Potensi Ancaman Cyber Crime di Pemilu Serentak 2024 di Indonesia

Oleh
Juni Thamrin dan Sumarno
Dosen Fakultas Ekonomi Bisnis Universitas Bhayangkara Jakarta
dan Pusat Kajian Keamanan Nasional Universitas Bhayangkara Jakarta

Abstraksi

Kajian ini memberikan perhatian pada ancaman cybercrime terhadap pemilu serentak yang akan dilaksanakan pada tahun 2024. Ancaman tersebut akan dapat mengganggu hasil pemilu dan akan menimbulkan gangguan terhadap hilangnya kepercayaan publik akan siklus demokrasi yang pada ujungnya dapat menimbulkan bencana sosial politik dalam perjalanan negara dan bangsa di masa mendatang. Berdasarkan pengalaman banyak negara, digitalisasi dan penggunaan IT dalam proses pemilu sudah merupakan keniscayaan, sehingga penyelenggara pemilu harus didukung dengan mekanisme keamanan yang sistematis terhadap ancaman serangan cyber.

Kata kunci: Cybercrime, Pemilu Serentak, Demokrasi, Keamanan Nasional

Abstraction

This review is having pays attention to the threat of cybercrime against the Indonesian's simultaneous elections which will be held in year 2024. This threat will be able to disrupt the election results and will cause disruption to the loss of public confidence in the democratic cycle which in the end can cause a socio-political disaster and in the end of the day can destroying the life of country. Based on the experience of many countries, digitalization and the use of IT in the election process is a necessity, so election organizers must be supported by a systematic security mechanism against the threat of cyber-attacks.

Keyword: Cybercrime, Simultaneous Elections, Democration, National Security

I. Pendahuluan

Pemilihan umum serentak pada tahun 2024 merupakan sebuah tonggak bersejarah bagi bangsa dan negara Indonesia. Peristiwa itu akan menjadi penentu arah selanjutnya dalam perjalanan negara ini kedepannya. Sehingga, peristiwa sejarah itu bukan berarti merupakan peristiwa yang otomatis akan terbebas dari ancaman dan gangguan. Saat kini, ancaman yang dapat mengganggu bahkan menggagalkan penyelenggaraan dan hasil penting dari "pesta rakyat" tersebut adalah gangguan serangan *cyber* (Wibowo dan Harimurti, 2021).

Dalam konteks demokrasi, pemilihan umum adalah manifestasi tertinggi dari suara rakyat dalam memilih pemimpin dan arah kebijakan negara. Namun, di tengah pesatnya perkembangan teknologi informasi, pemilu tidak hanya menciptakan peluang demokrasi, tetapi juga menjadi target utama bagi ancaman keamanan *cybercrime*. Pada era dimana hampir seluruh proses pemilu didigitalisasi, risiko keamanan *cyber* mengemuka sebagai ancaman yang harus mendapat perhatian serius semua pihak (Siburian BSSN, 2023; KPU, 2023 dan Caldarudo, *et.all*, 2022).

Ancaman *cybercrime* pada pemilu tidak hanya merusak integritas proses pemilihan, tetapi juga dapat menggoyahkan sendi kepercayaan masyarakat terhadap hasil pemilu dan stabilitas politik. Kasus-kasus serangan siber pada pemilu di berbagai negara telah memicu keraguan publik dan menimbulkan kerusakan yang serius terhadap sistem demokrasi. Lebih lanjut dapat menimbulkan kekacauan politik dan negara kehilangan legalitas atas hasil pemilu yang dapatkannya. Lebih lanjut Tantowi[1] (2021) menyatakan bahwa: *"KPU tentu harus mempertimbangan keamanan siber menjadi aspek penting yang perlu dikelola dalam mengadopsi teknologi informasi yang akan diterapkan untuk memastikan seluruh sistem yang digunakan terjamin keamanannya serta tidak menimbulkan kerugian bagi salah satu pihak. Semua ini dilakukan dalam rangka meningkatkan kepercayaan peserta dan publik terhadap hasil-hasil pemilu".*

Kajian ini bertujuan untuk menganalisis dan memahami ancaman *cybercrime* yang mungkin muncul pada Pemilu Serentak 2024. Kajian ini akan mengidentifikasi jenis-jenis ancaman yang potensial, motivasi pelaku, serta dampak-dampaknya terhadap proses pemilihan dan kepercayaan masyarakat. Selain itu, kajian ini juga akan mengidentifikasi upaya pencegahan dan perlindungan yang dapat diambil oleh pemerintah, lembaga terkait, dan masyarakat untuk mengurangi risiko ancaman *cybercrime* pada pemilu.

Sebagai sebuah negara yang besar seperti Indonesia, saat ini sudah menjadi keniscayaan dalam penggunaan IT sebagai

1 Anggota KPU RI, Pramono Ubaid Tantowi, dalam sambutannya menyampaikan kemajuan teknologi informasi saat ini merupakan sesuatu yang tidak dapat dinafikan. Telah banyak teknologi informasi yang diterapkan dalam tahapan pemilu, semata-mata untuk mempermudah dan menyederhanakan kerja KPU dalam mengelola setiap tahapan. Sangatlah tidak mungkin apabila KPU sebagai penyelenggara pemilu tidak menggunakan teknologi informasi dalam setiap tahapannya, mengingat kerja pemilu di Indonesia sangat kolosal dengan beban kerja yang besar. Dengan perkembangan teknologi informasi yang pesat, isu keamanan siber pun semakin meningkat.

Sumber: mediaindonesia.com

instrumen untuk mempermudah dan mempercepat proses perhitungan suara. Disanalah sekaligus merupakan lokus yang sering menjadi sasaran serangan *cyber* sehingga dapat merusakan konten suara yang sudah didapatkan secara sah dalam perhitungan satu persatu secara manual, kerusakan system dan infrastruktur, distorsi hasil perhitungan suara, gangguan layanan yang berujung dapat hilangnya kepercayaan public akan hasil perhitungan suara.

