Jurnal Edunity: Kajian Ilmu Sosial dan Pendidikan
Volume 1 Number 03, November, 2022
p- ISSN 2963-3648- e-ISSN 2964-8653

ANALISIS INTELIJEN ATAS POTENSI ANCAMAN SERANGAN SIBER PADA PRESIDENSI KTT G20 TAHUN 2022 DI INDONESIA

Widyanto Pudyo P.
Universitas Brawijaya Malang, Indonesia
E-mail: widhi9843al@gmail.com

INFO ARTIKEL
Diterima:
1 November 2022
Direvisi:
5 November 2022
Disetujui:
10 November 2022

ABSTRAK

Pada tanggal 15-16 November 2022, Indonesia akan melaksanakan event besar yang tidak hanya menjadikan kebanggaan bangsa Indonesia, tetapi juga menjadikan pertaruhan nama baik Indonesia di forum Internasional dalam menyelenggarakan KTT G20. Suksesnya penyelenggaraan KTT G20 selain akan menumbuhkan tingkat kepercayaan internasional terhadap Indonesia, juga akan menaikkan posisi tawar Indonesia di forum internasional. Demikian juga sebaliknya, kurang suksesnya penyelenggaraan KTT G20, tidak saja menurunkan kredibilitas Indonesia, tetapi juga dapat menurunkan tingkat kepercayaan terhadap Indonesia. Oleh karena itu, kesuksesan penyelenggaraan KTT G20 merupakan harga mutlak yang tidak bisa ditawar-tawar lagi. Penelitian ini merupakan penelitian berjenis deskriptif kualitatif terhadap potensi ancaman serangan siber yang dapat terjadi pada perhelatan KTT G20 di Bali, Indonesia.tujuan dari penelitian ini adalah untuk menganalisis intelijen atas potensi ancaman serangan siber pada presidensi ktt g20 tahun 2022 di indonesiaPenelitian ini dilakukan dengan pendekatan studi kasus. Hasil penelitian menunjukkan bahwa potensi serangan siber pada event KTT G20 relatif besar. Hal ini didasarkan pada fakta-fakta dan data tentang penyelenggaraan sebelumnya dan perkembangan ancamanan siber saat ini. Selain itu kecenderungan meningkatnya serangan siber dan belum kondusifnya situasi global serta banyaknya kepentingan negara-negara tertentu terhadap negara lain, juga menjadi dasar perkiraan potensi ancaman serangan siber pada penyelenggaraan KTT G20 yang relatif besar. Faktor-faktor yang berpengaruh terhadap peluang ancaman serangan siber pada KTT G20 perlu mendapatkan perhatian khusus, agar deteksi dini dan cegah dini terhadap setiap ancaman serangan siber KTT G20 dapat dilaksanakan secara maksimal.

Kata kunci: Serangan Siber; Analisis Intelijen; KTT G20

ABSTRACT

On November 15-16, 2022, Indonesia will hold a big event that will not only make the Indonesian nation proud, but also put Indonesia's reputation at stake in international forums in holding the G20 Summit. The success of the G20 Summit will not only increase the level of international trust in Indonesia, but will also increase Indonesia's bargaining position in international forums. Vice versa, the lack of success in holding the G20 Summit, not only reduces Indonesia's credibility, but can also reduce the level of trust in Indonesia. Therefore, the success of holding the G20 Summit is an absolute and non-negotiable price. This research is a qualitative descriptive study on the potential threats of cyber attacks that can occur at the G20 Summit in Bali, Indonesia. case. The results showed that the potential for cyber attacks at the G20 Summit event was relatively large. This is based on facts and data about previous implementations and the current development of cyber threats. In addition, the trend of increasing cyber attacks and the unfavorable global situation as well as the many interests of certain countries against other countries, are also the basis for estimating the potential threat of cyber attacks at the relatively large G20 Summit. Factors that affect the threat of cyberattacks at the G20 Summit need special attention, so that early detection and early prevention of every cyberattack threat at the G20 Summit can be carried out optimally.

Keywords: cyber attacks; intelligence analysis; G20 Summit

PENDAHULUAN

Sejak didirikan pada tahun 1999, KTT G20 selalu diselenggarakan secara rutin, yang pada awalnya diselenggarakan dua kali dalam setahun, namun mulai tahun 2011 hanya diselenggarakan sekali dalam setahun. Kali ini Indonesia yang akan menyelenggarakan KTT tersebut pada tanggal 15-16 November 2022 di Bali (Astuti & Fathun, 2020) tersebut sesuai dengan kapasitas dan peran intelijen untuk melaksanakan deteksi dini dan cegah dini setiap potensi ancaman terhadap penyelenggaraan KTT G20 di Indonesia. Berbagai dimensi ancaman yang berpotensi timbul selama penyelenggaraan KTT G20 harus benar-benar diantisipasi. Ancaman yang timbul dapat berupa ancaman fisik yang menyangkut aspek keamanan personel, materiil, instalasi, kegiatan, dokumen maupun berita. Di samping itu, ancaman non fisik yang berupa ancaman serangan siber, juga merupakan ancaman potensial yang benar-banar harus diwaspadai.

