Tendensi Politis Kejahatan Dunia Maya

Bambang Mudjiyanto[1], Launa[2*], Franky P. Roring[3]
[1,2,3]Universitas Bung Karno, Jl. Pegangsaan Timur No. 17A, Menteng, Jakarta Pusat 10310, Indonesia
launa.ubk@gmail.com

ABSTRACT

This study aims to search a number of data, documents and literature to explore cyber crimes which are not only economically motivated, but also have political tendencies. Various cases of data hacking carried out by regional and global hackers and crackers have positioned cyber space as an arena for aggressive political contestation that has shaken the foundations of political, military, defense, security and intelligence life. The concept of cybersecurity is currently projected to protect national interests/sovereignty (cyberdefence) through developing cyberwar and cyberdiplomacy strategies to overcome the increasingly intense threat of cybercrime. This qualitative study using a descriptive analysis method based on a literature study approach tries to analyze the political tendencies underlying the motives for cybercrime, both at the global and national levels. The results of the study show: cyber space in many countries (including Indonesia) has been transformed into an arena of aggression and a realm of political contestation which—if not anticipated through breakthroughs and extra efforts—has the potential to thwart Indonesia in safeguarding its national interests, maintaining the sovereignty of its citizens from cyber threats, and it is difficult to expose Indonesia's national diplomatic capabilities in responding to cyber crimes that continue to move wildly.

Keywords: *Cybercrime, Cyber defense, Cyber diplomacy, Cyber security, Cyber war, Political tendencies.*

ABSTRAK

Studi ini bertujuan melakukan penelusuran sejumlah data, dokumen, dan literatur untuk mengeksplor kejahatan dunia maya yang tak hanya bermotif ekonomis, namun juga bertendensi politis. Beragam kasus peretasan data yang dilakukan para *hacker* dan *cracker* regional dan global telah memosisikan ruang siber sebagai arena agresi kontestasi politik yang telah menggoncang sendi-sendi kehidupan politik, militer, pertahanan, keamanan, dan intelijen. Konsep *cybersecurity* saat ini lebih diproyeksikan untuk menjaga kepentingan/kedaulatan nasional (*cyberdefence*) melalui penyusunan strategi *cyberwar* dan *cyberdiplomacy* guna mengatasi ancaman kejahatan siber yang kian intens. Studi kualitatif dengan metode analisis deskriptif berbasis pendekatan studi pustaka ini coba menganalisis tendensi politik yang melatari motif kejahatan dunia maya, baik di level global maupun di nasional. Hasil studi menunjukkan: ruang siber di banyak negara (termasuk Indonesia) telah bertransformasi menjadi arena agresi dan ranah kontestasi politik yang—jika tidak diantisipasi dengan terobosan dan upaya ekstra—berpotensi menggagalkan Indonesia dalam menjaga kepentingan nasionalnya, merawat kedaulatan warganya dari ancaman dunia siber (*cyber defence*), dan sulit mengekspose kapasitas diplomasi nasional Indonesia dalam merespon tindak kejahatan dunia maya yang terus bergerak liar.

Kata-kata Kunci: Diplomasi siber, Keamanan siber, Kejahatan dunia maya, Pertahanan siber, Perang siber, Tendensi politik.

Korespondensi: Launa. Universitas Bung Karno. Jl. Pegangsaan Timur No. 17 A, Menteng, Jakarta Pusat 10310.
No. HP, WhatsApp: 081213801971 | ***Email*****:** launa.ubk@gmail.com

Submitted: September 2023 | **Accepted:** Desember 2023 | **Published:** April 2024
P-ISSN 2620-3111 | E-ISSN 2685-3957 | Website: https://ejournal.unma.ac.id/index.php/jika/

PENDAHULUAN

Kejahatan dunia maya, tindak kriminal jagad mayantara, atau *cybercrime*—yang diinisiasi oleh para *hacker* atau *cracker*—tak hanya terus terjadi dan berulang, namun sudah berada pada level membahayakan. Sebagai fenomena sosial yang muncul di era revolusi informasi yang kian disruptif saat ini, kejahatan dunia maya (*cybercrime*) telah membuat kepanikan global karena pengaruhnya yang luas dan daya rusaknya yang tinggi. Tahun 2017, misalnya, serangan Ransomware WannaCry telah menginfeksi lebih dari 230.000 komputer di 150 negara di dunia, mengakibatkan kerugian ekonomi lebih dari 4 miliar US dolar, dan menimbulkan dampak serius di sektor pendidikan, pemerintahan, keuangan, layanan kesehatan, dan sektor pelayanan publik lainnya (Chen, et al., 2023: 2).

Internet Complaint Crime Center (IC3) juga melaporkan ada 5.679.259 pengaduan yang telah dilaporkan ke IC3 selama lima tahun (2016-2020). IC3 menerima rata-rata 440.000 pengaduan per tahun terkait beragam penipuan internet yang merugikan banyak pihak, baik individu, korporasi maupun pemerintah di seluruh dunia. Tahun 2020, ada 105.301 item pengaduan yang diterima IC3 dari korban berusia di atas 60 tahun dengan total kerugian lebih dari 966 juta US dolar. Korban yang berusia di atas 60 tahun menjadi target penipuan (atau peretasan data) paling besar, karena mereka dianggap sudah mapan dan diyakini memiliki aset dan sumber keuangan yang besar (IC3, 2020).

Grafik 1. Statistik Pengaduan IC3 Sepanjang Tahun 2020
(Komparasi 5 Jenis Kejahatan Teratas, 2016-2020)

Sumber: IC3, 2020, p. 6.

Catatan: *Phisihing* = pencurian/penipuan data melalui email | *Vishing* = penipuan melalui telpon | *Smishing* = penucurian/penipuan data melalui SMS | *Pharming* = mengarahkan korban untuk membuka/masuk ke website palsu | *Non-Payment/Non-Delivery* = pesanan melalui online yang tidak dibayar si pemesanan | *Extoriton* = pemerasan online dengan ancaman membuka data pribadi/data rahasia korban | *Personal Data Breach* = penyalahgunaan data pribadi | *Identity Thef* = pencurian data pribadi oleh *hacker*/*cracker* tanpa diketahui oleh pemilik data (korban).

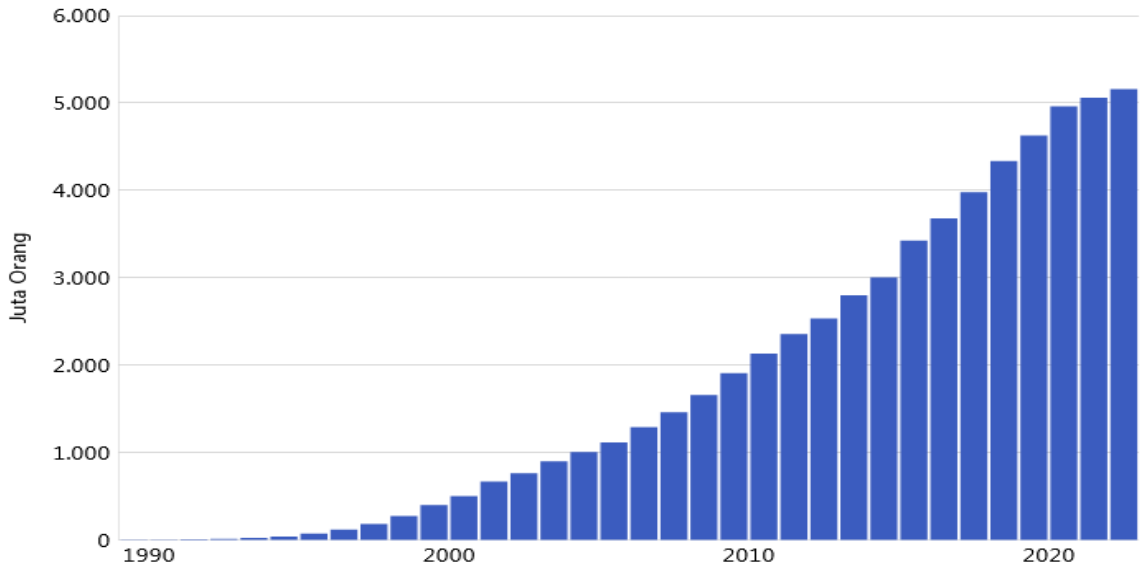
Cybercrime tak hanya bermotif ekonomis, namun juga bermuatan politis. Seperti dikatakan Gandhi, et al (2011): "*Cybercrime not only deals with profit or financial interests, but also extends to political and power matters, especially the interests of political elites who have power*". Presiden Prancis, Emannuel Macron, dan partai yang dipimpinnya (La République en Marche) pernah menjadi korban serangan siber tahun 2017 lalu. Lebih dari 20.000 data email kampanye pemilu milik partainya diretas dan dipublikasikan secara online. Macron juga mengalami peretasan ponsel (juga ponsel milik sebagian besar menteri kabinetnya) oleh Pegasus, perusahaan perangkat lunak yang dikembangkan oleh Israel (NSO Group). Peretasan data ini memungkinkan operator Pegasus mengekstrak pesan, foto, email, panggilan seluler, dan mengaktifkan mikrofon dari ponsel milik Marcron dan anggota kabinetnya yang telah terinfeksi (Kotze, 2022).

Kasus lain, pembocoran rahasia keuangan milik perusahaan oleh Wikileaks, pada 17 Januari 2008, dimana Wikileaks menerbitkan data rekening milik 2000 politisi dan konglomerat terkemuka pemilik perusahaan multinasional, perusahaan keuangan, dan para konglo asal Inggris, AS, dan Jerman. Situs berita yang dikelola oleh Julian Assange dan Kristinn Hrarfnsson ini ditengarai juga kerap membocorkan berbagai skandal politik di banyak negara, seperti serangan helikopter Apache milik AS pada warga sipil Irak, meretas dokumen rahasia militer AS yang menyiksa para tahanan di penjara Guantanamo, membongkar sindikat pemalsuan data perubahan iklim global milik Universitas East Anglia (di Inggris), membongkar daftar internet hitam yang menjadi mitra pemerintah dan politisi Australia, dan kasus lainnya (Soren, 2015; Chivers, 2019; Sandrawati, 2022).

Berikutnya, pada ajang pilpres AS tahun 2016, Rusia dituding melakukan sabotase pada kampanye Hillary Clinton, mendukung kampanye Donald Trump, dan meningkatkan perselisihan politik dan segregasi sosial antar pendukung kedua calon presiden AS tersebut. Menurut laporan intelijen AS, (CIA) maupun FBI, operasi serangan siber (dengan sandi "Proyek Lakhta") ada di bawah perintah langsung Vladimir Putin. Laporan Mueller setebal 448 halaman (yang dipublikasi pada media April 2019) menemukan lebih dari 200 kontak tim kampanye Trump dengan para pejabat intelijen militer Rusia (Glavnoye Razvedyvatelnoye Upravlenie/GRU). Laporan Mueller menyimpulkan ada indikasi konspirasi dalam pilpres AS melalui peran Internet Research Agency (IRA) yang berbasis di Saint Petersburg, Rusia. IRA telah menciptakan ribuan akun boot di media sosial yang mendukung Trump untuk melawan Hillary Clinton. Mereka menjangkau jutaan pengguna media sosial warga negara AS antara tahun 2013 dan 2017. Artikel palsu, disinformasi, dan *fake news* yang diinisiasi IRA disebarkan dari media yang

dikontrol pemerintah Rusia dan disebar di media sosial. Selain itu, IRA—yang berafiliasi dengan GRU—juga melakukan penyusupan ke jaringan sistem informasi Komite Nasional Demokrat yang mengusung pencapresan Hillary (justice.gov, 2022).