Kajian ini memiliki relevansi yang sangat penting dalam konteks keamanan pemilu dan keberlanjutan demokrasi. Dengan pemahaman yang lebih baik tentang ancaman *cybercrime* (kejahatan siber) pada pemilu, pemerintah, lembaga terkait, dan masyarakat dapat mengambil langkah-langkah konkret untuk melindungi proses pemilu yang adil dan transparan. Kajian ini juga dapat memberikan wawasan bagi peneliti, praktisi keamanan siber, dan pembuat kebijakan dalam menghadapi tantangan ancaman siber pada pemilu di masa depan (Chen and Zhao, 2019).

Keamanan siber dalam lingkup pemilu merupakan tindakan yang sistematis untuk melindungi komputer, jaringan, aplikasi perangkat lunak, sistem kritis, dan data KPU dari potensi ancaman digital pihak eksternal yang bertujuan untuk mendistorsi dan mengacaukan hasil-hasil pemilu yang sebenarnya. KPU dalam hal ini mewakili apparatus negara memiliki tanggung jawab besar untuk mengamankan data guna menjaga kepercayaan publik dan memenuhi kepatuhan terhadap peraturan.

Dalam konteks global, Indeks Keamanan Siber Indonesia masih berada pada Peringkat ke-3 Terendah di Antara Negara G20 (Zhang dan Wang, 2021). Laporan National Cyber Security Index (NCSI) mencatat, skor indeks keamanan siber Indonesia sebesar 38,96 poin dari 100 pada 2022. Angka ini menempatkan Indonesia berada di peringkat ke-3 terendah di antara negara-negara G20. Peringkat itu memberi signal bagi kita, baik itu pemerintah maupun semua

pemangku kepentingan demokrasi untuk mewaspadai pada adanya ancaman keamanan siber penyelenggaraan Pemilu. Bukan hanya menyangkut keamanan website penyelenggara Pemilu (KPU), tetapi juga partai politik sebagai aktor dalam sistem demokrasi yang diyakini sebagai road map terbaik menuju masyarakat Indonesia yang adil dan makmur.

Untuk itu naskah jurnal ini akan membahas secara komprehensif topik yang sangat penting ini, dimulai dengan tinjauan literatur tentang *cyber crime*, sejarah dan perkembangan *cyber crime*, serta hubungan antara pemilu dan ancaman *cyber crime*. Selanjutnya, kajian ini akan menguraikan metode kajian yang digunakan, hasil analisis mengenai ancaman *cyber crime* pada Pemilu Serentak 2024, dan upaya-upaya pencegahan yang dapat diimplementasikan. Terakhir, naskah ini akan menyajikan studi kasus dan kesimpulan yang merangkum temuan utama serta implikasi dan rekomendasi untuk pengembangan keamanan pemilu di masa depan.

II. Review Kepustakaan

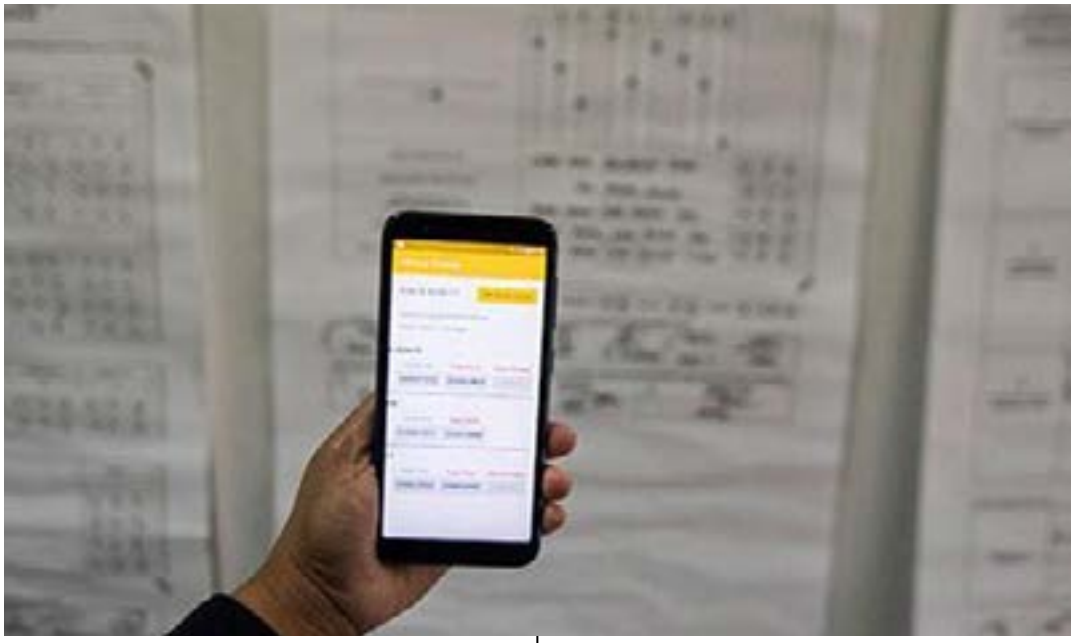
Cybercrime, juga dikenal sebagai kejahatan dunia maya atau kejahatan siber, adalah aktivitas kejahatan yang dilakukan dengan menggunakan teknologi komputer dan jaringan internet sebagai alat utama. *Cyber crime* melibatkan penggunaan teknologi informasi untuk merusak, mencuri, mengganggu, atau melakukan aktivitas ilegal lainnya. Definisi *cyber crime* mencakup berbagai jenis tindakan kriminal yang dapat merugikan individu, organisasi, atau negara (Mohanty dan Pattnaik, 2021; Drury, Rahman dan Ulah, 2022).