Ancaman siber merupakan salah satu ancaman potensial yang dapat terjadi selama penyelenggaraan KTT G20 di Bali. Di era digital sekarang ini, dimana hampir seluruh aktifitas terhubung dengan internet, ditambah lagi belum kondusifnya situasi global dan banyaknya kepentingan perorangan, kelompok atau negara, menyebabkan ancaman siber merupakan salah satu ancaman yang perlu diantisipasi secara serius. Diperlukan langkah-langkah efektif dan terintegrasi untuk dapat meminimalkan potensi ancaman siber pada KTT G20 di Bali (Dewi, 2022)

Untuk dapat mengetahui potensi ancaman siber yang berpotensi terjadi selama penyelenggaraan KTT G20, maka diperlukan pengkajian mendalam terkait fakta-fakta serangan siber secara umum, serangan siber terhadap penyelenggaraan KTT G20, perkembangan serangan siber saat ini serta kondisi Indonesia dalam menghadapi ancaman siber itu sendiri. Beberapa fakta-fakta terkait perkembangan siber dan ancaman siber yang terjadi beberapa tahun terakhir di antaranya sebagai berikut:

1. **Keamanan Siber Salah Satu Fokus Pembahasan Digital Economy Working Group**

   Pada tanggal 20 Juli 2022 Menteri Komunikasi dan Informatika Johnny G. Plate menyatakan bahwa, dunia tidak lagi bisa menghindari masa depan yang kian bertumpu pada pemanfaatan data, termasuk data-driven policy yaitu keinginan dalam melakukan suatu tindakan untuk mencapai suatu perubahan tertentu dan mencapai tujuan. Pemanfaatan data makin meluas di kalangan institusi pemerintah maupun privat sehingga membutuhkan kesepahaman mengenai kedaulatan data dan tata kelola data global. Saat ini dunia akan semakin membutuhkan tata kelola data yang diterima berdasarkan kesamaan pandangan. Pernyataan tersebut disampaikan dalam forum Pertemuan Ketiga Digital Economy Working Group (3rd DEWG meeting) di Labuahan Bajo Nusa Tenggara Timur. Salah satu fokus pembahasan dalam pertemuan tersebut adalah masalah keamanan siber.

2. **Keamanan Digital Menjadi Kunci untuk Mendukung Komunitas Bisnis DEWG G20**

   Pada tanggal 18 Juli 2022 telah dilaksanakan pertemuan kedua Digital Economy Working Group (2nd DEWG G20) di Yogyakarta yang membahas lima sub-topik terkait teknologi dan informasi, salah satunya keamanan siber. Dalam pertemuan tersebut Menteri Kementerian Komunikasi dan Informatika (Kominfo) Johnny G Plate mengatakan, bahwa keamanan digital menjadi kunci untuk mendukung komunitas bisnis DEWG G20, karena keamanan siber menjadi tantangan transformasi digital tiap negara saat ini. Khususnya, bagi pelaku ekonomi yang terdigitalisasi.

3. **Indonesia Masuk ke Tahap Red Alert Serangan Siber.**

   Pada tanggal 24 Januari 2022 pakar keamanan siber dari Cissrec, Pratama Persadha, mengatakan bahwa, dalam beberapa waktu terakhir lembaga pemerintahan Indonesia jadi sasaran serangan siber bahkan membuat datanya bocor hingga dijual para peretas (Islami, 2017). Indonesia sudah masuk ke tahap Red Alert. Serangan di negara lain rata-rata satu kali dalam satu caturwulan, tapi di Indonesia bisa berkali-kali dalam satu bulan. Banyaknya serangan siber, salah satunya karena pengambil kebijakan masih awam soal keamanan dan pertahanan siber, belum besarnya politic will dalam membangun pondasi siber, karena semua itu harus datang dari negara seperti UU, maupun kerjasama antar lembaga dan antar negara. Kekurangan lain yang cukup serius adalah tata kelola manajemen keamanan siber yang masih lemah. Selain itu, kesadaran keamanan siber masih rendah (Soewardi, 2013).