Grafik 2. Jumlah Pengguna Internet Global Tembus 5,6 Milyar Tahun 2023



Sumber: katadata.co.id., 2023

Di Indonesia, kasus peretasan data yang bertendensi politis juga tak kalah marak, diantaranya peretasan dokumen surat menyurat (berlabel rahasia) milik Presiden Jokowi dengan Badan Intelijen Negara (BIN) antara tahun 2019-2021 (total ada 679.180 data yang diretas) oleh *hacker* berinisial Bjorka; peretasan data 10 kementerian dan lembaga (K/L) oleh *hacker* Mustang Panda Group (asal Cina); peretasan halaman muka situs (*defacement*) milik Badan Siber dan Sandi Negara (BSSN); dan kebocoran data Badan Intelijen Negara (BIN) oleh *hacker* Strovian di situs breached.to yang berhasil meretas data personil BIN berisi nama, tempat tanggal lahir, pangkat/golongan, dan jabatan fungsional agen intelijen (bbc.com, 2022; Ramadhan & Asril, 2022; Purnamasari, 2022).

Berikutnya, peretasan data pemilih yang ada di Daftar Pemilih Tetap (DPT) Pemilu milik Komisi Pemilihan Umum (KPU). Info terbaru, peretasan data DPT Pemilu kembali terjadi di awal pelaksanaan kampanye pemilu 2024, yakni kebocoran 252 juta data pemilih DPT. Data pemilih dalam DPT yang bocor itu diduga diperjualbelikan di forum daring yang diunggah akun anonim Jimbo. Kasus peretasan data DPT menjelang pemilu juga pernah terjadi di tahun 2014 (2,3 data DPT KPU) dan September 2020 (105 juta data DPT KPU) (Siregar, 2023).

Seperti dikatakan Eleanor Hill, et al (2017: 773), manipulasi pemilu saat ini terbagi ke dalam tiga kategori: (1) fokus mendeteksi modus kecurangan pemilu; (2) fokus pada

metode yang dipakai untuk menginisiasi atau memberi alasan pembenar pada kecurangan pemilu; dan (3) fokus pada manipulasi dan risiko dalam praktik pemungutan suara elektronik (*e-election*). Meminjam tesis Hill di atas, maka studi kecurangan pemilu yang dimakasud dalam kajian ini adalah kecurangan pemilu (peretasan data pemilih) pada poin 3, yakni praktik kecurangan pemilu yang fokus pada kejahatan siber berbasis elektronik (*e-election*); termasuk kejahatan *cyberdemocracy* dan *cyberpolitics*.

Dari paparan di atas, terlihat tendensi politis kejahatan pemilu era siber (*e-election*) umumnya diawali oleh tindak pencurian data atau peretasan informasi publik, seperti informasi pribadi yang tersimpan dalam basis data online, informasi pribadi dalam transaksi online, catatan milik pemerintah (semisal KTP atau DPT Pemilu), dan lainnya. Senada dengan temuan Hill, dkk (2017), temuan Dragan (2018) juga menyebut bahwa:

> "Jaringan internet adalah sistem perlindungan data paling rentan. Masalahnya, internet banyak menawarkan kemudahan, seperti penyimpanan data, digitalisasi data, transmisi dan pemrosesan data dalam jumlah besar, aksesibilitas, kemudahan penggunaan, tidak dibatasi oleh jarak (bebas ruang dan waktu), serta murah dan mudah untuk digunakan. Kerentanan ini memberi ruang bagi tindak kriminal peretasan, pencurian, atau pembocoran data sebagai fenomena kriminal baru yang dikenal sebagai *cybercrime*".

Di Indonesia, tren demokrasi digital (*cyberdemocracy*) dan praktik politik digital (*cyberpolitics*) kerap diidentikkan dengan keriuhan politik publik di media sosial yang telah ikut mewarnai hajat politik besar politik di tanah air, seperti pilpres 2014, pilkada Jakarta 2017, pilpres 2019, hingga pilpres 2024. Padahal makna demokrasi digital tidak bisa direduksi sebatas pada ramainya perhatian dan keterlibatan masyarakat pada peristiwa tersebut di ranah media sosial, yang konon telah memicu polarisasi yang cukup tajam di tengah masyarakat. Namun, lebih dari itu, tren *e-lection*, demokrasi digital, dan politik digital juga menyimpan sisi buruk seperti maraknya praktik *hacktivism*.

Berbagai kasus peretasan data publik seperti diungkap media massa yang terus berulang tentu akan berimbas pada tergerusnya legitimasi politik pemerintah dan integritas KPU selaku institusi penyelenggara pemilu. Kebocoran data DPT Pemilu jelas bukan hal sepele, apalagi ia terjadi di masa-masa menjelang pemilu 2024 yang menjadi periode "panas" dan "sensitif". Apabila setiap peretas, *hacker* maupun *cracker*, bisa dengan mudah meretas situs KPU, ini tentu sangat berbahaya, bukan hanya bagi keamanan data pribadi warga negara, namun juga bagi legitimasi (proses dan hasil) pemilu yang dihasilkan. medio Februari 2024 ini akan dilaksanakan secara serentak.

Serangan *hacker* (atau *cracker*) yang beroperasi di dunia maya terhadap institusi pemerintah, partai politik, institusi penyelenggara pemilu, dan berbagai institusi publik lain

memberi alasan kuat bagi publik untuk bersikap skeptis terkait kesiapan Indonesia memasuki era *cyberdemocracy* dan *cyberpolitics*. Praktis, kepercayaan publik atas pemilu (yang demokratis) tengah mengalami ancaman serius kejahatan digital. Wajar, jika calon pemilih (*voters*) khawatir modus ini biasa dimanfaatkan pihak-pihak tertentu untuk mengubah hasil rekapitulasi penghitungan suara pemilu. Jika itu terjadi, pesta demokrasi sudah pasti akan tercederai. Bahkan tidak tertutup kemungkinan kasus-kasus kebocoran data pribadi akan memicu gelombang protes dan kericuhan politik nasional pasca pemilu.

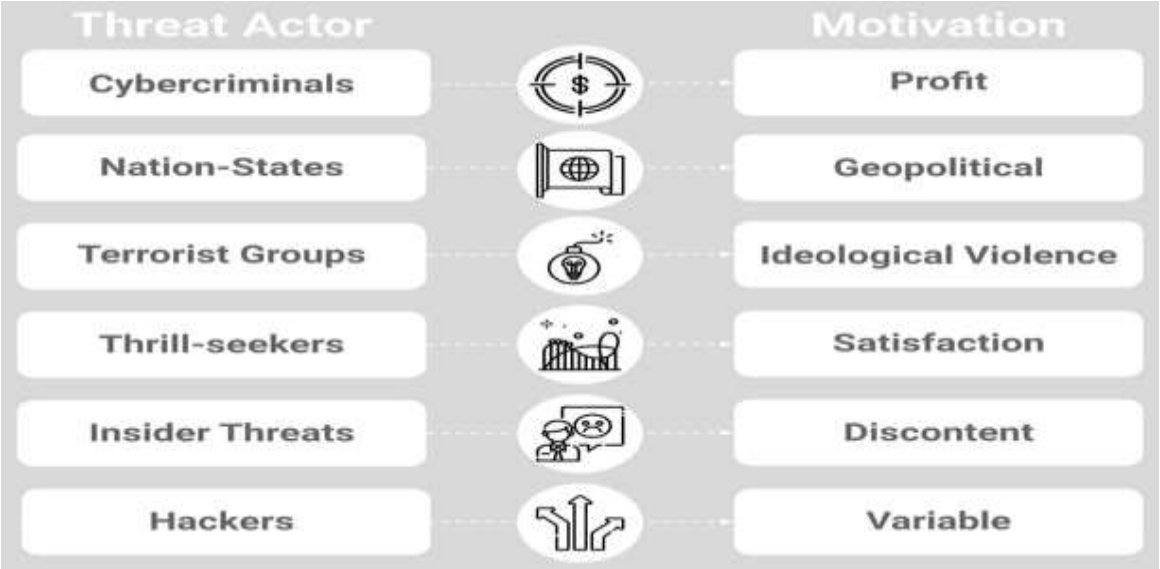
DEFINISI KONSEPTUAL DAN TINJAUAN PUSTAKA

Per definisi, *cybercrime* adalah penggunaan komputer sebagai instrumen untuk mencapai tujuan ilegal, seperti penipuan, perdagangan pornografi anak dan kekayaan intelektual, mencuri identitas, atau melanggar privasi (www-britannica-com). *Cybercrime* adalah aktifitas kriminal (seperti penipuan, pencurian, pembocoran data, atau distribusi pornografi anak) yang dilakukan menggunakan komputer terutama untuk mengakses, mengirimkan, atau memanipulasi data secara ilegal (merriam-webster.com).

Cybercrime adalah kejahatan yang dilakukan oleh seseorang atau sekelompok orang atau korporasi melalui jaringan komputer. *Cybercrime* adalah tindak kejahatan di dunia maya, lawan dari kejahatan tradisional yang ada di dunia nyata (Widodo, 2009: iii). *Cybercrime* adalah sisi gelap dari kemajuan teknologi yang memiliki dampak sangat luas. *Cybercrime* melahirkan berbagai istilah dalam kejahatan dunia maya, seperti: *economic cybercrime*, *electronic funds transfer crime* (EFT), *cybank crime*, *internet banking crime*, *on-line business crime*, *cyber money laundering*, *white collar crime*, *internet fraud*, *cyber terrorism*, *cyber stalking*, *cyber sex*, *cyber child pornography*, *cyberporn*, *cyber defamation*, *cyber criminals*, dan sebagainya (Arief, 2006: 1-2).

Sementara kejahatan dunia maya bermotif politik (*political motive of cybercrime*) adalah tindak krimimal yang terkait secara ideologis, sosial, budaya atau kepentingan sempit dengan anggota kelompok ekstremis/radikal untuk menyebarkan propaganda, menyerang situs web dan jaringan internet, mencuri uang untuk mendanai kegiatan para peretas, atau untuk merencanakan dan mengoordinasikan kejahatan mereka di dunia nyata. Kejahatan terorganisir adalah kelanjutan dari upaya ilegal dengan tujuan untuk meraih benefit politik dari aktifitas yang melibatkan perencanaan, sumberdaya pelaku, dan jejaring ilegal untuk mengatur kejahatan siber secara lebih terstruktur dan sistematis. Kejahatan dunia maya dengan motivasi politik bisa dimulai dari peretas yang hanya ingin membuat pernyataan politik, memicu kepanikan publik, hingga kelompok teroris terorganisir, seperti

ISIS atau Al-Qaeda. Kejahatan ini umumnya menggunaan jaringan internet untuk mengganggu infrastruktur penting dan layanan digital milik pemerintah di suatu negara (Shinder & Cross, 2008).