Lebih jauh banyak ahli dan peneliti bidang IT telah mengidentifikasi berbagai jenis serangan dan gangguan yang dapat merusak data, jaringan maupun fisik dari IT itu sendiri, antara lain:

1. Ancaman dan kerusakan fisik, jenis ancaman ini masih banyak disepelekan oleh pengguna IT lantaran pengguna berpikir bahwa serangan tersebut hanya terjadi pada *software*. Padahal, ancaman terhadap keamanan jaringan juga muncul pada *hardware* atau perangkat fisik. Contoh ancaman fisik adalah kerusakan pada *software* berupa data, file, aplikasi akibat ulah pihak tidak bertanggung jawab. Kerusakan tersebut ternyata mengancam keselamatan *hardware* kita sehingga tidak bisa berfungsi seperti biasa. Kerugian pada *hardware* biasanya berupa gangguan dan kerusakan pada *hardisk* secara fisik, baik disebabkan atas persoalan gangguan berupa korsleting listrik, gangguan koneksi, dan sebagainya.
2. Virus, serangan ini biasanya merupakan hasil oleh program yang dirancang oleh pihak yang ingin menggagalkan program besar atau hasil "kreasi" para peminat program untuk menduplikasi dirinya agar bisa menyusup ke program komputer lain. Virus bisa berasal dari *website* atau spam e-mail. Virus bekerja untuk merusak data dalam komputer sehingga tidak bisa diakses oleh pengguna lagi, sehingga keseluruhan data dapat dikacaukan atau dirusak. (Nugroho., 2020; Pusat Data Dan

Analisa Tempo., 2020)

3. *Worm*, sama seperti virus, worm juga bisa berduplikasi sehingga bisa menyebar ke seluruh jaringan internet. Aktivitas duplikasi *worm* bersifat otomatis dan tidak melibatkan penggunanya. Perbedaannya dengan virus adalah *worm* tidak menyerang aplikasi lain di komputer. (Beranda Agency, 2013; Sarjito., Aris, dan Editha Praditya Duarte; 2023)
4. *Trojan Horse,* Trojan horse merupakan *malware* atau program berbahaya yang mampu berkamuflase sehingga terlihat normal dan bekerja sesuai keinginan kita, padahal ia dapat merusak. Sumber *trojan* biasanya berasal dari *software* yang *di-install* dalam perangkat. Itulah alasan pentingnya meninjau aplikasi yang ada dalam komputer anda. Trojan ini masuk dalam keluarga *Malware* yang merupakan perangkat lunak berbahaya yang dirancang orang lain atau lawan politik untuk merusak, mencuri data, atau mengendalikan komputer KPU tanpa izin. Keluarga yang masuk dalam hal ini adalah meliput*i virus, worm, trojan horse, ransomware, dan spyware*. (Ludwig., 1991, digitalized 2011)
5. *Eavesdropping,* Ancaman ini umumnya datang dari para pihak yang menghendaki kondisi politik pasca pemilu menjadi tidak stabil dengan melakukan penyadapan dan kerusakan atas jaringan data yang dimiliki dan dikuasai oleh KPU/D. Para predator ini berupaya untuk dapat merusak, mengontrol atau mematai-matai rantai dan alur komunikasi atau transmisi data pada jaringan komputer KPU atau network pendukungnya. Salah satu contoh dari *eavesdropping* adalah penanaman penyadap suara pada jaringan komputer.
6. *Logic Bomb.* Ancaman ini muncul dalam bentuk potongan kode yang disusupkan ke dalam *software* secara sengaja. *Logic bomb* biasanya dirancang atau ditulis oleh orang dalam yang sudah mengetahui seluk-beluk jaringan komputer KPU/D kemudian menjual informasi tersebut pada para pihak yang berkepentingan dengan perubahan hasil. Karena isinya familier, *logic bomb* bekerja secara normal padahal mengandung fungsi yang mencurigakan.
7. *Spoofing.* Ancaman ini biasanya dikerjakan oleh pelaku dengan cara memalsukan Alamat pengguna agar bisa dipercaya oleh jaringan KPU/D. *Spoofing* dilakukan berkat bantuan beberapa tools, di antaranya URL *spoofing* yang bekerja dengan cara menampilkan URL palsu dan menyalahgunakan DNS *Cache*. Pelaku yang sudah sangat familiar dengan jaringan KPU/D yang mudah melakukan penyerangan tersebut.
8. *Denial-of-Service (DOS).* Ancaman ini menargetkan server website sehingga situs web tidak bisa diakses untuk sementara waktu. *Pelaku Denial-of-Service* melumpuhkan sistem server KPU/D dengan cara mengirim traffic sebanyak-banyaknya sampai server tidak mampu menampung request lagi. Ketika server-nya tumbang, pelaku langsung melancarkan aksi pembobolan dan mencuri data di



dalamnya.

9. *Phishing*. Ancaman ini dilancarkan dengan cara memancing operator KPU/D agar memberikan informasi atau data pribadinya. Pelaku menyaru sebagai pihak tepercaya agar bisa mencuri akun pengguna dan menyalahgunakannya. Teknik ini biasanya banyak terjadi juga di system keuangan dengan menyamar sebagai entitas terpercaya. Mereka mengirimkan pesan atau email palsu yang mengarahkan korban untuk mengungkapkan informasi sensitif seperti kata sandi, nomor kartu kredit, atau informasi bank lainnya. Para penyerang menggunakan jaringan botnet (jaringan komputer yang telah diretas) untuk mengirim lalu lintas yang besar ke target, membuatnya lumpuh.
10. *Man-in-The-Middle*. Ancaman ini, *man-in-the-middle* melibatkan seorang penyerang yang bekerja menghalangi komunikasi antara pengirim dan penerima pesan. Istilah lainnya, pembicaraan antara kedua belah pihak tersebut harus melalui penyerang tersebut. Kesempatan tersebut menjadi celah bagi penyerang untuk menyadap dan memalsukan komunikasi yang sedang berlangsung.
11. Pencurian Identitas (*Identity Theft*): Pencurian identitas terjadi ketika seseorang menggunakan informasi pribadi seseorang, seperti nama, nomor KTP, atau nomor kartu kredit, dan identitas lainnya untuk melakukan tindakan kriminal atau penipuan.
12. *Hacking*. Ancaman ini melibatkan peretasan sistem komputer atau jaringan dengan tujuan mencuri data, merusak sistem, atau mendapatkan akses ilegal. *Hacker* dapat beroperasi sebagai individu atau kelompok, dan mereka dapat memiliki motivasi yang berbeda, termasuk keuangan, politik,

atau ideologis. Mereka dapat bekerja dari dalam dan luar negeri.