4. **Situs Resmi Kostrad dan TNI AD Diserang Hacker**

   Pada tanggal 15 Agustus 2022 dari media online www.msn.com diperoleh informasi, kelompok hacker internasional yang mengatasnamakan diri sebagai Indian Cyber Mafia telah melakukan penyerangan terhadap Komando Cadangan Strategis TNI Angkatan Darat (Kostrad). Situs dengan nama domain www.kostrad.mil.id tidak bisa diakses, hanya muncul tulisan "INDIAN CYBER MAFIA WAS HERE" (Parulian et al., 2021)

5. **Database BIN dan Polri ditawarkan dalam forum jual beli data**

   Pada tanggal 26 Juli 2022 dari media online cyberthreat.id diperoleh informasi Database yang di duga milik Badan Intelijen Negara (BIN) dan Kepolisian Republik Indonesia ditawarkan di forum jual beli data. Seorang pengguna Twitter dengan username @b00km4rkz

mengungkapkan bahwa pada tanggal 14 April 2022, user dengan nama Strovian menjual database miliki BIN dan Kepolisian RI. Database itu berisi 180 dokumen, berisi laporan, strategi, list nama pegawai, ddan data lain. Data tersebut juga memuat data nama, tempat tanggal lahir, pangkat/Gol, NIP/NRP, TMT, serta jabatan terakhir. Sementara itu, untuk database Kepolisian RI, berisi data milik 467.149 anggota polisi yang tersebar di 34 provinsi. Data tersebut berisi nama, unit, email, dan nomor telepon. Artinya bahwa begitu rentannya keamanan siber hal ini diharapka nagar kita dapat meningkatkan kepedulian keamanan dan memperkuat sistem yang dimiliki karena rendahnya kepedulian keamanan siber, menjadi salah satu penyebab mengapa banyak situs pemerintah yang jadi korban peretasan (Putra et al., 2018).

6. **Indonesia Menjadi Negara dengan Index Keamanan Siber Terburuk di Asia Dan Dunia.**
   Pada tanggal 16 Agustus 2022, diperoleh dari media online https://hmstimes.com/ hasil riset Reboot Digital PR Service yang berbasis di Inggris, menyatakan bahwa Indonesia dianggap tidak aman untuk bekerja dari jarak jauh. Indonesia menduduki peringkat pertama dengan skor 82,8 dari 100. Reboot mendapati ada sebanyak 643 komputer yang terinfeksi virus, 1.080 situs phising, dan 1.040 situs mengandung malware (Parulian et al., 2021)

Banyaknya pengguna internet di Asia Tenggara sekitar 70% dari populasi, mengakibatkan rawan terjadinya serangan siber. Pada tanggal 6 Januari 2021, General Manager Kaspersky untuk Asia Tenggara, Yeo Siang Tiong, mengatakan bahwa, pengguna internet di Asia Tenggara berjumlah kurang lebih 70% dari populasi atau sekitar 400 juta orang. Hal ini menjadi celah peretas untuk melancarkan serangan di wilayah Asia Tenggara, karena keterampilan digital yang tidak merata, sehingga faktor manusia menjadi penyebab peretas dapat melancarkan serangan siber. Sepanjang tahun 200 serangan terbanyak berupa:

- Cryptomining artinya istilah lain dari bitcoin mining, yang berarti penambangan bitcoin atau cara mendapatkan bitcoin;
- Phishing artinya upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan;
- Ransomware artinya serangan malware yang dikirim peretas untuk mengunci dan mengenkripsi perangkat komputer milik korban;
- DDos kependekan dari Distributed Denial of Service atau dalam bahasa Indonesia dapat diartikan sebagai Penolakan Layanan secara Terdistribusi (Sudarmadi & Runturambi, 2019)

Penelitian serupa juga pernah dilakukan oleh Anna Rufaidah dengan judul "PENGARUH INTELEGENSI DAN MINAT SISWA TERHADAP PUTUSAN PEMILIHAN JURUSAN" Pada tahun 2015 dalam penelitiannya mengatakan bahwa hasil analisis data menunjukkan terdapat pengaruh yang signifikan antara kecerdasan dan minat siswa terhadap keputusan pemilihan program studi penelitian terdahulu meneliti objek secara gelobal sedangkan dalam penelitian ini objek penelitian lebih spesifik pada faktor-faktor yang berpengaruh terhadap peluang ancaman serangan siber pada KTT G20 perlu mendapatkan perhatian khusus, agar deteksi dini dan cegah dini terhadap setiap ancaman serangan siber KTT G20 dapat dilaksanakan secara maksimal.

