms
฿0.14



Mushroom Indoor
Growing - Easy...
฿0.29

Nature of Cyber Crime



Cyber crime is a Transnational Crime

- It is committed in more than one State;
- It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;
- It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or
- It is committed in one State but has substantial effects in another State.

(Art 3.2 of the UN Convention Against Transnational Organized Crime 2000)

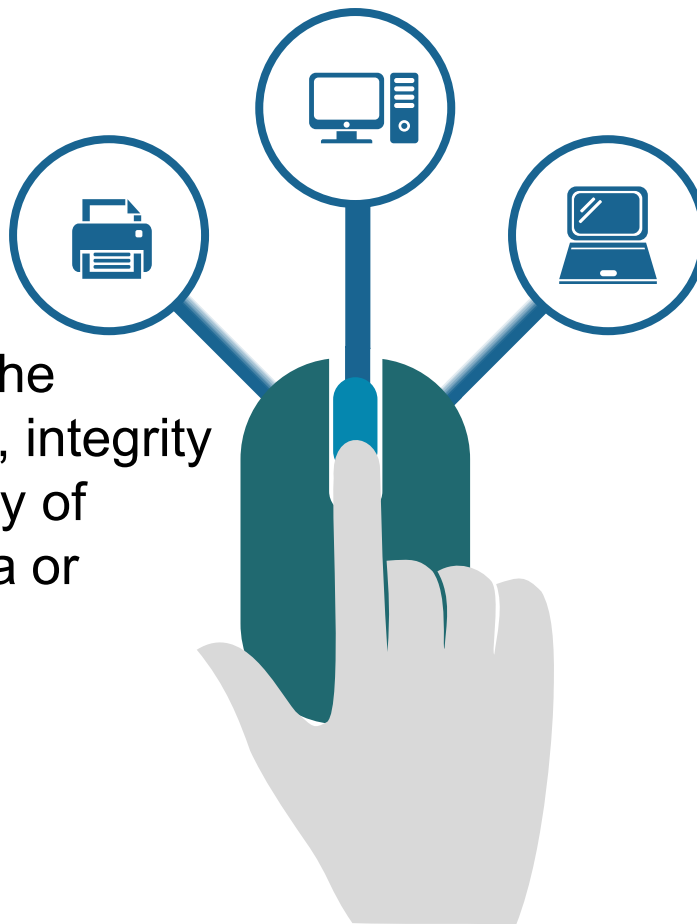


Categories of Cyber Crime

Computer-related acts

Acts against the confidentiality, integrity and availability of computer data or systems.

Computer content-related acts





Justification for a Cybercrime Convention

- Challenges of the **digitalisation**, **convergence** and **globalisation** of computer networks;
- Risk that computer networks and electronic information may be **used for committing criminal** offences and **storing related evidences**
- Need for **co-operation** between States and private industry in combating cybercrime
- Need to protect **legitimate interests** in the use of information technologies
- Need for an increased, rapid and well-functioning **international co-operation** in cyber criminal matters
- Need to **eliminate safe havens** for cyber criminals



The Objectives of Cybercrime Convention

Harmonising the domestic criminal **substantive law elements of offences** and connected provisions in the area of cyber-crime

Providing for **domestic criminal procedural law powers** necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system

Setting up a fast and effective regime of **international co-operation.**

International Cybercrime Treaties

United Nations Convention against Cybercrime;
*Strengthening International Cooperation for Combating
Certain Crimes Committed by Means of Information and
Communications Technology Systems and for the Sharing of
Evidence in Electronic Form of Serious Crimes*

**A new Convention adopted by the UN General Assembly
in New York on 24th December 2024 by Resolution 79/243.**

Article 7: Illegal access

Article 8: Illegal interception

Article 9: Interference with electronic data

Article 10: Interference with an information and
communications technology system

Article 11: Misuse of devices

Article 12: ICT technology system-related forgery

Article 13: ICT system-related theft or fraud

Article 14: Offences related to online child sexual abuse or
child sexual exploitation material

Article 15: Solicitation or grooming for the purpose of
committing a sexual offence against a child

Article 16: Non-consensual dissemination of intimate images

Article 17: Laundering of proceeds of crime

**Budapest Convention on
Cybercrime 2001**

**Adopted in Budapest in 2001 as a
European Treaty, and was further
expanded to be opened to the
rest of the World.**

Article 2. Illegal access

Article 3. Illegal interception

Article 4. Data interference

Article 5. System interference

Article 6. Misuse of devices

Article 7. Computer- related forgery

Article 8. Computer- related fraud

Article 9. Offences related to child
pornography

Article 10. Offences related to infringements
of copyright and related right



Legal Responses in Indonesia

Law No. 11/2008 (E-Information and E-Transaction)

Law No. 19/2016 (Amendment to Law No. 11/2008)



Law No. 44/2008 (Pornography)

Law No. 14/2008 (Freedom of Public Information)



Presidential Regulations No. 95/2018 (Electronic-Based Government System)
Presidential Regulations No. 39/2019 (One Data Indonesia)

Presidential Regulations No. 28/2021 (National Cyber and Crypto Agency)



Presidential Regulations No. 74/2017 (E-Commerce Roadmap)
Government Regulations No. 71/ 2019 (Administration of Electronic System and E-Transaction)
Government Regulations No. 80/2019 (Electronic Commerce)



Law No. 27/2022 (Personal Data Protection)

Challenges in Regulating Digital Technologies



Responsive Legislation and Judiciary

Indonesia shall ensure its legal framework responds all new legal challenges with new offences, new procedures or new evidentiary rules.