13. *Ransomware Conti*, merupakan sebuah kelompok ransomware yang dikelola sebagai *Ransomware-as-a-Service (RaaS*). Ransomware ini pertama kali terdeteksi pada tahun 2020 dan diduga dikendalikan oleh kelompok kejahatan siber berbasis Rusia yang menggunakan pseudonim Wizard Spider (Dora Tudor, 2022). Sejak Agustus 2021, jenis serangan ini menjadi berita utama dalam keamanan siber. Badan Keamanan Infrastruktur Siber (CISA*), Federal Bureau of Investigation (FBI), dan National Security Agency* (NSA) telah memberikan peringatan bersama tentang ancaman yang dihadirkan oleh kelompok *ransomware Conti* dan kerentanannya yang dieksploitasi. Pada awal Mei 2022, pemerintah Amerika Serikat mengumumkan hadiah hingga $10 juta untuk informasi tentang kelompok *Conti ransomware*. Untuk menghadapi kelompok ransomware berbahaya seperti Conti, organisasi/institusi perlu menerapkan pendekatan berbasis risiko untuk melindungi diri. Serangan terbaru di Indosia dialami oleh Bank Indonesia Bengkulu pada Januari 2022, dan Bank Syariah Indonesia (BSI) pada Mei 2023. Akibat serangan tersebut, layanan Anjungan Tunai Mandiri (ATM) dan mobile banking BSI lumpuh (DSoesatyo, 2023)

III. Diskusi dan Pembahasan

Setelah kita pahami ancaman-ancaman *cybercrime* yang potensial akan terjadi pada pemilu serentak tahun 2024 di Indonesia yang segera akan dijalankan, maka mulai sekarang kita harus petakan dan identifikasikan potensi ancaman tersebut sehingga dapat segera diantisipasi tindakan pencegahannya. Ancaman-ancaman tersebut harus diantisipasi dan diatasi dengan langkah-langkah keamanan *cyber* yang efektif Gupta dan Rana, 2018). Berikut ini beberapa ulasan atas serangan *cybercrime* dalam pemilu yang pernah terjadi di Indonesia dan di belahan dunia lain. Melalui pengalaman-pengalaman tersebut, maka langkah strategis dan taktis harus segera dipersiapkan.

Pengalaman Pemilu di Indonesia:

Indonesia juga telah mengalami serangan *cybercrime* selama pemilu pada tahun 2014 dan 2019. Pada tahun 2014, situs web Komisi Pemilihan Umum (KPU) Indonesia mengalami serangan *Distributed Denial of Service (DDoS)* yang mengganggu akses publik terhadap informasi pemilu. Serangan phishing juga telah menjadi pada pemilu di Indonesia. Serangan DDoS merupakan serangan di mana sejumlah besar komputer atau perangkat yang terinfeksi (disebut sebagai "bot" atau "zombie") bekerja sama untuk mengganggu layanan atau sumber daya komputer yang ditargetkan, seperti situs web, server, atau jaringan. Serangan paling terkenal yang telah ada di Internet selama lebih dari tiga decade ini, bertujuan mengganggu koneksi antara target dan penggunanya, melumpuhkan akses jaringan, serta menguras sumber daya server. Serangan DDoS muncul pada tahun 1999 dan menjadi bentuk utama serangan DoS. Tujuan utama mereka adalah merusak server korban, yang

mengakibatkan kerugian pendapatan dan biaya yang signifikan untuk mitigasi dan pemulihan layanan.

Kemajuan dalam teknologi memberikan pelaku serangan lebih banyak sumber daya, memungkinkan serangan siber yang lebih merusak dan lebih mudah dilakukan. Banyak serangan DDoS sekarang memanfaatkan botnet yang terorganisir dan dikendalikan dari jarak jauh, terdiri dari banyak mesin zombie yang terinfeksi malware. Para bot ini secara bersamaan menyerang target dengan volume data besar, yang pada akhirnya melambatkan dan merusak sistem. Penggunaan botnet melindungi anonimitas penyerang dan meningkatkan tingkat keparahan serangan DDoS.

Lanskap baru untuk serangan DDoS telah muncul dengan mencolok, disebut "*DDoS as a Service*," yang mengubah cakupan dan dampak serangan DDoS. Situs web DDoS-for-hire yang mudah diakses memungkinkan peretas untuk menjalankan serangan DDoS dengan biaya serendah $5 per jam. Sejak rilis kode sumber botnet Mirai pada tahun 2016, permintaan dan penawaran layanan serangan semakin meningkat. Laporan menunjukkan bahwa hingga 40% serangan lapisan jaringan dikaitkan dengan *botnet DDoS-for-hire*. Layanan ini sering diiklankan sebagai layanan "Stresser" atau "Booster" yang menawarkan pemecahan masalah dan pengujian untuk mengidentifikasi kerentanan jaringan.

Studi terbaru mengungkap peningkatan baik dalam frekuensi maupun tingkat keparahan serangan DDoS. Cisco memprediksi bahwa serangan DDoS akan menjadi lebih sering, melonjak dari 7,9 juta pada tahun 2018 menjadi lebih dari

Sumber: kpu.go.id

15 juta pada tahun 2023. Pada tahun 2020, serangan DDoS mengalami peningkatan yang signifikan dengan pertumbuhan tahunan sebesar 341,21%. Salah satu serangan DDoS terbesar yang pernah tercatat menargetkan *Amazon Web Services* (AWS) pada Februari 2020, dengan puncak serangan mencapai 2,3 Tbps. Downtime layanan IT dapat mengakibatkan kerugian perusahaan mencapai antara $300.000 hingga $1.000.000 per jam. Kerugian finansial akibat serangan DDoS selama enam bulan terhadap ribuan alamat IP Google pada Oktober 2020 juga sangat besar, dilakukan oleh tiga ISP asal China dengan laju serangan mencapai 2,5 Tbps.