METODE

Artikel ini ditulis dengan menggunakan metode kualitatif dengan desain penelitian deskriptif kualitatif dengan tujuan untuk memperdalam pemahaman publik terkait ancaman siber, khususnya

pada gelaran KTT G20. Untuk menjawab pertanyaan penelitian, penulis memanfaatkan data bekas yang diperoleh dari penelitian kepustakaan. Data tersebut kemudian dianalisis secara bertahap, pertama, tahap pengumpulan data yang sudah dimulai bahkan sejak awal penyelidikan; kedua, fase kondensasi data yang terdiri dari meringkas, memfokuskan pada hal-hal penting untuk mendapatkan tema dan polanya untuk mendapatkan deskripsi yang lebih baik dan memungkinkan penulis untuk mendapatkan data tambahan jika diperlukan; ketiga, tahap tampilan data untuk melihat hubungan antar kategori dengan menggunakan teks naratif; dan terakhir, fase penarikan kesimpulan. Hasil investigasi bersifat eksploratif untuk mengidentifikasi, menghitung dan menguraikan masalah atau pertanyaan penelitian, terutama mengenai peran yang dapat dilakukan oleh badan intelijen untuk membantu pemerintah Indonesia mengantisipasi potensi ancaman dari serangan siber baik eksternal maupun internal.

Gambaran singkat mengenai faktor-faktor pendukung dan permasalahan yang dihadapi di lapangan yang dihadapi oleh komunitas intelijen siber untuk melakukan tugas-tugasnya, tulisan ini membatasi topik pembahasan yang terutama akan fokus pada ancaman siber pada gelaran KTT G20. Untuk mendukung argumentasi tersebut, akan disajikan data-data yang diperoleh dari penelitian kepustakaan sehingga memungkinkan pencarian jawaban atas pertanyaan penelitian, “bagaimana potensi ancaman serangan siber pada kegiatan KTT G20 di Indonesia”.

HASIL DAN PEMBAHASAN

Sejak satu dekade terakhir, ketika perkembangan digital semakin bertumbuh, serangan siber di Indonesia meningkat tajam. Hal ini sesuai dengan data yang dikemukakan oleh Badan Siber dan Sandi Negara (BSSN), dimana serangan siber di Indonesia pada Januari-Mei 2020 meningkat drastis jika dibandingkan periode yang sama tahun sebelumnya. Ancaman terhadap hilangnya potensi ekonomi hingga kedaulatan negara cenderung meningkat jika tren peningkatan tersebut terus berlanjut.

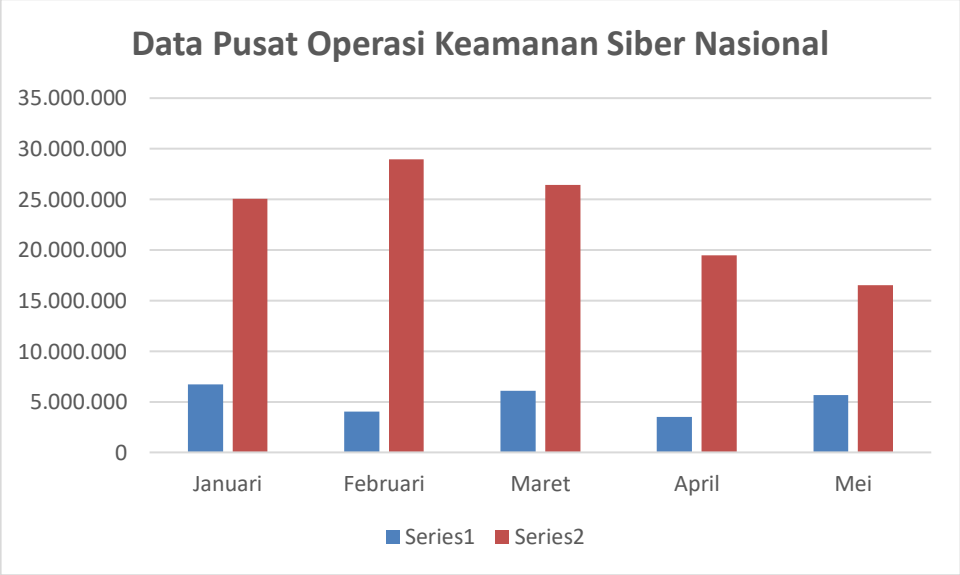


Diagram 1

Serangan siber selama penyelenggaraan KTT G20 di beberapa negara. Penyelenggaraan KTT G 20 yang telah dilaksanakan pada waktu sebelumnya di beberapa negara tidak terlepas dari

serangan siber. Hal ini terindikasi dari berbagai fakta insiden siber pada penyelenggaraan KTT G20 sebagai berikut:

Tabel. 1

Serangan Siber pada KTT G20 di Dunia

Tahun	Lokasi	Keterangan
2009	Amerika-Inggris	Insiden Penyadapan
2010	Amerika, Inggris, Argentina, Korea Selatan	Terjadi insiden penyadapan dan serangan siber terhdap website dan email serta serangan crypto currency Korea Selatan
2011	Perancis	Terjadi serangan siber yang menargetkan dokumen-dokumen mengenai pertemuan G20 dan dokumen yang berhubungan dengan masalah ekonomi internasional. Lebih dari 150 komputer pemerintahan telah diserang. Para aktor tersebut didalangi oleh kaum professional dan teroganisir.
2013	Rusia	Penyelenggaraan KTT G20 di Rusia terjadi penyadapan terhadap 5 menteri Luar Negeri Eropa dan penyebaran malware melalui USB dan Charger telepon genggam. HaL Ini diperkuat Berdasarkan laporan dari kantor Dewan Eropa yang diserahkan kepada intelijen Italia, ditemukan adanya alat penyadap dalam hadiah tersebut. Laporan itu langsung memicu kontroversi, setelah adanya laporan intelijen Amerika Serikat (AS) yang menyadap sekira 34 pemimpin negara di dunia. Rusia pun membantah keras laporan penyadapan tersebut.
2014	Australia	terjadi serangan siber di dukung negara sponsor. Ada sejumlah

		email berbahaya muncul yang berhubungan dengan KTT G20 dikirim ke instansi pemerintah Australia dalam upaya untuk memasuki jaringan komputer dan mencari informasi.
2017	Jerman	Terjadi insiden siber yang menargetkan peserta G20 melalui file pdf atau yang biasa dikenal Acrobat File Format yang diinfeksi dengan berbagai macam virus dimana gadget target akan terinveksi bila membukanya.
2020	Arab Saudi	Terjadi insiden siber mentargetkan infrastruktur penting dan kebocoran data email kementrian keuangan detail yg dirusak
2021	Roma	Terjadi serangan siber di wilayah Italia yang mencakup ibu kota Roma dimana jaringan kesehatannya dilumpuhkan oleh apa yang disebut pemerintah regional, Serangan itu menutup portal Health Lazio dan menghentikan peluncuran vaksinasi di kawasan itu.

Sumber: Olahan Peneliti (2022)

Mencermati berbagai fakta serangan siber dari tahun ketahun baik yang terjadi di Indonesia maupun serangan siber pada penyelenggaraan KTT G20 di berbagai negara sebelumnya, menunjukkan bahwa serangan siber merupakan ancaman nyata dan potensial dan dapat dipastikan akan dilaksanakan oleh aktor-aktor tertentu pada penyelenggaraan KTT G20 di Indonesia.

Berdasarkan fakta-fakta diatas, menunjukkan bahwa serangan siber senantiasa meningkat dari waktu ke waktu. Berbagai bentuk serangan siber selalu berkembang seiring dengan kemajuan teknologi digital itu sendiri. Sasaran serangan siber pun sangat bervariasi sesuai dengan tujuan subyek pelaku dan kepentingan yang ingin dicapainya. Dilihat dari kepentingannya, serangan siber dilakukan, mulai dari hanya kegiatan iseng atau coba-coba, kepentingan finansial untuk mendapatkan keuntungan materi, kepentingan politik untuk mencapai tujuan politik tertentu, kepentingan keamanan/pertahanan maupun kepentingan-kepentingan lainnya sesuai dengan kapasitas dan tujuan pelaku itu sendiri. Perbedaan kepentingan dan tujuan serangan siber tersebut berpengaruh pada sasaran siber itu sendiri. Sehingga jenis-jenis sasaran serangan siber sangat tergantung dari kepentingan atau tujuan serangan siber dilaksanakan.

Secara umum, sasaran serangan siber dapat dikategorikan menjadi tiga jenis sesuai dengan tujuan masing-masing. Sasaran pertama adalah ditujukan untuk mengambil data-data yang akan digunakan untuk bebagai kepentingan. Sasaran kedua, adalah untuk tujuan merusak perangkat atau

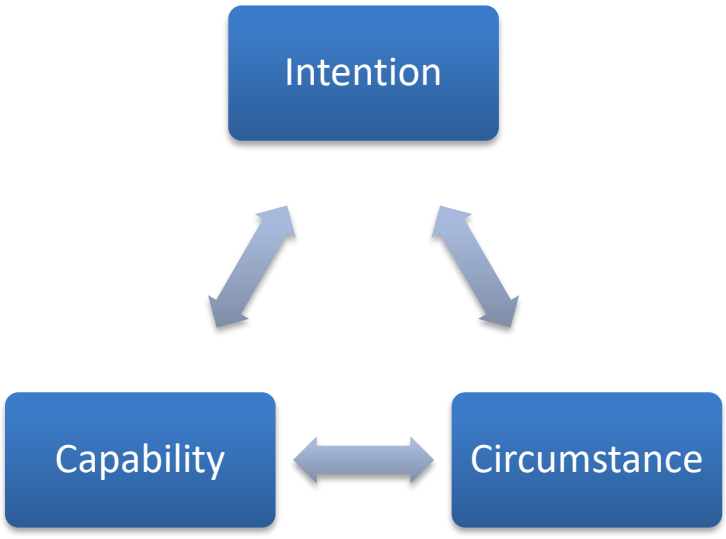
sistem, baik perangkat lunak maupun perangkat keras. Sasaran ketiga, siber digunakan sebagai sarana penyampaian pesan penggalangan, propaganda dan sebagainya.