Gambar 1. Latar Motif Kejahatan Siber
Sumber: sentinelone.com

Tabel 1. Aktor dan Ciri Kejahatan Siber

Aktor	Aktifitas
Hacker	Meski dipersepsi sebagai sosok jahat di jagad maya, secara harafiah *hacker* tidak selalu merupakan orang jahat. *Hacker* bisa berupa individu atau kelompok yang memiliki keahlian pemrograman dan mampu menerobos sistem keamanan komputer untuk tujuan tertentu. *Hacker* terbagai dalam tiga kategori berikut: *White hat hacker* adalah individu atau kelompok *hacker* yang bertugas melakukan *hacking* (peretasan) dengan tujuan positif. Umumnya jasa mereka disewa oleh perusahaan sebagai konsultan untuk menjaga keamanan jaringan komputer perusahaan (*cybersecurity*) dari tindak kejahatan *black hat hacker*. *Black hat hacker* atau *unetichal hacker* adalah *hacker* yang bertujuan melakukan *hacking* (peretasan) untuk tujuan kejahatan. *Black hat hacker* sangat berbahaya bagi individu, organisasi, atau perusahaan. Mereka biasanya mencuri data atau informasi sensitif sebuah perusahaan atau organisasi tertentu menggunakan teknik *phising* dan *spoofing*. Data yang mereka peroleh bisanya untuk dijual kembali atau dimanfaatkan untuk tujuan kriminal lainnya. *Grey hat hacker* adalah gabungan dari *black hat* dan *white hat*. Biasanya mereka melakukan *hacking* (peretasan) untuk menguji keamanan sistem jaringan komputer tanpa sepengetahuan pemilik jaringan; dan memberitahu pemilik sistem begitu menemukan titik lemah. *Grey hat hacker* tidak bertujuan mencuri da ta atau merusak sistem, mereka melakukannya hanya untuk bersenang-senang.
Cracker	*Cracker* adalah aktifitas ilegal untuk menyusup dan merusak situs, website, dan sistem keamanan jaringan online, baik untuk tujuan profit maupun hobi (kesenangan). Korbannya bisa perusahaan atau individu. Para *cracker* umunya memiliki IP address dan perangkat yang sangat sulit untuk dilacak agar lebih leluasa dalam menjalankan aktifitas *hacking* (peretasan)-nya.
Carder	*Carder* (atau *carding*) adalah jenis tindak kejahatan penipuan online. Modusnya melakukan transaksi melalui kartu kredit milik *netter* (korban peretasan data). Cara kerja *carder* umumnya menggunakan email, banner atau pop-up window

	untuk menipu *netter* ke suatu situs web palsu, dimana *netter* diminta untuk memberikan informasi pribadinya. Pelaku kemudian mencuri nomor kartu kredit, melakukan konfirmasi PIN (password), dan setelah mendapat informasi dari *netter* para *carder* kemudian mencuri dana dari kartu kredit milik korban.
Deface	*Deface* adalah salah satu bentuk kejahatan online yang sering menyasar website milik individu, perusahaan, hingga pemerintah. *Deface* sendiri merupakan bentuk serangan yang membuat website korban berubah tampilan. Selain menggganti tampilan, biasanya konten yang ada di dalamnya juga tak luput dari serangan para *hacker*, misalnya menghapus atau memodifikasi konten.
Phreaker	*Phreaking* adalah istilah *slank* untuk menggambarkan aktifitas eksperimentasi peralatan dan sistem yang terhubung ke jaringan telepon umum. Istilah *phreak* adalah gabungan dari kata "telepon" dan "aneh", merujuk pada penggunaan frekuensi audio untuk memanipulasi sistem telepon. *Phreak*, *phreaker*, atau *phone phreak* adalah istihan untuk menunjuk individu atau kelompok yang berpartisipasi dalam aktifitas *phreaking.* Saat jaringan telepon telah terkomputerisasi, *phreaking* menjadi terkait erat dengan peretasan komputer. *Phereaking* juga dikenal sebagai budaya H/P (H = *Hacking* dan P = *Phreaking*).

Sumber: Fuady, 2005, p. 257-258.

Table 2. Bentuk, Modus, dan Aksi Kejahatan Siber

Jenis Kejahatan	Aktifitas
Pencurian data	Mengambil data pribadi milik orang lain secara tidak sah, baik digunakan untuk kepentingan sendiri maupun untuk kepentingan orang lain.
Mengakses ke sistem dan layanan komputer secara tidak sah	Memasuki/menyusup secara tidak sah ke dalam suatu sistem jaringan Komputer. Tujuannya adalah sabotase, pencurian data, atau pemalsuan informasi penting dan rahasia milik individi/perusahaan/pemerintah.
Membuat konten ilegal	Memasukkan data atau informasi ke dalam jaringan internet terkait infor masi yang tidak benar, tidak etis, melanggar hukum, dan mengganggu ketertiban umum, seperti pemuatan berita bohong, fitnah, pornografi, pembocoran rahasia negara, agitasi/propaganda untuk melawan pemerintahan yang sah. Unsur utama pada jenis kejahatan ini adalah pada isi data yang di-*upload* atau di-*share* ke dalam jaringan komputer.
Pemalsuan data	Meretas dokumen-dokumen penting yang tersimpan dalam sistem komputer sebagai *scriptless document* melalui internet. Kejahatan ini kerap ditujukan pada dokumen-dokumen *e-commerce* dengan cara membuat pesan seolah-olah terjadi "salah ketik". Karena korban sudah terlanjur meng-*insert* data pribadi atau PIN kartu kredit-nya, maka para pemalsu data dimungkinkan untuk menyalahgunakan data pribadi milik korban.
Spionase	Memanfaatkan jaringan internet untuk melakukan spionase terhadap pihak lain dengan cara memasuki sistem jaringan komputer pihak lain tanpa ijin. Kejahatan ini biasanya ditujukan kepada orang atau saingan bisnis yang dokumen atau data rahasia (*data base*)-nya tersimpan dalam suatu sistem komputer yang terhubung ke jaringan komputer eksternal.
Sabotase dan pemerasan	Membuat gangguan, perusakan/penghancuran terhadap data, program, atau sistem jaringan komputer yang terhubung dengan internet secara tidak sah, melalui penyusupan suatu *logic bomb*, virus komputer, atau suatu program infeksi tertentu, sehingga data program atau sistem jaringan komputer tidak bisa digunakan (gagal beroperasi/*failed to operate*).
Pelanggaran hak cipta	Mengambil dengan sengaja hak cipta atau hak kekayaan intelektual milik pihak lain di internet, seperti menjiplak tampilan *web pages* (hala-man muka) suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang menjadi rahasia dagang milik pihak lain.

Pelanggaran privasi	Melakukan peretasan data atau informasi seseorang yang bersifat pribadi dan rahasia (*sacred*). Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada data formulir pribadi yang tersimpan secara *computerized*. Jika data tersebut diketahui oleh orang lain, dapat merugikan pemilik data/informasi, baik secara materiil maupun imateriil, seperti nomor kartu kredit, PIN, ATM, catatan-catatan pribadi, cacat tubuh, atau penyakit-penyakit bawaan yang tersembunyi.

Sumber: data diolah dari berbagai sumber

Adapun kajian pustaka yang terkait tendensi politis kejahatan dunia maya dalam studi ini mengacu pada beberapa hasil studi terdahulu, seperti studi Aaron Shull (*Global Cybercrime: The Interplay of Politics and Law: Internet Governance Papers,* 2014); Tom Sorel (*Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous,* 2015); Emily Goldman (*Fresh Thinking and New Approaches are Needed on Diplomacy's Newest Frontier*, 2021); Dmitriy Lobach dan Sergey Shestopal (*Cyberattacks as a Crime of Aggression and International Terrorism: Legal Qualification Problems*, 2021); Brendan Kotze (*Why Politically Motivated Cyber-Attacks are a Threat to Democracy*, 2022); Ani Petrosyan (*U.S. Government and Cybercrime: Statistics & Facts*, 2022); Anita Lavorgna (*Unpacking the Political-Criminal Nexus in State-Cybercrimes: A Macro-Level Typology*, 2023); Apurva Venkant (*Cyberattacks Against Governments Jumped 95% in Last Half of 2022***,** 2023); dan Ray Fernandes (*Hacking Democracy: The Cyberattacks that Shaped Global Politics*, 2023).

METODE PENELITIAN

Jenis penelitian yang digunakan dalam penelitian ini adalah jenis penelitian kualitatif dengan pendekatan studi kasus. Penelitian kualitatif adalah metode ilmiah untuk memotret fenomena alamiah yang: (1) berakar pada kerangka berpikir filsafat positivisme (metode berpikir interpretif); (2) peneliti sebagai instrumen kunci dalam proses penelitian; (3) teknik pengumpulan data berciri triangulasi atau bersifat kombinatif (observasi, wawancara, dan dokumentasi); (4) analisis data bersifat induktif; (5) sumber data bersifat kualitatif (mengandalkan kajian pustaka, studi dokumen, dan observasi); dan (6) hasil penelitian dielaborasi secara deskriptif-interpretif. Sementara pendekatan studi kasus umumnya digunakan untuk melakukan telaah secara rinci dan mendalam atas satu peristiwa/fenomena alamiah dengan mengumpulkan berbagai sumber informasi untuk diolah dan dianalisis. Hasil analisis dan pengolahan data kemudian diberi makna untuk memahami fenomena, menarik makna, dan menemukan hipotesis (Priya, 2021).

Kajian ini menyandarkan sumber data dari hasil pengamatan dan studi pustaka, seperti buku, jurnal, dokumen serta artikel dan berita online. Adapun struktur pembahasan

dalam kajian terdiri dari empat bagian. Bagian pertama, membahas ruang siber sebagai arena agresi politik. Bagian kedua, mengurai ruang siber sebagai ranah kontestasi politik. Bagian ketiga, coba mengaitkan tendensi politik kejahatan dunia maya dengan kasus-kasus peretasan data yang terjadi di level global maupun di Indonesia. Bagain akhir, akan ditutup oleh kesimpulan.

HASIL DAN PEMBAHASAN

Ruang Siber Sebagai Arena Agresi Politik

Saat ini, ancaman dunia maya dalam kondisi modern perkembangan informasi dan lingkungan digital dianggap sebagai tantangan baru yang tidak hanya mengancam kepentingan masyarakat, korporasi, dan institusi negara, antar negara di tingkat global, juga hukum dan protokol internasional. Meluasnya transformasi digital yang memicu kejahatan siber dari tingkat lokal, nasional, domestik hingga ke level global faktual telah mengakibatkan kerugian materi, citra/reputasi, termasuk perubahan doktrin pertahanan, strategi keamanan nasional dan dinamika hubungan internasional. Kejahatan siber antar negara saat ini telah masuk kualifikasi kejahatan agresi politik dan teror internasional.