Serangan DDoS yang cukup menonjol di Indonesia di antaranya menyangkut dugaan adanya kebocoran data BPJS Kesehatan. Setelah menginvestigasi satu juta data sampel yang diklaim pelaku, Kementerian Kominfo menemukan bahwa sampel data diduga kuat identik dengan data milik BPJS Kesehatan. Data itu meliputi Nomor Kartu, Kode Kantor, Data Keluarga/Data Tanggungan, dan status Pembayaran (Permadi 2021).

Kebocoran data juga terjadi pada data Daftar Pemilih Tetap (DPT) tahun 2014. Data dimaksud memuat data pribadi seperti nomor kartu keluarga, nama lengkap, Nomor Induk Kependudukan (NIK), alamat rumah, tempat dan tanggal lahir, dan lain-lain (Samad & Persadha, 2022). Menurut Komisioner Komisi Pemilihan Umum (KPU) Viryan Aziz, sebanyak 2,3 juta data yang dicuri merupakan data DPT Pemilu 2014 yang berformat PDF (Setiawan 2020). Menurut Ketua Tim Tata Kelola Perlindungan Data Pribadi Kementerian Kominfo, Hendri Sasmita Yuda, data pribadi tidak hanya berkaitan dengan keamanan, tetapi juga pemenuhan hak-hak proporsionalitas untuk mewujudkan tata kelola perlindungan data pribadi (Andreya 2022).

Pada pemilu 2019, terdapat banyak penyebaran *hoaks* dan informasi palsu melalui media sosial yang bertujuan untuk mempengaruhi pandangan publik dan opini politik. Ini menciptakan lingkungan yang lebih kompleks dalam pemilihan. Pada Pemilu 2019 juga, terdapat laporan serangan siber yang mencurigakan terhadap situs web Komisi Pemilihan Umum (KPU) Indonesia. Situs web KPU mengalami peningkatan lalu lintas yang luar biasa sehingga menyebabkan gangguan akses bagi pengguna. Meskipun tidak ada bukti konkret bahwa ini adalah serangan siber yang disengaja, insiden ini menyoroti potensi ancaman *cybercrime* terhadap proses pemilu di Indonesia.

Pengalaman Pemilu di Amerika Serikat:

Pemilihan Presiden Amerika Serikat tahun 2016 ternyata melibatkan perang dan serangan siber yang signifikan yang diyakini berasal dari pihak Rusia. Entitas yang diduga terkait dengan pemerintah Rusia tersebut diklaim oleh US telah mencoba mempengaruhi pemilihan dengan meretas dan merilis informasi yang merugikan salah satu calon presiden. Serangan ini menimbulkan kekhawatiran tentang campur tangan asing dalam pemilihan dan menggarisbawahi pentingnya keamanan siber dalam pemilu di Amerika Serikat.

Kantor berita Turki menggambarkan, pada pemilihan midterm AS 2018, ada laporan serangan siber yang mencoba

meretas sistem pemilihan di beberapa negara bagian. Serangan ini menunjukkan bahwa ancaman *cybercrime* masih berlanjut dan dapat mengganggu proses pemilihan di tingkat negara bagian.

Pemilu AS tahun 2020[2] tetap menghadapi ancaman serangan siber yang menjadi perhatian serius. Pemerintah AS dan pihak berwenang dalam bidang keamanan siber secara aktif berusaha untuk melindungi integritas pemilihan ini dari serangan siber potensial. Meskipun belum ada bukti konkret tentang campur tangan yang berhasil, kita perlu menyadari tingginya risiko yang terkait dengan pemilu modern saat ini.

Microsoft telah mengidentifikasi serangan siber yang telah ditargetkan pada individu dan organisasi yang terlibat dalam pemilihan presiden AS yang akan datang. Serangan ini mencakup upaya untuk meretas kampanye Presiden Donald Trump dan penantang Demokrat Joe Biden. Kelompok aktivitas yang terlibat dalam serangan ini berasal dari Rusia, China, dan Iran.

Strontium, yang berbasis di Rusia, telah menyerang lebih dari 200 organisasi, termasuk kampanye politik, kelompok advokasi, partai politik, dan konsultan politik. Zirkonium, yang berbasis di China, telah menargetkan individu terkemuka yang terkait dengan pemilu, termasuk orang-orang yang terlibat dalam kampanye presiden Joe Biden dan pemimpin dalam komunitas urusan internasional. Strontium juga terlibat dalam serangan terhadap kampanye presiden Demokrat pada tahun 2016. Sedangkan Fosfor, yang berbasis di Iran, terus melancarkan serangan terhadap rekening pribadi individu yang terkait dengan kampanye Presiden Donald Trump.

Microsoft berhasil menggagalkan sebagian besar serangan ini dengan menggunakan alat keamanan yang ada di produk-produk mereka, dan mereka telah memberitahu target-targetnya agar dapat mengambil tindakan perlindungan tambahan. Perusahaan ini mendorong otoritas pemilihan di tingkat negara bagian dan lokal di AS untuk memperkuat operasi keamanan siber mereka dan bersiap menghadapi potensi serangan. Mereka juga menekankan pentingnya alokasi dana federal yang lebih besar untuk melindungi infrastruktur pemilu.