Preventive (+ reactive) Approach

Law on digital landscape shall provide clear set of due-diligence and risk-based approaches, so that we do not rely only on punitive measures, e.g. through corporate liability, fault-based damages, administrative licensing.



Risks of Over-criminalisation

Unclear law and weak enforcement will only lead to public distrust and tendency of over-criminalization and over-litigation



Securing International Cooperation

Mostly required when addressing the difficulty of enforcing the law against foreign perpetrators. Also helpful to combat international crimes, transnational organized crimes (eg Terrorism) or issues of cross-border data transfer/data localisation.



Keeping in Mind the Geopolitics of Cybercrime

As Indonesia plays an active and open diplomatic role, keeping the geopolitics of cybercrime Conventions in check is crucial.





Closing Remarks

01

As a social instrument, the law changes with the change of the society. The dynamics of cybercrime requires Indonesia to keep its cybercrime law relevant and responsive

02

Cybercrime emerges as another international and transnational crimes. Geopolitics, globalization, international trade and regionalism are all playing important role.

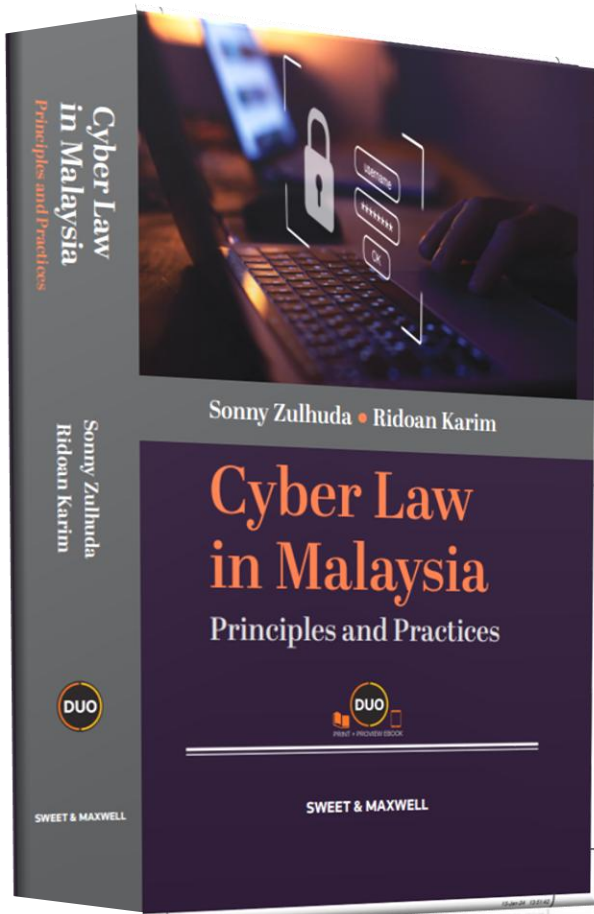
03

Reform on cybercrime legal landscape requires unconditional commitment at home to seriously enforce the law.

Reading List

1. Brenner, S.W. & Clarke, L.L. (2005). Distributed security: Preventing cybercrime. *The John Marshall Journal of Computer & Information Law*, 23 J. Marshall J. Computer & Info. L., 659.
2. Budi Agus Riswandi, Sonny Zulhuda, Ari Wibowo, Ratna Hartanto, Nabilla Maryam Luthfidyfa and Vania Lutfi Safira Erlangga. (2023). *Personal Data Protection Law (Comparative study on Indonesian and Malaysian Law)*. UII Press, Yogyakarta, Indonesia.
3. Lawrence Lessig. (1999). The Law of the Horse: What Cyberlaw might Teach. 113 *Harvard Law Review* 501.
4. Shoshana Zuboff (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books Ltd.
5. Sonny Zulhuda & Ridoan Karim (2024). *Cyber Law in Malaysia: Principles and Practices*, Sweet & Maxwell, Kuala Lumpur.
6. Viktor Mayer-Schönberger, Kenneth Cukier. (2013). *Big Data: A Revolution that Will Transform How We Live, Work and Think*. London: John Murray.





THANK YOU DR SONNY ZULHUDA

 sonny@iium.edu.my
 sonnyzulhuda.com

SCOPUS ID: 35782606500
ORCID ID: 0000-0003-0192-1971
GOOGLE SCHOLAR ID: [B99CpLkAAAAJ&hl](https://scholar.google.com/citations?user=B99CpLkAAAAJ&hl)
IREP IIUM PAGE: <http://irep.iium.edu.my/>



Check the book at:
sweetandmaxwellasia.com.my