Penjahat dunia maya, terutama di Asia Tenggara, menggunakan Darknet dan Darkweb (yaitu semua konten yang di hosting di Darknet) sebagai sarana untuk meretas informasi milik pribadi/individu, bisnis, dan berbagai organisasi publik yang telah berkembang pesat selama enam tahun terakhir. Data tersebut kerap dijual, dipasarkan, atau dibocorkan di situs Darkweb sehingga mendorong terjadinya maraknya serangan dunia maya dan kejahatan siber. Data yang bocor inilah yang sering menyebabkan serangan seperti penargetan korban tertentu, *phishing*, faktur palsu, pencurian kartu kredit, peniruan identitas, dan penjualan dokumen rahasia..

Fakutal, ruang siber saat ini telah menjadi arena *interplay* bagi agresi politik, terutama agresi politik dalam perspektif *state-actor crime* maupun *non-state-actor crime*. Bahkan, isu "diplomasi siber" saat ini telah menjadi kekuatan "*soft power*" untuk mengatasi dampak yang muncul dari serangan dunia maya. Isu-isu tersebut mencakup berbagai topik keamanan, ekonomi, dan hak asasi manusia, termasuk standar keamanan siber internasional, akses internet, privasi, kebebasan internet, kekayaan intelektual, kejahatan dunia maya, konflik dan persaingan dunia maya yang disponsori negara, penggunaan teknologi digital, dan perdagangan (*e-commerce*) yang etis. Inilah sebabnya mengapa dunia maya—dalam ekosistem digital—telah menjadi isu sekaligus arena utama persaingan politik strategis di tingkat global (Goldman, 2021: 21).

Menurut Stephen Blank (2013), agresi politik yang dilakukan negara di dunia saat ini bukan lagi dalam bentuk pendudukan fisik (kolonisasi atau okupasi politik) satu negara atas negara lain, namun agresi politik saat ini eksis dalam bentuk perang informasi (*information war*), operasi siber (*siber operation*), perang siber (*cyber war*) atau perang psikologis (*psyco-war*). Rusia misalnya, adalah satu negara di dunia yang mengombinasi keempat operasi di atas sebelum melakukan tindakan operasi militer sebagai bagian dari kebijakan agresi politik (*intelligence war*) untuk menyelamatkan negara dari ancaman spionase (peretasan, pencurian, pembobolan data negara) yang dilakukan para *hacker*.

Tabel 3. Taksonomi Ancaman Dunia Maya

Jenis Ancaman	Motif	Target Serangan	Metode	Kemampuan
Negara-bangsa (dalam kondisi damai)	Ekonomi, militer, politik	Sektor intelijen, sektor ketahanan nasional, sektor pemerintah/birokrasi, perusahaan komersial	Doktrin serangan siber khusus oleh agen-agen intelijen, militer, dan para aktor siber.	Penggunaan domain simetris jaringan siber
Negara-bangsa (dalam kondisi perang)	Ekonomi, militer, politik	Sektor intelijen, sektor ketahanan nasional, sektor pemerintah/birokrasi, perusahaan komersial	Doktrin serangan siber khusus oleh agen-agen intelijen, militer, dan para aktor siber.	Penggunaan domain simetris jaringan siber
Terorisme dunia maya dan pemberontakan	Politik	Jaringan siber negara, proses/aktifitas politik dalam jejaring (*daring procces*)	Kombinasi ancaman persisten level lanjut (APT)	Melakukan serangkaian serangan siber terhadap institusi milik negara/organisasi inter nasional
Kejahatan dunia maya (pasar gelap)	Finansial	Pemerasan melalui peretasan infrastruktur siber	Eksploitasi melalui ransomware, malware, worm, trojan, dan jenis virus lainnya	Melakukan serangan berbasis sel melalui serangkaian ancaman persisten tingkat lanjut (APT)
Organisasi kriminal si-ber	Finansial	Pencurian hak cipta, pem-bajakan jaringan kompu-ter	Eksploitasi data bisnis/perusahaan melalui penyebaran virus ransom mware, malware, worm, trojan	Serangan siber dengan level ancaman yang berbahaya (*dangerous level*)
Kelompok penipu Siber (Anonymous, scattered spider, dll)	Finansial	Pencurian hak kekayaan intelektual, atau tekanan langsung/tidak langsung terhadap sumberdaya ekonomi/finansial	Peretasan data secara organik dan terencana (target bersifat spesifik)	Melakukan koordinasi dan sentralisasi serangan dalam waktu cepat

Sumber: www.pinterest.com

Motif di balik serangan siber politik seringkali lebih dari sekadar uang, dan sasaran utamanya adalah perlawanan politik, penuruan legitimasi negara, perusakan sistem

demokrasi, atau menciptakan kekacauan pemilu. Serangan siber bermotif politik sering dikaitkan dengan "*scyber-terrorism*" yang diotaki atau dikendalikan oleh intelijen, aktor-aktor negara, atau para *hacker*/*cracker* bayaran bereputasi internasional. Serangan seringkali menargetkan lembaga pemerintah atau infrastruktur penting milik negara, organisasi bisnis atau entits politik yang dianggap sebagai musuh mereka (Munk, 2022).

Munn dan Turner (2021) membedakan antara serangan siber yang berasal dari ransomware atau malware dengan serangan yang dilakukan oleh jaringan *hactivism*. Jika ransomware/malware secara umum adalah serangan siber bermotif politis, organ jaringan *hactivism* adalah kelompok aktivis yang serangannya lebih mengarah ke bentuk serangan untuk mempromosikan agenda ideologis. *Hacktivism* adalah organ perlawanan sipil (*civil disobidience*) yang bertindak dengan motif non-finansial. Tujuannya membuat perhatian dan sensasi politik. Menurut Fernandes (2023), serangan siber bermotif politik umumnya dipengaruhi oleh beberapa faktor, seperti faktor geopolitik, keyakinan ideologis, perang informasi, dan faktor demonstrasi kekuasaan.

Tabel 4. Motif *Cyber attack*

Motivasi	Peristiwa
Pengaruh geopolitik	Aktor-aktor yang disponsori negara kerap melakukan *cyberattack* untuk mendapatkan keuntungan strategis, mengganggu proses politik dan demokrasi, atau menggoyahkan pihak lawan. Tujuan para aktor bukan mencari keuntungan finansial, melainkan untuk membentuk opini, merusak reputasi, memberi pengaruh, menabur perselisihan, atau merancang agenda-agenda geopolitik tertentu.
Keyakinan ideologis	*Cyberattack* didorong oleh keyakinan ideologis atau agenda politik tertentu. Kelompok *hacktivist* misalnya, mayoritas melancarkan serangan untuk menarik perhatian terhadap isu sensitif agenda publik, mempengaruhi preferensi publik, atau mempromosikan tujuan tertentu.
Perang informasi	Di era digital, informasi adalah *the real power*. Dengan meretas sistem politik, para aktor/kelompok penyerang dapat memperoleh akses masuk ke informasi/data-data sensitif yang dapat digunakan untuk memeras publik, merusak reputasi institusi pelayanan publik dan lembaga-lembaga negara.
Demonstrasi kekuasaan	Beberapa serangan dilakukan hanya untuk menunjukkan kemampuan dunia maya kepada suatu kelompok atau negara. Ini adalah cara untuk menunjukkan kekuatan mereka, dan mengirimkan pesan yang jelas kepada lawan.

Sumber: Fernandes, 2023

Ruang Siber: Ranah Intevensi dan Rakayasa Politik

Dinamika politik dalam konteks relasi global (persaingan, perselisihan, konflik, dan peperangan) antar negara yang kian kompetitif telah memicu peningkatan perang siber di banyak negara. Studi kejahatan siber (*cyberattack*) sebagai bentuk serangan intervensi/rekayasa politik setidakya mengacu pada beberapa peristiwa politik di banyak negara di dunia, yang kemudian dipotret para ahli, seperti terekam dalam studi berikut:

Tabel 5. Studi Agresi Siber Sebagai Arena *Interplay* Politik di Level Global

Penulis/Topik Studi	Jenis Kajian	Temuan Penting
Aaron Shull (2014): *Global cybercrime: The interplay of politics and Law (internet governance papers)*	Laporan riset Center for International Governace Innovation (CIGI)	McAfee (perusahaan keamanan internet glo-bal) menemukan kasus kejahatan siber perusa-haan minyak Barat terhadap perusahaan mi-nyak yang beroperasi di Cina. *Cyber-attacks* Barat menggunakan teknik rekayasa informasi, *spear-phishing*, eksploitasi kerentanan sistem operasi Microsoft Windows, penyusupan ke Microsoft Active Directory, dan menggunakan alat transmisi administrasi jarak jauh (RAT) untuk mencuri data-data sensitif secara ilegal.
Tom Sorel (2015): *Human rights and hacktivism: The cases of Wikileaks and Anonymous*	Hasil riset ilmiah yang dipublikasi oleh *Journal of Human Rights Practice*.	Wikileaks dan Anonymous bukanlah kumpu-lan aktifitas dari entitas yang stabil. Aktifitas kedua kelompok ini cenderung fluktuatif, ber-ciri politis (tidak semata ekonomis); bersifat *hacktivism* (ekspresi pesan politik); mewakili banyak spektrum kelompok marjinal; bero-perasi secara bersamaan (simultan); dan dalam banyak kasus, Wikileaks kerap dipersepsi para pendukungnya sebagai gerakan moral yang membela hak asasi kelompok yang dirugikan.
Emily Goldman (2021): *Fresh thinking and new approaches are needed on diplomacy's newest frontier*	Kajian lepas yang dipu-blikasi oleh *majalah in-afa.com*	Kejahatan siber dan isu keamanan siber yang menguat dalam beberapa tahun terahir ini telah melecut signifikasi diplomasi siber untuk me-ngatasi dampak yang muncul dari *cybercrime*. Isu diplomasi siber mencakup berbagai topik keamanan, politik, ekonomi, sosial, dan isu hak asasi manusia termasuk standar keamanan siber internasional: akses internet, privasi, kebebasan internet, kekayaan intelektual, kejahatan dunia maya, konflik dan persaingan dunia maya yang disponsori negara, penggunaan teknologi digi-tal dan perdagangan yang etis. Isu perang siber telah menjadi arena utama persaingan strategis.
Dmitriy Lobach & Ser-gey Shestopa (2002): *Cyberattacks as a crime of aggression and international terrorism: legal qualification problems*	*Proceeding* Ilmiah yang dipublikasi oleh *euro-peanproceedings.com*	Tren modern dalam perkembangan hubungan internasional dan mempertimbangkan akselera-kemajuan ilmu pengetahuan dan teknologi saat ini menunjukkan serangan siber sebagai tindak kejahatan yang mengarah ke modus baru: poli-tik agresi dan terorisme global.
Brendan Kotze (2022): *Why politically motivated cyber-attacks are a threat to democracy*	Artikel lepas yang dipu-blikasi oleh *majalah in-fosecurity.com*	Pemerintah negara di dunia harus mampu men-desain sistem mitigasi informasi dan keamanan siber dari ancaman predatorik para "*hacker* politik" melalui penggunaan teknologi dan SDM yang tepat untuk mengantisipasi risiko potensi serangan siber yang dapat merusak ke-hidupan ekonomi, sistem politik, dan ketahanan demokrasi yang hari-hari ini terus menghadapi teror dari para *hacker* politik global.
Ani Petrosyan (2022):	Artikel lepas yang dipu-blikasi oleh situs lem-	Meningkatnya praktik digitalisasi data di dunia telah memposisikan AS sebagai target utama