a. Sasaran serangan siber pencurian data dan dokumen. Serangan siber yang ditujukan untuk mengambil data-data tertentu merupakan sasaran serangan siber yang banyak terjadi. Hal ini sesuai dengan data BSSN, bahwa serangan siber dengan sasaran mengumpulkan data/informasi terhitung sampai bulan April 2022 sebanyak 43%. Pada penyelenggaraan KTT G20 di Indonesia yang akan digelar pada bulan November 2022, serangan siber yang ditujukan pada sasaran pencurian data atau pengumpulan data, berpotensi besar akan terjadi. Hal ini disebabkan penyelenggaraan KTT G20 merupakan kegiatan yang sangat penting untuk membahas isu-isu strategis berbagai bidang yang sangat dibutuhkan banyak kalangan, baik kalangan negara tertentu maupun non negara. Disamping itu, dalam kegiatan KTT G20 juga terdapat berbagai dokumen penting yang dibutuhkan oleh berbagai kepentingan. Seperti halnya pada penyelenggaraan KTT G20 yang diselenggarakan sebelumnya di berbagai negara, serangan siber dengan sasaran pencurian data, dokumen dan informasi lainnya, selalu menjadi ancaman potensial dalam event tersebut. Apalagi dalam event tersebut masih dalam suasana pertikaian negara Rusia dengan Ukraina yang didukung masing-masing aliansinya, sehingga kemungkinan serangan siber terhadap negara yang saling bertikai maupun negara pendukungnya sangat mungkin terjadi.
b. Sasaran serangan siber untuk perusakan system/perangkat. Sasaran serangan siber dengan menyasar/bertujuan untuk merusak sistem juga merupakan potensi ancaman yang perlu diwaspadai. Berbagai data menunjukkan bahwa serangan siber yang mengancam sistem perangkat lunak maupun perangkat keras sering kali ditemukan. Ancaman tersebut dapat dimulai dari menjebol situs, merubah konten situs, memasukkan berbagai macam virus sehingga data yang ada rusak atau tidak bisa diakses, sampai pada perusakan perangkat keras seperti komputer atau perangkat keras lain yang terhubung dengan computer. Kasus serangan virus Stuxnet pada instalasi nuklir Iran merupakan fakta yang dapat dijadikan acuan adanya sasaran serangan siber untuk merusak sistem atau perangkat yang terkait dengan komputer. Serangan siber lain ditambahkan yg merusak perangkat, kemudian Serangan WannaCry membuat ransomware dan malware dikenal oleh semua pengguna, termasuk mereka yang tidak dapat membedakan byte dengan bite. Dalam empat hari, penyebaran WannaCry membuat lumpuh lebih dari 200 ribu komputer di 150 negara yang Terjadi di beberapa rumah sakit, WannaCry mengenkripsi keseluruhan perangkat, termasuk peralatan medis. Bahkan beberapa pabrik terpaksa menghentikan kegiatan produksi.

   Beberapa kasus lain tentang kerusakan perangkat, terutama perangkat komputer akibat serangan siber juga banyak terjadi. Termasuk pada penyelenggaraan G20 di Perancis serangan siber juga menyasar komputer-komputer pemerintah sebanyak kurang lebih 150 komputer diserang oleh aktor-aktor professional. Mencermati berbagai fakta tersebut, serangan siber dengan sasaran perusakan sistem atau perangkat pada penyelenggaraan G20 di Indonesia sangat mungkin dilaksanakan oleh aktor-aktor tertentu dengan tujuan utama untk mengganggu jalannya event KTT G20 tahun 2022.
c. Sasaran serangan siber digunakan sebagai sarana penggalangan. Sasaran serangan siber selain menyasar pencurian data dan perusakan berbagai perangkat, juga seringkali digunakan untuk sasaran psikologi, opini masyarakat atau dalam terminologi intelijen lebih dikenal dengan penggalangan. Sasaran ini tidak kalah berbahayanya dengan sasaran