Pengalaman Pemilu di Beberapa Negara Eropa:

Pemilihan umum di Perancis pada tahun 2017 terancam oleh serangan *cyber* yang menargetkan salah satu kandidat presiden, Emmanuel Macron. Para penyerang mencoba meretas email dan akun-akun pribadi staf kampanye Macron. Meskipun serangan ini tidak berhasil, itu menunjukkan tingkat ancaman *cyber* yang dapat mempengaruhi hasil pemilihan tingkat nasional Perancis. Serangan ini dilaporkan berasal dari kelompok yang memiliki kaitan dengan pemerintah Rusia. Hasil pemilu Prancis kemudian menjadi perhatian dunia, menunjukkan betapa serius ancaman *cyber*crime

2 Serangan Ransomware WannaCry mengenkripsi data pada komputer korban dan menuntut pembayaran tebusan dalam bentuk cryptocurrency untuk mendapatkan kunci dekripsi. Serangan ini menargetkan berbagai organisasi di seluruh dunia, termasuk rumah sakit dan perusahaan besar

dapat mempengaruhi pemilu di tingkat internasional[3].

Pemilihan umum di Jerman pada tahun 2017 juga menghadapi potensi ancaman *cybercrime*. Serangan siber yang mencoba meretas data partai politik dan pejabat pemerintah Jerman menjadi perhatian utama. Serangan ini menimbulkan kekhawatiran tentang keamanan pemilu di Eropa[4].

Pemilu di Inggris telah menjadi target potensial bagi ancaman *cybercrime*. Ancaman seperti serangan siber yang mencoba merusak integritas pemilu atau mencuri data sensitif telah menjadi perhatian. Salah satu sumber kredibel yang dapat memberikan wawasan tentang ancaman siber pada pemilu di Inggris *adalah "National Cyber Security Centre*" (NCSC), yang merupakan badan keamanan siber nasional Inggris. NCSC telah menerbitkan laporan dan panduan terkait dengan keamanan siber dalam pemilihan dan pemrosesan suara.

Ukraina menghadapi serangan siber yang signifikan selama pemilu tahun 2014 dan 2019. Serangan tersebut terkait erat dengan konflik geopolitik di wilayah tersebut dan menunjukkan bahwa ancaman *cybercrime* dapat digunakan sebagai alat untuk mencampuri urusan

3 Serangan *Ransomware WannaCry* mengenkripsi data pada komputer korban dan menuntut pembayaran tebusan dalam bentuk cryptocurrency untuk mendapatkan kunci dekripsi. Serangan ini menargetkan berbagai organisasi di seluruh dunia, termasuk rumah sakit dan perusahaan besar.

4 Kasus ini mencatatkan dalam "*Cyber Threats and Vulnerabilities in Kenya: The 2017 General Elections*" (Ancaman dan Kerentanan Siber juga terjadi di Kenya: Pemilu Umum 2017). Pada tahun 2019, terdapat insiden serangan siber terhadap situs-situs pemerintah yang berkaitan dengan pemilu, yang dicatat dalam *"Cyber Threats and Vulnerabilities in Kenya: The 2017 General Elections"* [sumber: "*Cyber Threats and Vulnerabilities in Kenya: The 2017 General Elections"].*

dalam negeri dan mempengaruhi hasil pemilu

Pemilu dan Ancaman Serangan Cyber

Mengapa ancaman *cybercrime* seringkali terjadi pada pemilu? Dengan mempertimbangkan beberapa kasus terdahulu yang melibatkan pemilu, maka dapat ditarik pembelajaran penting, yaitu:

Kasus-kasus di atas mencerminkan kerentanan sistem pemilu dari ancaman *cybercrime* di berbagai negara. Ancaman serangan siber dapat berasal dari aktor dalam maupun luar negeri, dan penting bagi negara-negara untuk mengambil langkah-langkah keamanan yang serius untuk melindungi integritas proses pemilihan dan kepercayaan masyarakat.

Ancaman *cybercrime* yang terjadi pada pemilu dapat dijelaskan dengan berbagai alasan yang kompleks. Salah satu alasan utama adalah pentingnya pemilu dalam konteks politik dan kebijakan. Sebagaimana yang dijelaskan oleh Bruce Schneier, seorang pakar keamanan siber terkemuka, dalam bukunya "*Click Here to Kill Everybody*," pemilu adalah "peristiwa besar" dalam suatu negara, dan oleh karena itu, mereka menjadi target utama bagi pihak-pihak yang ingin mempengaruhi atau merusak proses demokrasi. Schneier menggarisbawahi bahwa serangan siber pada pemilu dapat memberikan pengaruh yang signifikan pada hasilnya, dan inilah yang membuat pemilu menjadi target yang menarik bagi para penyerang.

Selain itu, Jenny S. Martinez, dalam jurnalnya yang berjudul "*Cyberattacks and International Law,*" menjelaskan bahwa pemilu seringkali menjadi sasaran serangan siber, karena hasil pemilu dapat memiliki dampak langsung pada hubungan internasional dan kebijakan luar negeri. Dalam era globalisasi, pemilihan umum suatu negara dapat mempengaruhi negara-negara lain secara langsung, dan serangan siber dapat digunakan sebagai alat untuk mencampuri urusan dalam negeri negara lain.

Ancaman *cybercrime* pada pemilu dapat dijelaskan dengan berbagai alasan yang kompleks. Selain pandangan Bruce Schneier dan Jenny S. Martinez yang telah disebutkan sebelumnya, Ben Buchanan dalam bukunya "*The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*" menggarisbawahi bahwa pemilu adalah titik lemah dalam keamanan siber negara-negara demokratis. Dia menjelaskan bahwa pemilu seringkali beroperasi dalam jaringan yang terbuka untuk meningkatkan transparansi, tetapi hal ini juga membuatnya rentan terhadap serangan siber. Penyerang dapat memanfaatkan sifat terbuka ini untuk mempengaruhi pemilihan.