U.S. government and cybercrime: Statistics & facts	baga penghimpun data *statista* (statista.com)	serangan politik dan ekonomi para *hacker* dari kelompok teroris, ekstremis, krimi-nal, dan para *hacker* global. Tahun 2018 pemerintah AS harus menanggung kerugian lebih dari 13,7 miliar US dolar akibat serangan siber.
Anita Lavorgna (2023): *Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology*	Hasil riset ilmiah yang dipublikasi oleh *Journal Trends in Organized Crime*	Dalam literatur kriminologi bentuk-bentuk kejahatan siber negara belum mendapat perhatian. *State crime* adalah aktifitas ilegal yang merugikan hak-hak politik warga negara yang diinisiai institusi siber milik negara. Tujuannya, untuk melindungi kepentingan politik dan bisnis para elite negara, mempengaruhi opini publik, dan mengonversi tuntutan publik menjadi dukungan publik melalui *cyber attack* dan pengendalian penuh (*surveillance*) informasi di ruang virtual.
Apurva Venkant (2023): *Cyberattacks against governments jumped 95% in last half of 2022*	Artikel lepas yang dipublikasi oleh website *csoonline.com*	*Cyber attack* pada situs-situs pemerintah melonjak tajam (naik 95%) pada paruh akhir tahun 2022, dibanding periode tahun 2021. Peningkatan *cyber-attack* dipicu oleh proses digitalisasi yang pesat sepanjang pandemi Covid-19. *Cyber attack*, ke depan, diprediksi akan makin meluas dan membuka jalan bagi eskalasi dan intensitas perang informasi, baik intra maupun ekstra *state actors* vs *non-state actors*.
Ray Fernandes (2023): *Hacking democracy: The cyber-attacks that shaped global politics*	Artikel lepas yang dipublikasi oleh website *moonlock.com*	Tekanan dan pengaruh geopolitik yang kian kompetitif telah membuat aktor-aktor yang disponsori negara seringkali melakukan serangan untuk memetik benefit strategis, mengganggu proses demokrasi, atau menggoyahkan stabilitas politik pihak lawan. Tujuan utama bukanlah keuntungan ekonomis atau finansial melainkan untuk menebar pengaruh, menabur perselisihan, atau memenangkan agenda geopolitik tertentu.

Sumber: Data diolah oleh penulis

Beberapa kasus serangan siber bermotif politik, diantaranya adalah kasus pilpres AS tahun 2016 mengalami ancaman serius serangan siber dan intervensi agen intelijen Rusia. Banyak bukti menunjukkan bagaimana intelijen Rusia (dan agen-agen *proxy*-nya) meretas dokumen hasil Konvensi Nasional Partai Demokrat dan membocorkan info sensitif untuk men-*down grade* integritas Hillary Clinton (capres yang diusung Partai Demokrat); menyebarkan berita palsu (*fake news*), menyusun informasi sesat (disinformasi), dan membangun propaganda (melalui saluran media konvensional dan media sosial) untuk memecah belah (segregasi) warga AS; dan men-*drive* preferensi pemilih AS dengan pemasangan ratusan iklan bertarget dan troll berbayar (Pope, 2018).

Kedua, kasus peretasan data pribadi milik Presiden Prancis dan dan email rahasia Partai La République en Marche tahun 2017. Lebih dari 20.000 email kampanye pemilu milik Partai République en Marche disebar secara online. Peretasan ponsel Macron dan

anggota kabinetnya oleh Pegasus (perusahaan perangkat lunak NSO Group milik Israel) memungkinkan Pegasus mengekstrak pesan, foto, email, panggilan seluler, dan aktivasi mikrofon dari ponsel milik Marcron dan anggota kabinetnya (Kotze, 2022).

Ketiga, kasus Wikileaks, situs berita milik Julian Assange ini ditengarai sering membocorkan data berbagai skandal politik di banyak negara, seperti serangan helikopter Apache milik AS kepada warga sipil Irak, dokumen rahasia operasi militer AS yang menyiksa para tahanan di Guantanamo, sindikat pemalsuan data perubahan iklim global di Unit Penelitian Iklim Universitas East Anglia (di Inggris), daftar internet hitam di Australia yang menjadi mitra (informan) pemerintah dan politisi Australia, Pusat Intelijen Siber CIA yang beranggotakan 200 orang dilaporkan ditugaskan sebagai spesialis digital untuk melakukan peretasan informasi rahasia milik pemerintah Rusia, Cina, Afghanistan, Iran, dan negara-negara musuh AS lainnya (Soren, 2015; The Guardian, 2017).

Kasus Peretasan Data Bermotif Politis

Teknologi siber, saat ini praktis telah digunakan untuk menyerang beragam aktifitas politik melalui situs web dan layanan online sebagai sarana politik karena menganggap metode politik konvensional (*lobby*, negosiasi, dan diplomasi) tidak lagi efektif digunakan sebagai alat *bargaining position*. Serangan siber bermotif politik saat ini digunakan banyak pihak sebagai senjata "perlawanan" (agresi) atau "pertahanan diri" (*defence*) untuk mengantisipasi serangan atau memberi ancaman pada negara lain. *Cyber-attacks* yang dilakukan para peretas mencakup perusakan situs web, pengungkapan situs web, serangan penolakan layanan (DoS) atau serangan penolakan layanan terdistribusi (DDoS), distribusi ransomeware/malware, pencurian/pembobolan data, dan sabotase. Semua taktik ini melibatkan akses ilegal ke sistem situs web atau data target. Anonymous dan Wikileaks misalnya, menargetkan berbagai lembaga swasta (perusahaan) dan institusi publik (sektor pelayanan masyarakat) karena berbagai alasan "politis" (Unodc, 2020).

Data di bawah mencatat berbagai insiden dunia maya dengan motif "politis" (baik yang berlangsung di level regional maupun global) yang terjadi sejak tahun 1998. Fokus yang menjadi target/sasaran serangan, antara lain: lembaga pemerintah, institusi bisnis, lembaga-lembaga ekonomi, sektor militer, sektor pertahanan, dan sektor intelijen.

Tabel 6. Data Kejahatan Siber di Tingkat Global (1998-2020)

Tahun	Peristiwa
1998	Penemuan virus baru bernama "Morris Worm" (salah satu virus berbahaya yang bisa membelah diri) oleh Robbert Morris yang di kemudian hari digunakan untuk menyerang jaringan infrastruktur komputer di AS secara massif. Morris Worm sukses menginfeksi

	komputer *host* (tempat penyimpanan data/server yang terhubung dalam jaringan) dan memperlambat performa komputer. Varian virus baru versi Morris ini adalah bentuk penyalahgunaan teknologi yang sangat membahayakan kepentingan pemerintah AS, terutama di sektor pertahanan dan keamanan.
2005	Sel-sel jejaring *hacker* Cina berhasil meretas jaringan komputer milik NASA yang ada di bawah pengelolaan Lockheed Martin. Peristiwa ini tercatat sebagai salah satu konspirasi terbesar intelijen Cina yang menargetkan fasilitas siber milik Departemen Pertahanan AS (yang sangat vital, strategis, dan sangat rahasia bagi pemerintah AS).
2006	▪ *Intelligence and Security Committee* (ISC) melaporkan para peretas yang disponsori Cina kerap menargetkan anggota parlemen Inggris sebagai sasaran serangan. Laporan menyimpulkan, pemerintah Inggris harus siap menghadapi risiko *national security* para *hacker* Cina, karena kemampuan para *hacker* Cina dan jaringan *proxy*-nya sangat canggih. Kapasitas mumpuni Cina itu dapat digunakan untuk melakukan serangan siber terhadap infrastruktur penting di Inggris setiap saat. ▪ Laporan NATO menyebutkan sepanjang tahun 2006, berbagai serangan siber telah dilakukan para *hacker* internasional yang menargetkan fasilitas siber pertahanan militer dan intelijen berbagai negara, terutama negara-negara di kawasan Eropa, Jepang, dan Australia yang menjadi anggota NATO.
2007	▪ Data *prototype* pesawat tempur rahasia F-35 dan proyek pesawat tempur dicuri oleh peretas Cina, diikuti dengan penutupan jaringan email Universitas Pertahanan Nasional di AS. Para peretas asing yang tidak dikenal banyak meninggalkan *spyware* dalam sistem jaringan komputer yang mereka retas. ▪ Pemerintah Estonia mempertahankan jaringan IT-nya setelah beberapa serangan dilakukan oleh *hacker* asing yang tidak dikenal. Agen intelijen Rusia dituding sebagai pelaku serangan. ▪ Kementerian Pertahanan AS (melalui jaringan Pentagon) menerima percobaan peretasan asing untuk mengeksploitasi *data base* melalui jaringan email yang tidak aman. Intelijen Rusia dan Cina dituding ada dibalik skenario serangan ini. ▪ Kementerian Keamanan Nasional Cina juga melaporkan, mencurigai jaringan peretas asal Taiwan dan AS melakukan *spywere* atau *cyber espionage* (menembus jaringan komputer sistem keamanan nasional pemerintah Cina).
2008	▪ Industri properti asal Amerika, Eropa, dan Jepang mengalami serangan siber yang menginfeksi jaringan TI properti dan bisnis mereka. Peretasan ini diduga adalah bagian dari kejahatan spionase industri dan kegiatan teror yang dilakukan para *hacker* yang berideologi "anti-Barat". ▪ Kelompok peretas yang berbasis di Shanghai yang terkait dengan departemen TI Tentara Rakyat Cina dituding menjadi otak pencurian informasi rahasia (pesan data surat elektronik beserta lampiran PDF) milik pemerintah AS. ▪ *Data base* milik Partai Demokrat dan Partai Republik di AS diretas oleh komunitas *hacker* asing. Para *hacker* juga melakukan serangan terhadap situs web milik pemerintah negara bagian Georgia. Pemerintah AS menuding peretas asal Rusia menjadi otak dan penggerak di balik serangan tersebut.
2009	Internet Israel diretas oleh oleh *hacker* profesional yang tidak dikenal. Pemerintah Israel secara resmi menuduh Hamas dan Hizbullah adalah pelaku dibalik serangan ini.
2010	Natanz dan instalasi nuklir Iran lainnya juga menjadi sasaran serangan siber melalui virus Stuxnet yang melumpuhkan sistem komputer di sejumlah instalasi nuklir Iran. Serangan dilakukan oleh AS dan Israel dengan nama sandi operasi "*Olympic Games*". Kasus ini merupakan salah satu serangan siber terbesar sepanjang tahun 2010.
2011	▪ Situs layanan *search engine* terbesar di China, Baidu.com, dilumpuhkan *cracker* asal Iran. Layanan Baidu.com dilaporkan sempat berhenti beroperasi akibat serangan itu. *Cracker* melakukan serangan *defacing* (mengganti wajah halaman muka situs Baidu.com dengan tulisan berbahasa Inggris yang berarti "Situs ini telah di-*hack* oleh Tentara Cyber Iran").