lainnya, karena dampak yang ditimbulkan lebih luas menyangkut berbagai efek. Serangan siber dengan sasaran penggalangan adalah untuk menciptakan opini tertentu sesuai dengan keinginan aktor pelakunya. Serangan ini dapat berupa penyesatan informasi, penyebaran berita hoaks, konten-konten provokasi untuk memancing kemarahan massa, serta konten-konten lainnya yang bertujuan menciptakan ketidak percayaan kepada pemerintah (Herdiana et al., 2021). Kasus serangan ini sudah banyak terjadi dan telah menimbulkan dampak kerusakan fisik, perpecahan dan berbagai dampak lainnya, termasuknya tumbuhnya rasa kebencian terhadap obyek tertentu. Berbagai fakta tentang kasus pergerakan masa, bentrokan antar kelompok dan terjadinya polarisasi dikalangan masyarakat yang dipicu oleh konten-konten media sosial adalah salah satu bukti nyata dampak dari penggunaan siber untuk mempengaruhi opini massa. Dalam konteks penyelenggaraan KTT G20 di Indonesia. Kasus-kasus tersebut masih sangat mungkin dilakukan oleh pihak-pihak tertentu dengan tujuan utama adalah untuk mendegradasi penyelenggaraan KTT G20 itu sendiri dan tujuan utamanya adalah untuk menciptakan citra buruk pemerintah. Hal ini sudah dapat dirasakan, pada saat pertama kali pemerintah terpilih sebagai presidensi G20 dan rencana penyelenggaraan KTT G20 di Indonesia. Serangan media sosial yang berupaya mempengaruhi opini massa dengan mendiskreditkan kredibilitas pemerintah terkait G20, sangat sering terjadi.

Berdasarkan fakta dan analisis yang telah disebutkan di atas dapat menunjukkan bahwa ancaman siber pada penyelenggaraan KTT G20 di Indonesia merupakan ancaman nyata, yang dapat dipastikan akan terjadi. Namun demikian ancaman siber dapat terjadi karena ada faktor faktor yang mempengaruhi, sehingga ancaman tersebut bisa terlaksana. Secara umum ada tiga faktor yang berpengaruh terjadinya suatu ancaman siber, yaitu faktor niat pelakunya, faktor kemampuan pelakunya dan faktor lingkungan sararan yang menjadi target (Vandepeer, 2011).



Tabel 1 Faktor-faktor yang mempengaruhi ancaman

Faktor pertama adalah faktor niat atau kehendak *(Intentions)* pelaku ancaman. Selama tidak ada niat pelaku untuk melakukan tindakan tertentu sehingga berdampak timbulnya potensi

ancaman, maka potensi ancaman tersebut relatif tidak ada. Dalam konteks niat melakukan serangan siber pada penyelenggaraan KTT G20, maka dapat dipastikan terdapat niat yang relative besar. Hal ini setidaknya didasarkan pada tiga analisis.

Analisis pertama adalah berdasarkan fakta-fakta penyelenggaraan KTT G20 sebelumnya, dimana serangan siber terhadap penyelenggaraan event tersebut selalu ada. Dengan asumsi tersebut dapat dipastikan bahwa niat untuk melakukan serangan siber pada penyelenggaraan KTT G20 di Indonesia pun pasti ada. Analisa kedua, didasarkan pada nilai pentingnya event tersebut, sehingga tentu banyak negara atau pihak pihak yang mempunyai kepentingan untuk mendapatkan data-data, dokumen atau melakukan Tindakan tertentu sesuai dengan kepentingannya masing-masing. Analisa ketiga, didasarkan perkembangan IT itu sendiri yang telah mengalami kemajuan yang begitu pesat dan digunakan di berbagai bidang dengan segala bentuk keperluannya. Perkembangan IT yang begitu pesat, telah menimbulkan berbagi efek positif dan negatif. Positifnya, perkembangan IT telah banyak memberikan kemudahan-kemudahan dalam melaksanakan aktifitas sehari-hari. Sedangkan efek negatifnya, kemajuan IT juga sering digunakan untuk tindakan yang merugikan, diantaranya melakukan serangan siber. Kejadian serangan siber ini terjadi setiap saat yang menyasar ke berbagai bidang. Artinya kemajuan IT dan kemudahan penggunaan IT menimbulkan dorongan atau niatan untuk melakukan serangan siber selalu ada setiap saat, ke berbagai bidang sasaran, yang tidak menutup kemungkinan juga menyasar kepada KTT G20.