Untuk lebih memahami hubungan antara pemilu dan ancaman *cybercrime,* penting untuk mengevaluasi beberapa kasus terdahulu yang melibatkan pemilu. USAID mencatat bahwa Pemilihan umum di seluruh dunia telah menjadi target serangan siber; selain insiden-insiden yang disebutkan di bawah ini, ada contoh-contoh di Eropa, Amerika Utara, Amerika Latin (Marañon, A.; 2021), Afrika (Allen, N. and N. van der Waag-Cowling, 2021), Asia (Lim, Y., 2020), dan Oseania (Galloway, Anthony., 2020). Warga negara pada umumnya menyadari kemungkinan serangan tersebut, dan banyak yang meragukan, dengan alasan yang cukup

kuat, bahwa negara mereka siap untuk berhasil melawannya (Poushter, J. and Fetterolf, J., 2019). Pemilihan umum terbaru di Kenya dan Republik Demokratik Kongo, misalnya, telah melihat hasil elektronik seolah-olah menghilang begitu saja - bahkan tanpa dugaan campur tangan eksternal.Dalam kasus di Kenya misalnya, serangan tersebut melibatkan situs web komisi pemilihan umum yang diretas dan distribusi informasi palsu melalui media sosial.

Selain itu, dalam buku "*Election Cybersecurity: A Comprehensive Guide,*" yang disunting oleh Gregory A. Baker, dijelaskan beberapa kasus serangan siber pada pemilu di berbagai negara, termasuk Amerika Serikat dan Prancis. Kasus-kasus seperti serangan *DDoS* dan serangan *phishing* pada pemilu telah menimbulkan kekhawatiran serius tentang keamanan pemilu di seluruh dunia.Melalui analisis kasus-kasus tersebut, kita dapat melihat bahwa pemilu rentan terhadap ancaman *cybercrime*, dan serangan semacam itu dapat memiliki dampak yang signifikan pada proses demokrasi. Oleh karena itu, perlu adanya upaya yang serius untuk melindungi sistem pemilu dari ancaman ini, baik melalui tindakan teknis maupun regulasi yang tepat.

IV. Saran Penanganan *Cyber Crime*

Di Indonesia, dalam kontestasi politik saat ini berkembang pesat apa yang dinamakan dengan *cyber troops*, yaitu berserakannya kelompok Masyarakat yang membuat akun-akun media sosial yang dibayar untuk memanipulasi opini publik. Ada pula yang dinamakan *computational propaganda,* yakni penggunaan algoritma untuk isu-isu yang menjadi *concern public*. Pola seperti ini sering ditemukan di media sosial, dan diprediksi di tahun 2024 yang akan datang cara seperti ini masih akan digunakan. Inilah salah satunya yang seringkali menjadi penyebab terjadinya Dis-Informasi seperti yang dijelaskan sebelumnya.

Oleh karenanya, dampak yang perlu diantisipasi oleh KPU/D sebagai penyelenggara pemilu terkait masalah siber, yakni mengenai informasi *hoax* yang dapat mempengaruhi kepercayaan publik. Peran media juga menjadi penting untuk menjadi referensi. KPU perlu mendorong kerja sama dengan media agar ketika terdapat isu-isu berkaitan dengan KPU, dapat segera diklarifikasi. Saran penanganan dan control terhadap potensi *cybercrime* adalah sebagai berikut:

1. Membangun koordinasi antar semua institusi negara yang bergerak dalam IT dan dunia digital untuk menyepakai *platform* bersama dalam mengantisipasi ancaman *cybercrime* pada pemilu serentak tahun 20024. *Platform* itu harus terinci sampai dengan penyusunan SOP dalam setiap kerjanya.
2. Kerja penting dari *network* dan *platform* perlindungan *cybercrime* ini perlu *di back up* keamanan nasional dengan peraturan perundangan yang dikeluarkan setingkat Lembaga negara.
3. Membuat peta jalan dari setiap tahapan kerja KPU/D dengan dibarengi dengan dukungan IT dan data serta kelengkapan pendukung bila terjadi serangan terhadap sistem IT KPU/D.
4. Menyiapkan tim kerja taktis pelindung

dan tim perbaikan bila terjadi serangan IT dan system KPU/D.

5. Pengamanan Data Pemilih dengan ketat dan hanya dapat diakses oleh pihak yang berwenang. Ini menghindari potensi penyebaran data pribadi secara ilegal atau penipuan pemilu.
6. Perlu ada status penetapan ancaman dan gangguan jaringan IT yang memberikan peringatan dini bila terjadi serangan IT. Dengan 4 tahapan analisis awal terhadap Kesehatan jaringan IT KPU/D, yaitu: tahapan pertama mengantisipasi vulnerability, yakni memetakan bagian yang rawan terhadap serangan. Kedua, memetakan pihak-pihak yang berpotensial mengancam jalannya pemilu dan perhitungan hasil serta intervensi kepada system jaringan IT KPU/D. Ketiga, memperkirakan impact kerusakan atas serangan yang mungkin terjadi. Keempat, analisis frekuensi terhadap gangguan dan serangan. Kelima, memberikan scenario countermeasure berupa Langkah pencegahan dan peningkatan pengamanan system IT.
7. Hukum dan Hukuman yang Tegas, yakni dengan menerapkan undang-undang yang tegas dan hukuman yang sesuai terhadap pelaku kejahatan siber dapat menjadi deterrensi yang efektif. Dan tidak kalah pentingnya adalah menjaga tingkat transparansi dalam proses pemilihan, termasuk proses pemilihan dan penghitungan suara, adalah langkah penting untuk memastikan kepercayaan masyarakat.
8. Upaya-upaya untuk meningkatkan keamanan jaringan IT adalah sebagai berikut: (6.1) sering ganti Alamat SSID, (6.2) Gunakan Enkripsi, (6.3) Non aktifkan fitur-fitur interface router, (6.4) instal berbagai anti virus, (6.5) lakukan back up berlapis yang tidak hanya 2 atau tiga tempat, (6.6) lakukan pemeriksaan sistematis terhadap semua operator secara rahasia oleh tim pengawasan internal. ❖

Sumber foto: https://ldii.or.id/mengenal-cyber-crime-jenisnya-dan-cara-mengatasinya/