	▪ Terjadi serangan siber terhadap Google, Adobe, dan perusahaan online besar Barat lainnya yang dilakukan oleh peretas asing yang tidak dikenal dengan memanfaatkan celah keamanan dalam sistem bingkai *cyberwall*.
2012	▪ Serangan siber "Oktober Merah" pada tahun 2012 menargetkan beberapa negara bekas Uni Soviet, khususnya sistem TI pemerintahnya. Virus ini berhasil mengumpulkan data sensitif dan vital tentang pangkalan militer, kedutaan besar, proyek penelitian pemerintah, sistem nuklir, dan basis data infrastruktur lainnya. ▪ Pemimpin Spiritual Iran, Ayatollah Ali Khamenei, pada Maret 2012, membentuk Dewan Tertinggi Siber (*Supreme Council of Cyberspace*) yang mewadahi lembaga-lembaga siber di Iran, dengan dua tugas pokok: tugas pertahanan dan tugas penyerangan. Tugas pertahanan adalah melindungi infrastruktur proyek-proyek strategis, terutama proyek nuklir Iran. Sementara tugas penyerangan melancarkan serangan siber balik atas serangan siber dari musuh-musuh Iran.
2013	▪ Para pemimpin NATO untuk pertama kalinya mengadakan pertemuan darurat untuk membahas masalah keamanan siber dan sepakat untuk membentuk Aliansi Pertahanan Siber NATO yang secara kontinu mendapat serangan siber. Tujuan pertemuan adalah untuk menyiapkan teknologi siber yang mampu melakukan serangan balik dan mencegah hilangnya data penting dan rahasisa milik NATO. ▪ NATO meningkatkan aliansi strategis dengan berbagai organ *cybersecurity* global untuk melawan serangan siber melalui implementasi "*NATO Computer Incident Response Capability (NCIRC)*" yang bernilai lebih dari 58 juta Euro.
2014	▪ Departemen Kehakiman Amerika mendakwa empat orang mata-mata Rusia yang diduga kuat mencuri informasi pribadi jutaan orang dalam kasus peretasan Yahoo tahun 2014. Pemerintah Rusia menyatakan tidak terlibat dalam aktifitas *cyber ilegal* apapun termasuk keterlibatan Dinas Keamanan Federal Rusia (FSB). ▪ Peretasan data Sony Pictures Entertainment oleh kelompok yang meng-*claim* diri sebagai "Penjaga Perdamaian Dunia". Para peretas yang disinyalir sebagai *proxy* dari agen intelijen Korea Utara (RGB) mencuri sejumlah besar informasi penting dari jaringan komputer milik Sony.
2015	Pemerintah Rusia membentuk "Divisi Siber" untuk melakukan *cyber attack* sektor ketenagalistrikan milik pemerintah Ukraina untuk tujuan spionase dan pengendalian infrastruktur penting Ukrainia, seperti jaringan tenaga listrik, sistem angkutan massal perkotaan, lalu lintas udara serta jaringan distribusi minyak dan gas Ukraina.
2016	▪ Microsoft mendeteksi peretasan yang menargetkan lembaga pemerintah (termasuk badan intelijen), pusat penelitian pertahanan, dan penyedia layanan telekomunikasi di Asia Selatan dan Asia Tenggara sejak 2009. ▪ Campur tangan Rusia dalam Pilpres AS 2016 melalui badan intelijen militer Rusia (GRU). CIA dan FBI menuduh GRU berada dibalik peretasan data milik tim pemenangan Hillary Clinton untuk tujuan "*black campaign*", memecah konsentrasi pendukung Hillary, dan membentuk opini untuk pemenangan Donald Trump. ▪ Perangkat lunak dan data Yahoo diretas, dimana 500 juta data pengguna Yahoo telah dicuri dan disusupi. Peretas dilaporkan memiliki motif politis (*hacktivism*). ▪ Yahoo melaporkan peretasan dan mengungkap ada 500 juta data penggunnya telah dicuri oleh kelompok *hacker* yang di-*back up* oleh suatu negara. Data pengguna Yahoo yang diretas antara lain: nama, nomor telpon, kata sandi, dan email.
2017	▪ Serangan ransomware WannaCry telah menginfeksi lebih dari 230.000 komputer di 150 negara di dunia, mengakibatkan kerugian ekonomi lebih dari 4 miliar US dolar, dan menimbulkan dampak serius di sektor pendidikan, layanan publik pemerintah, keuangan, kesehatan, dan sektor layanan publik lainnya. ▪ Pada 2017, pemerintah situs dan jaringan pemerintah Arab Saudi dan sektor energinya diserang oleh serangan siber yang diinisiasi agen rahasia Iran. ▪ Pada tahun 2017, kampanye *spyware* yang didukung suatu negara yang tidak diketahui menyerang jaringan militer dan pemerintah India dan Pakistan.

2019-2020	▪ Jaringan industri hotel AS diretas oleh peretas asal Cina yang menyebabkan lebih dari 500 juta data pelanggan hotel dicuri. ▪ Dewan Keamanan PBB pada 2019 mengungkapkan bahwa Korea Utara melalui jaringan siber ilegalnya mencoba mencuri 670 juta US dolar dalam mata uang kripto antara 2015 hingga 2018. ▪ Pada 2019, *data base* pemilih pemilu legislatif dan presiden Indonesia diretas oleh aktor yang berasal dari China dan Rusia. ▪ Kementerian luar negeri Australia mendapat serang siber pada Januari 2020 selama beberapa minggu. ▪ Akun staf WHO dicoba diretas oleh peretas Iran di tengah pandemi Covid-19.
2021	Pemerintah Iran secara resmi menuduh Israel berada di balik sabotase terhadap instalasi nuklir Natanz. Sabotasi melalui serangan siber melalui jaringan komputer ini telah menyebabkan putusnya aliran listrik di instalasi nuklir tersebut. Serangan siber Israel ini adalah bagian dari rangkaian panjang pertarungan siber antara Iran dan Israel yang telah berlangsung selama satu dekade terakhir ini.
2022	Pemerintah AS, melalui Jaksa Agung Merrick B. Garland, menghapus malware Rusia dari jaringan komputer di seluruh dunia. Tindakan ini dilakukan AS agar malware yang dikirim para peretas Rusia tersebut tidak digunakan untuk memonitor, menciptakan botnet yang dikendalikan, dan merusak sistem jaringan komputer golbal.
2023	▪ Peretas yang terkait dengan Israel (jaringan *hacker proxy* Israel) meretas 70% jaringan komputer pengaturan pompa bensin di Iran sebagai balasan atas tindakan agresi Iran dan proksinya di wilayah Israel. Pemerintah Iran menunding Israel dan AS berada dibalik serangan itu jaringan komputer milik Iran itu. ▪ Peretas Rusia menyerang penyedia telepon seluler terbesar di Ukraina, Kyivstar, menonaktifkan akses ke 24 juta pelanggannya di Ukraina. Peretas mengklaim telah menghancurkan lebih dari 10.000 komputer dan 4.000 server, termasuk penyimpanan *cloud* dan sistem cadangan. Serangan itu dimulai beberapa jam sebelum Presiden Zelensky bertemu dengan Presiden Biden di Washington DC.
2024	▪ Peretas Rusia melancarkan serangan ransomware/malware terhadap penyedia layanan digital di Swedia untuk layanan pemerintah. Serangan itu mempengaruhi operasi 120 kantor pemerintah (termasuk industri perbankan dan keuangan). Serangan ini terjadi ketika Swedia bersiap untuk bergabung dengan NATO. ▪ Peretas Rusia menyerang 65 departemen dan lembaga pemerintah Australia dan mencuri 2,5 juta dokumen dalam serangan siber terbesar di Australia. Peretas menyusup ke firma hukum Australia yang bekerja sama dengan oknum-oknum pemerintah untuk mendapatkan akses ke berbagai file milik pemerintah.

Sumber: Data diolah oleh penulis

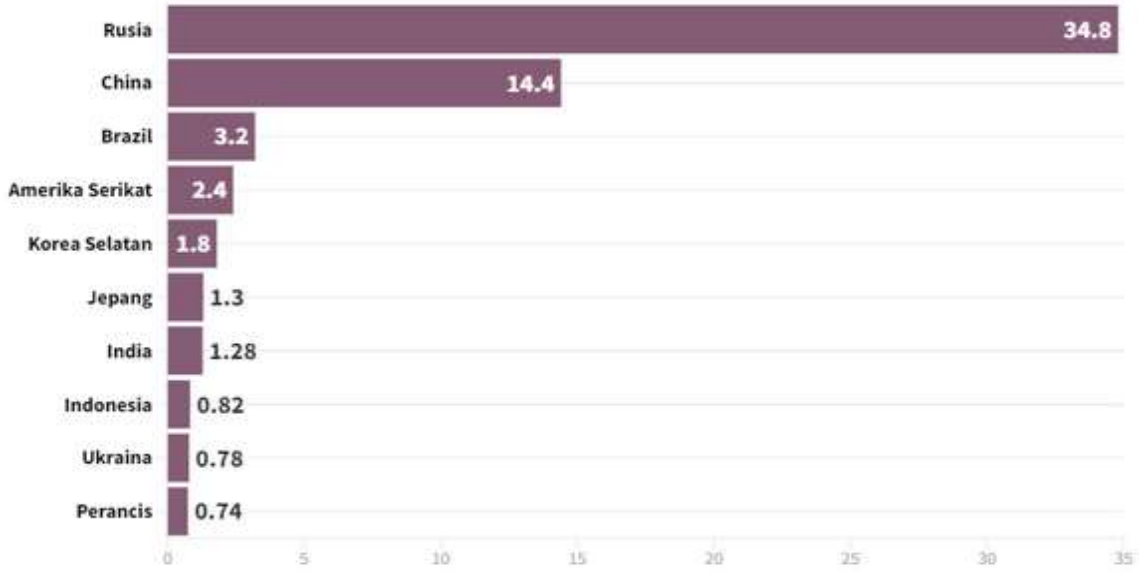
Indonesia, mengutip laporan Shurfshark (industri keamanan siber yang berbasis di Balanda), adalah negara *high risk* terkait pembobolan data cukup tinggi. Data Shurfshark menyebut, Indonesia menempati posisi 10 negara di dunia dengan tingkat kebocoran data pribadi tertinggi. Kebocoran data pada kuartal II/2022 bahkan mengalami kenaikan sebesar 143 persen dari kuartal I/2022 (*quarter to quarter*). Sejak tahun 2004, total kasus kebocoran data di Indonesia sudah mencapai angka 120,9 juta (lhat grafik 3).

Senada dengan laporan Shurfshark, laporan ASEAN Cyberthreat 2021 juga menyebut Indonesia berada di posisi cukup riskan di antara negara-negara ASEAN. Indonesia sering menjadi korban serangan ransomware/malware dengan 1,3 juta kasus. Jumlah tersebut hampir setengah dari total keseluruhan ancaman ransomware/malware di

antara negara-negara ASEAN. Vietnam berada di urutan kedua dengan 886.874 kasus, dan Brunei menjadi yang terendah dengan 257 kasus. Sementara laporan terbaru yang dirilis oleh National Cyber Security Index (NCSI) menunjukkan keamanan siber Indonesia berada di peringkat ke-6 di antara negara- negara ASEAN lainnya; atau urutan ke 83 dari 160 negara secara global (lihat tabel 7) (CNN Indonesia, 2022).

Data Shurfshark dan ASEAN Cyberthreat relevan dengan studi yang dilakukan Digital Readliness Index (lembaga pengukuran indeks digital yang berpusat di Australia) yang mengukur kesiapan digital di 146 negara berdasarkan tujuh indikator besar: (1) tingkat pemenuhan kebutuhan dasar masyarakat; (2) investasi pemerintah dan swasta di sektor teknologi; (3) kemudahan berbisnis; (4) kualitas sumber daya manusia; (5) iklim usaha rintisan (*start-up*); (6) tingkat adopsi (dan inovasi) teknologi digital; (7) kondisi infrastruktur digital di setiap negara (lihat tabel 8) (katadata.co.id, 2023).

Grafik 3. Negara Dengan Tingkat Kebocoran Data Tertinggi (Kuartal II/2022)



Sumber: Naurah, 2022

Tabel 7. Indeks Keamanan Siber di Negara-Negara Asia Tenggara (2020)

No.	Negara	Nilai / Skor
1	Malaysia	79,22
2	Singapura	71,43
3	Thailand	63,94
4	Filipina	63,64
5	Brunai Darussalam	41,56
6	Indonesia	38,96
7	Vientam	36,36
8	Laos	18,18

9	Kamboja	[redacted]	15,58
10	Myanmar	[redacted]	10,39

Sumber: katadata.co.id, 2022

Tabel 8. Skor Indeks Digital Negara Asia Tenggara

No.	Nama Negara	Nilai/Poin (Skala -2,5 – 2,5)	Status
1	Singapura	2,37	High readiness
2	Malaysia	0,46	Ready
3	Thailand	0,32	Ready
4	Vietnam	0,22	Ready
5	Indonesia	- 0,06	Not ready
6	Filipina	- 0,25	Not ready
7	Kamboja	- 0,38	Not ready
8	Timor Leste	- 0,80	Not ready
9	Myanmar	- 0,85	Not ready
10	Laos	- 0,89	Not ready

Sumber: katadata.co.id, 2023

Di Indonesia, isu serangan siber pada hingga kini masih menjadi problem serius. Kasus peretasan data yang bertendensi politis juga tak kalah marak, diantaranya peretasan dokumen surat menyurat milik Presiden Jokowi dengan Badan Intelijen Negara (BIN) antara tahun 2019-2021 berlabel rahasia (total ada 679.180 data yang diretas) oleh *hacker* berinisial Bjorka; peretasan data 10 kementerian dan lembaga (K/L) oleh *hacker* Mustang Panda Group (asal Cina); peretasan halaman muka situs (*defacement*) Badan Siber dan Sandi Negara (BSSN); dan kebocoran data Badan Intelijen Negara (BIN) oleh *hacker* dari kelompok Strovian di situs breached.to yang berhasil meretas data personil BIN berisi nama, tempat tanggal lahir, pangkat/golongan, dan jabatan fungsional agen intelijen.

Contoh lain adalah serangan siber yang dialami institusi layanan publik milik pemerintah dan swasta, seperti pencurian data pemegang kartu BPJS Ketenagakerjaan, BPJS Kesehatan, pengguna aplikasi e-HAC Kementerian Kesehatan, data nasabah Bank Syariah Indonesia, data pengguna MyIndiHome, data nasabah BRI Life, dan data WNI pemegang paspor. Jauh sebelumnya, di tahun 2014, juga terjadi pencurian 2,3 data kependudukan pada Daftar Pemilih Tetap (DPT) Pemilu yang tersimpan di *data base* milik KPU (Tamtomo & Galih, 2022; Widi, 2023).

Tabel 9. Berbagai Kasus Kebocoran Data DPT Pemilih

Bulan/Tahun	Keterangan
September, 2020	105 juta data DPT Pemilu KPU bocor di Internet. Kebocoran ini diungkap akun @underthebreach pada Kamis 21 Mei 2020. Data DPT Pemilu yang diretas dibagikan di komunitas *hacker* yang men-*share* tayangan gambar sebagai info

	bahwa peretas memiliki 2,3 juta data DPT Pemilu 2014. *Hacker* juga meng-*claim* masih memiliki 200 juta data WNI yang akan di-*share* di forum tersebut.
Mei, 2022	Jutaan data WNI yang bersumber dari DPT Pemilu 2014 bocor di internet. Meski data yang tersebar baru 2,3 juta, sang *hacker* mengaku memiliki 200 juta data yang akan disebar. Data dibagikan di forum raidxxx.com pada Rabu, 20 Mei 2020 oleh akun berinisial Arlinst sebanyak 2,3 juta, dimana DPT berasal dari Provinsi DIY yang berisi nama, tempat/tanggal lahir, NIK, dan alamat. Data tersebut tidak bisa di *download* gratis; harus ditukar dengan 8 credit atau setara dengan 8 euro.
September, 2022	Pada 6 September 2022, diduga kembali terjadi peretasan data, dimana lebih dari 105 juta data dijual oleh *hacker* berinisial Bjorka di laman Breached Forums yang diduga berasal dari KPU dengan judul "*Indonesia Citizenship Data Base From KPU 105M*". Bjorka mengklaim menyimpan 105.003.428 juta data lengkap penduduk Indonesia (seperti nama, NIK, kartu keluarga, tempat tanggal lahir, jenis kelamin, dan umur). Data pribadi itu dijual dengan harga US$5 ribu atau setara Rp 7,4 juta (US$1 = Rp 14.898,20). Semua data tersebut disimpan dalam file 20GB (*uncompressed*) atau 4GB (*compressed*).
November, 2023	Dugaan kebocoran data penduduk Indonesia kembali terjadi di penghujung tahun 2023. Data DPT Pemilu 2024 yang dikelola KPU telah diretas oleh akun anonim "Jimbo". Sebanyak 204 juta data yang diretas dari *website* KPU akan yang akan dijual Jimbo adalah DPT dari 514 kabupaten/kota dan 128 negara perwakilan senilai US$74 ribu (Rp 1,14 miliar). Data yang diretas mulai dari NIK, nomor kartu keluarga, nomor KTP, nomor paspor (untuk pemilih luar negeri), nama lengkap, jenis kelamin, tanggal lahir, tempat lahir, status pernikahan, dan alamat tinggal (lengkap dengan RT, RW, kode kelurahan, kecamatan, dan kabupaten sampai kode TPS). Sebagai bukti peretasan, Jimbo membagikan 500 sampel yang diunggah dalam situs darkweb Breach Forums.

Sumber: Data diolah dari berbagai sumber

Dalam konteks integritas politik dan legitimasi demokrasi, kebocoran data DPT Pemilu yang terus berulang tentu akan berimbas pada tergerusnya legitimasi politik pemerintah dan merosotnya integritas Komisi Pemilihan Umum (KPU). Kebocoran data DPT Pemilu jelas bukanlah hal sepele, apalagi jika kebocoran itu terjadi di masa-masa menjelang pemilu 2024 yang menjadi periode panas dan sensitif. Tak berlebihan jika publik khawatir modus seperti ini bisa "dimainkan" pihak-pihak tertentu untuk mengubah hasil rekapitulasi suara pemilu. Jika hal itu terjadi, pesta demokrasi akan dianggap ilegal, memicu gelombang protes massa, bahkan bisa memantik kericuhan politik nasional.

Fenomena kebocoran data yang terus terjadi di Indonesia setidaknya mengonfirmasi fakta, bahwa antisipasi serangan siber dan perlindungan data belum sepenuhnya menjadi prioritas pemerintah. Padahal, fakta kejahatan digital jauh sebelum berbagai kasus serangan siber dan pencurian data publik terjadi telah dipetakan oleh European Data Protection Supervisor (2019), dimana setiap negara diwajibkan untuk memperkuat sistem digitalnya guna menganstipasi dampak negatif yang bersumber dari lingkungan teknologi digital, seperti proteksi jaringan komputer, aplikasi perangkat lunak, sistem kritis, dan perlindungan data dari potensi ancaman tindak kejahatan digital. Riset akademis Pippa Norris (2020) dan Stephen Dawson (2023), juga telah mengingatkan bawah fenomena

serangan siber global yang eksis saat ini tak hanya berurusan dengan kejahatan bermotif semata ekonomi/finansial, namun ia telah bermetamorfosis menjadi tren kejahatan siber bermotif politik yang bisa merusak tatanan kehidupan politik, hukum, dan demokrasi.

SIMPULAN

Hasil analisis kajian menunjukkan, perkembangan internet dan masifnya migrasi pengguna internet praktis telah mengubah sistem, tatanan, *landscape*, dan kesadaran manusia untuk mengintegrasikan diri ke dalam tata nilai baru, termasuk dalam tata nilai kehidupan politik, hukum, dan demokrasi. Tren ancaman serangan siber akan terus menguat sejalan dengan perkembangan TI. Saat ini, serangan siber tak hanya menyasar sektor bisnis, namun juga sektor politik serta sektor pertahanan dan kemananan negara. Mengantisipasi hal itu, konsep *cybersecurity* saat ini telah diarahkan untuk menjaga kepentingan nasional (*cyberdefence*) melalui strategi *cyberwar* dan *cyberdiplomacy* guna mengatasi ancaman kejahatan siber yang kian intens dan terus bergerak liar.

Perkembangan teknologi digital akan selalu diikuti oleh peningkatan kejahatan pencurian data dan ruang kerentanan perlindungan data terkait proteksi data warga negara yang menjadi tanggung jawab pemerintah sebagai titik sentral krusial. Masalah keamanan siber menjadi tanggung jawab negara justru diarahkan untuk mendelegitimasi kontrol negara atas hegemoni teknologi siber yang menggejala di hampir seluruh negara di dunia.