DAFTAR PUSTAKA

- Allen, N. and N. van der Waag-Cowling. (2021, July 15). *How African States Can Tackle State-Backed Cyber Threats*.
- Brookings Institute. https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyberthreats/
- Brett Drury c d, Samuel Morais Drury e, Md Arafatur Rahman f, Ihsan Ullah.,(2022)., *A social network of crime: A review of the use of social networks for crime and the detection of crime* https://doi.org/10.1016/j.osnem.
- Buchanan., Ben ; (2016); *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*; London; Oxford University Press
- Chaudhary., Tarun; Thomas Chanussot, and Manuel Wally (lead authors). (2023); *UNDERSTANDING CYBERSECURITY THROUGHOUT THE ELECTORAL PROCESS: A REFERENCE DOCUMENT*, An Overview of Cyber Threats and Vulnerabilities in Elections; USAID
- Chen, C. L., & Zhao, Y. (2019). *"Cybersecurity and Privacy in the Smart City: A Case Study of Challenges and Solutions."* IEEE Access, 7, 154791-154803.
- Caldarulo Martia, Eric W. Welch, Mary K. Feeney., (2022)., *Determinants of cyber-incidents among small and medium US citieshttps:*//doi.org/10.1016/j.giq.2022.101703
- Cavelty, M. D., & Suter, M. (2016). "*The Politics of Cybersecurity in the Context of Critical Infrastructure Protection.*" International Studies Review, 18(1), 33-53.
- Galloway, Anthony. (2020, October 28). *Cyber Attacks on Elections Growing Amid Concern for Australia's Political Parties*. Sydney Morning Herald. https://www.smh.com.au/politics/federal/cyber-attacks-on-elections-growing-amidconcern-for-australia-s-political-parties-20201028-p569fg.html
- Gupta, M., & Rana, J. (2018). "*Cyber Threats to Critical Infrastructure: A Comprehensive Review.*" IEEE Access, 6, 17236-17261
- IPTEK-KOM (Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi) Vol. 24 No. 2, Desember 2022; (https://jurnal.kominfo.go.id/index.php/iptekkom/article/view/4878/1892)
- Komisi Pemilihan Umum Republik Indonesia. (2021). "*Pemilu Serentak 2024: Antisipasi Ancaman Siber.*"
- Komisi Pemilihan Umum Republik Indonesia. (2022). *"Buku Putih Keamanan Siber Pemilu Serentak Tahun 2024."*
- Lim, Y. (2020, November 22). *Election Cyber Threats in the Asia-Pacific Region. Mandiant*. https://www.fireeye.com/blog/threat-research/2020/11/election-cyber-threats-in-the-asia-pacific-region.html
- Liu, X., Zhang, L., & Wang, W. (2021). "*An Overview of Cybersecurity Risks and Countermeasures in the Internet of Things*." IEEE Access, 9, 27134-27147.
- Ludwig., Mark A.; (1991, digitalized 2011); *The little black book of computer viruses;* Pennsylvania State University; American Eagle Publications.

- Marañon, A. (2021, May 28). *How Have Information Operations Affected the Integrity of Democratic Elections in Latin America?* Lawfare. https://www.lawfareblog.com/how-have-information-operations-affected-integrity-democraticelections-latin-america
- Nugroho., Riyanto. (2020). *National Cyber Security: Tantangan Indonesia Terkini*; Rumah Reformasi Kebijakan [Institute for Policy Reform]
- Pusat Data Dan Analisa Tempo; (2020); *Waswas Virus WannaCry*; Jakarta; Tempo Publishing. Beranda Agency (2013); *Pengamanan Total Data Dan Informasi Penting;* Jakarta; Elex Media Komputindo.
- Permadi, Dedy. 2021. "*Update Terkait Dugaan Kebocoran Data Pribadi Penduduk Indonesia*." Kominfo, 2021. https://www.kominfo.go.id/content/detail/34628/siaran-pers-no-179hmkominfo052021-tentang-update-terkait-dugaan-kebocoran-data-pribadi-penduduk-indonesia/0/siaran_pers.
- Poushter, J. and Fetterolf, J. (2019, January 9). *International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security*. Pew Research Center. https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-electionsinfrastructure-national-security/
- Sarjito., Aris, dan Editha Praditya Duarte; (2023). *Geopolitik dan Geostrategi Pertahanan: Tantangan Keamanan Global*; Jakarta; Indonesia Emas Group
- Seema Gupta Bhol, JR Mohanty, Prasant Kumar Pattnaik., (2021)., *Taxonomy of cyber security metrics to measure strength of cyber security.* https://doi.org/10.1016/j.matpr.2021.06.228
- Samad., M. Yusuf, dan Pratama Dahlian Persadha; (2022); "*Memahami Perang Siber Rusia dan Peran Badan Intelijen Negara dalam Menangkal Ancaman Siber Understanding Russian Cyber Warfare and the Role of the State Intelligence Agency in Countering Cyber Threats*";
- Setiawan, Riyan. 2020. "*KPU Membenarkan 2,3 Juta Data Yang Bocor Merupakan DPT Tahun 2014.*" Tirto, 2020. https://tirto.id/kpu-membenarkan-23-juta-data-yang-bocor-merupakan-dpt-tahun-2014-fA5B.
- Singh., Anshuman, and Brij B. Gupta; (2022; "*Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions"*; International Journal on Semantic Web and Information Systems (IJSWIS) Vol. 18(1);
- Soesatyo., Bambang; (2023). "*Eskalasi Ketahanan Nasional dengan Angkatan Siber adalah Keniacayaan". Jayakarta News (Kolom/Oped), 6 Oktober 2023.*
- Tambawal, S., Wang, Z., & Lakshmanan, M. K. (2018). "*Cybersecurity Threats in Social Media Elections*." In Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp. 537-544).
- Tudor., Dora; (2022). *What Is Conti Ransomware?* https://heimdalsecurity.com/blog/what-is-conti-ransomware/
- Wibowo, A. C., & Harimurti, H. (2021). "*Pentingnya Keamanan Siber dalam Pemilu Serentak 2024*." Media Indonesia, 14 Januari 2021.