Dalam Undang-Undang No. 3 Tahun 2002 tentang Pertahanan Negara, ancaman pertahanan negara terdiri dari ancaman militer dan ancaman non militer, termasuk ancaman serangan siber. Jika pemerintah gagal mengantisipasi *cybercrime*, maka bisa dipastikan eskalasi kejahatan siber di Indonesia akan kian intens dan meluas. Potensi ini tentu bisa mengancam kedaulatan negara dan keselamatan bangsa. Sebagai upaya antisipatif mengatasi kejahatan *cyber-attack* ini, pemerintah merumuskan kembali agenda dan upaya ekstra untuk membangun institusi siber nasional yang sanggup menjaga postur siber nasional (*cyber defence*) dari ancaman tindak kejahatan dunia maya (*cybercrime*).

DAFTAR PUSTAKA

Annual Report: European Data Protection Supervisor, 2019 (2020, January 17). Diakses dari https://edps.europa.eu/sites/edp/files/publication/2020-03-17_annual_report_2020_en_0.pdf.

Annur, C. M. (2023, February 03). *Jumlah Pengguna Internet Global Tembus 5,6 Milyar Orang pada Januari 2023*. Diakses dari https://databoks.katadata.co.id/datapublish/2023/02/03/jumlah-pengguna-internet-global-tembus-516-miliar-orang-pada-januari-2023.

Arief, B. N. (2006). *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: PT. RajaGrafindo Persada.

bbc.com (2022, September 12). *Bjorka Klaim Retas Dokumen Presiden Jokowi, Pemerintah Bentuk Satgas dan Ungkap Motif*. Diakses dari https://www.bbc.com/indonesia/indonesia-62870532.

Blank, S. (2013). Russian information warfare as domestic counterinsurgency. *American Foreign Policy Interests*, *35*(1), 31–44. DOI: 10.1080/10803920.2013.757946.

Chen, S., et.al. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Science Communication*, *10*(71), 1-10. https://doi.org/10.1057/s41599-023-01560-x.

Choucri, N. (2012). *Cyberpolitics in international relations*. Cambridge: MIT Press.

Chivers, T. (2019, April 12). *Wikileaks' 11 Greatest Stories*. Diakses dari https://www.telegraph.co.uk/news/0/wikileaks-greatest-ever-stories-scandals/

CNN Indonesia (2022, July 01). *RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan*. Diakses dari https:/www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan.

CSIS (2022). *Significant Cyber Incidents*. Diakses dari https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

"Cybercrime". Diakses dari https://www.merriam-webster.com/dictionary/cybercrime.

Dawson, S. (2022) Electoral fraud and the paradox of political competition. *Journal of Elections, Public Opinion and Parties*, *32*(4), 793-812. https://doi.org/10.1080/17457289.2020. 1740716.

Dennis, M. A. (2024, January 31). "Cybercrime". Diakses dari https://www.britannica.com/topic/cybercrime.

Dihni, V. A. (2022, March 07). *Keamanan Siber Indonesia Peringkat ke-6 di Asia Tenggara*. Diakses dari https://databoks.katadata.co.id/datapublish/2022/03/07/keamanan-siber-indonesia-peringkat-ke-6-di-asia-tenggara.

Dragan, A. T. (2018). Child pornography and child abuse in cyberspace. *Journal of Legal Studies*, *21*(35), 52-60. http://dx.doi.org/10.1515/jles-2018-0004.

Fernandes, R (2023, August 07). *Hacking Democracy: The Cyberattacks that Shaped Global Politics*. Diakses dari https://moonlock.com/political-cyberattacks.

Fuady, M. E. (2005). Cybercrime: Fenomena kejahatan melalui internet di Indonesia. *MediaTor*, *6*(2), 255-264. https://doi.org/10.29313/mediator.v6i2.1194.

Fernandez, R. (2023). *Hacking Democracy: The Cyberattacks that Shaped Global Politics*. Diakses dari https://moonlock.com/political-cyberattacks

Gandhi, R. A., et al. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and politics. *IEEE Technology and Society Magazine*, *30*(1), 28-38. DOI: 10.1109/MTS.2011.940293.

Goldman, E. O. (2021). "Fresh Thinking and New Approaches are Needed on Diplomacy's Newest Frontier". Article in *The Foreigh Service Jorunal* (June Edition, 2021). p. 21-25.

Graham, R. S. (2017, October 19). *The Difference Between Cybersecurity and Cybercrime, and Why it Matters*. Diakses dari https://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654.

Hill, E., et al. (2017). Explaining electoral fraud in an advanced democracy: Fraud vulnerabilities, opportunities, and facilitating mechanisms in British elections. *The British Journal of Politics and International Relations*, *19*(4), 772-789. https://doi.org/10.1177/1369148117715222.

Internet Complaint Crime Center (2020). *Internet Crime Report* 2020. Diakses dari https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

Jose, H. S (2021). Politisasi agenda keamanan siber pada era Industri 4.0 di forum multilateral. *Populika*, 9(2), 70-85. https://doi.org/10.37631/populika.v9i2.390.

Kotze, B. (2022, January 10). *Why Politically Motivated Cyber-Attacks Are a Threat to Democracy*. Diakses dari https://www.infosecurity-magazine.com/opinions/politically-motivated-cyber/

Lavorgna, A. (2023). Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology: *Journal Trends in Organized Crime* (in Spirnger Link). https://doi.org/10.1007/s12117-023-09486-1.

Muhammad, N. (2023, September 20). *Indeks Kesiapan Digital Asia Tenggara*, *Skor Indonesia Tergolong Rendah*. In https://databoks.katadata.co.id/datapublish/2023/09/20/indeks-kesiapan-digital-asia-tenggara-skor-indonesia-tergolong-rendah.

Munk, T. (2022). *The rise of politically motivated cyber attacks: Actors, attacks and cybersecurity*. New York, NY: Routledge.

Munn, R., & Turne, M. (2021, December 02). *Politically Motivated Ransomware Attacks: Science Fiction or Reality?* Diakses dari https://securingdemocracy.gmfus.org/politically-motivated-ransomware-attacks/

Naurah, N. (2022, November 21). *Meninjau Tingkat Kasus Kebocoran Data Global*, *Apakah RI Aman*? Diakses dari https://goodstats.id/article/meninjau-tingkat-kasus-kebocoran-data-global-apakah-ri-aman-gsBoq.

NATO (2023, September 14). *Cyber Defence*. Diakses dari https://www.nato.int/cps/en/natohq/topics_78170.htm.

Norris, P. (2020) *Electoral Integrity in the 2020 U.S. Elections*. Diakses dari PEI-US-2020-Report-(Electoral_Integrity).pdf.

Petrosyan, A. (2022, July 06). *U.S. Government and Cybercrime: Statistics & Facts*. Diakses dari https://www.statista.com/topics/3387/us-government-and-cyber-crime/#topicOverview.

Pope, A. E. (2018). Cyber-securing our elections. *Journal of Cyber Policy*, *3*(1), 24-38. DOI: 10.1080/23738871.2018.1473887.

Priya, A. (2021) Case study methodology of qualitative research: Key attributes and navigating the conundrums in its application. *Sociological Bulletin*, *70*(1), 94-110. https://doi.org/10.1177/0038022920970318.

Purnamasari, D. W. (2022, September 09) *Dugaan Kebocoran Data BIN dan Rencana Peretasan Data Presiden Dinilai Ancam Kedaulatan Negara*. Diakses dari https://www.kompas.id/baca/polhuk/2022/09/09/dugaan-kebocoran-data-pegawai-bin-hingga-rencana-peretasan-data-presiden-ancam-kedaulatan-negara.

Ramadhan, A., & Asril, S. (2022, September 12). *Ulah Hacker Bjorka Bobol Data Surat Jokowi hingga Ancaman Dijerat Pidana*. Diakses dari https://nasional. kompas.com/read/2022/09/12/08223431/ulah-hacker-bjorka-bobol-data-surat-jokowi-hingga-ancaman-dijerat-pidana?page=all.

Sandrawati, N. A. (2022). Antisipasi cybercrime dan kesenjangan digital dalam penerapan TIK di KPU. *Electoral Governance: Jurnal Tata Kelola Pemilu Indonesia*, *3*(2), 138-159. https://doi.org/10.46874/tkp.v3i2.655.

Sentinelone.com (t.t). *What Is A Threat Actor? Types & Examples of Cyber Threat Actors*. Diakses dari https://www.sentinelone.com/cybersecurity-101/threat-actor/

Shinder, L., & Cross, M. (2008). *Understanding the People on the Scene*. Diakses dari https://www.sciencedirect.com/topics/computer-science/cybercriminals#:~:text= Politically-motivated-cybercriminals-include-members,coordinate-their-"real-world".

Shull, A. (2014). *Global Cybercrime: The Interplay of Politics and Law* (*Internet Governance Papers*, Number 8, June 2014). Diakses dari https://www.cigionline.org/static/documents/no8_1.pdf.

Siregar, H. R. (2023, November 30) *Data DPT di KPU Bocor Akibat Celah Internal*. Diakses dari https://newsletter.tempo.co/read/1803327/data-dpt-di-kpu-bocor-akibat-celah-internal.

Sorel, T. (2015). Human rights and hacktivism: The cases of Wikileaks and Anonymous. *Journal of Human Rights Practice*, *7*(3), 391–410. https://doi.org/10.1093/jhuman/huv012.

Tamtomo, A. B., & Galih, B. (2022, August 09) *Infografik: Kasus-kasus Besar Kebocoran Data Pribadi di Indonesia*. Diakses dari https://www.kompas.com/ cekfakta/read/ 2022/09/08/101500782/ infografik--kasus-kasus-besar-kebocoran-data-pribadi-di-indonesia.

The Guardian (2017, March 07). *WikiLeaks Publishes 'Biggest Ever Leak of Secret CIA Documents*. Diakses dari https://www.theguardian.com/media/2017/mar/07/ wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance.

UNODC (2020). *Ancaman Kejahatan Dunia Maya Darknet ke Asia Tenggara (Laporan Badan PBB Untuk Urusan Narkoba dan Kejahatan)*. Diakses dari https://www.unodc.org/roseap/uploads/documents/Publications/2022/Darknet_report_Indonesia_Bahasa.pdf

US Departement of Justice [Office of Public Affairs] (2020, September 10). *Russian Project Lakhta Member Charged with Wire Fraud Conspiracy*. Diakses dari hhttps://www.justice.gov/opa/pr/russian-project-lakhta-member-charged-wire-fraud-conspiracy.

Venkant, A. (2023, January 04). *Cyberattacks Against Governments Jumped 95% in Last Half of 2022, Cloudsek Says*. Diakses dari https://www.csoonline.com/article/574275/cyberattacks-against-governments-jumped-95-in-last-half-of-2022-cloudsek-says.html.

Widi, S. (2023, July 06) *Deret Kasus Kebocoran Data RI pada 2023, dari BSI hingga Paspor*. In https://dataindonesia.id/internet/detail/deret-kasus-kebocoran-data-ri-pada-2023-dari-bsi-hingga-paspor.

Widodo (2009). *Sistem pemidanaan dalam cyber crime*. Yogyakarta: LaksBang Mediatama.