Faktor kedua adalah kemampuan atau *Capability*. Kemampuan merupakan faktor yang diperlukan agar niat melakukan tindakan tertentu dapat dilaksanakan. Artinya, niat yang sudah dimiliki untuk melakukan tindakan tertentu dapat dilaksanakan apabila mempunyai kemampuan yang sesuai. Sebesar apapun niat yang dimiliki tanpa didukung dengan kemampuan yang mencukupi, maka niat tersebut tidak akan pernah tercapai. Faktor Kemampuan jika dikaitkan dengan potensi ancaman siber pada penyelenggaraan KTT G20, maka pelaku atau calon pelaku relative mempunyai kapasitas atau kemampuan untuk melakukan serangan siber pada penyelenggaraan KTT G20. Hal ini didasarkan pada fakta-fakta berbagai kejadian serangan siber yang menyasar berbagai obyek. Disamping itu, kemampuan melakukan serangan siber tersebut juga ditunjukkan pada perkembangan kecanggihan melakukan serangan siber itu sendiri yang semakin berkembang dari waktu ke waktu (Prananda, 2021)

Faktor ketiga adalah lingkungan sasaran serangan dilancarkan atau *Circumtances*. Circumtances adalah situasi lingkungan obyek serangan, dimana tempat/lokasi sasaran yang sudah ditetapkan oleh pelaku penyerangan. Berbeda dengan dua faktor sebelumnya, yang berasal dari diri pelaku/subyek yang melakukan serangan, maka Circumtances merupakan situasi obyek sasaran apakah rentan terhadap serangan atau tidak. Semakin rentan atau lemah obyek sasaran, maka akan semakin mudah mendapatkan serangan. Demikian juka semakin baik obyek sasaran dalam mengantisipasi serangan, maka pelaku akan semakin sulit untuk melakukan serangan. Dengan demikian, walaupun ada niat pelaku yang didukung oleh kemampuan untuk melakukan serangan, tetapi lingkungan/obyek serangan mempunyai proteksi yang terhadap potensi serangan, maka tidak akan terjadi serangan. Jika faktor circumtances dikaitkan dengan potensi ancaman siber pada penyelenggaraan KTT G20 di Indonesia, maka sangat tergantung pada kemampuan mendeteksi ancaman dan pemenuhan kapasitas dalam menghadapi ancaman serangan siber itu

sendiri. Namun jika dilihat dari banyaknya serangan siber yang terjadi di Indonesia dari tahun ke tahun, maka lingkungan kita masih sangat rentan mendapatkan serangan siber. faktor lingkungan *(circumtances)* menjadi faktor utama untuk menangkal serangan siber pada KTT G20.

Dari penjelasan tersebut, ada tiga cara yang dapat digunakan untuk menangkal serangan siber pada penyelenggaraan KTT G20 di Indonesia. Cara pertama adalah dengan membatal niatkan pelaku untuk melakukan serangan siber. Cara yang kedua adalah dengan meniadakan kemampuan pelaku untuk melakukan serangan siber. cara yang ketiga adalah dengan menciptakan situasi lingkungan sendiri terhindar dari serangan siber. Untuk cara pertama dan kedua mungkin lebih sulit dilaksanakan, karena selain pelakunya belum dapat diketahui, upaya untuk membatal niatkan dan meniadakan kemampuan pelaku serangan siber juga tidak mudah, karena niat dan kemampuan melakukan serangan di dunia maya/siber sifatnya tidak kasat mata. Oleh karena itu faktor lingkungan sendiri *(circumtances)* merupakan satu-satunya faktor yang dapat dilaksanakan untuk menghadapi serangan siber pada penyelenggaraan KTT G20 (Vandepeer, 2011).

Lingkungan atau obyek serangan siber merupakan faktor utama yang dapat dikembangkan untuk menangkal serangan siber pada penyelenggaraan KTT G20. Terdapat dua aspek penting yang sangat berpengaruh dalam menciptakan lingkungan yang mampu menangkal serangan siber pada KTT G20, yaitu sumber daya manusia (SDM) dan Material Khusus (Matsus) yang digunakan untuk kegiatan penyelenggaraan KTT G20 itu sendiri (Prananda, 2021) Keduanya merupakan dua hal pokok yang harus terpenuhi secara kuantitas maupun kualitas. Kekurangan salah satu dari hal tersebut berdampak pada tidak maksimalnya dalam menghadapi serangan siber. ketersedian kedua aspek tersebut (SDM dan Matsus) akan menciptakan beberapa kondisi ancaman sebagai berikut:

Ancaman minimal karena proteksi maksimal. Hal ini bisa terjadi apabila ketersediaan SDM yang memadai ditopang dengan ketersediaan Matsus yang cukup akan dapat meminimalkan ancaman siber, Hal ini disebabkan selain kesadaran pengamanan personel memadai, kapasitas untuk menangkal serangan siber dari luar juga terpenuhi karena ketersediaan matsus/fasilitas yang dibutuhkan.

Ancaman intern minimal tapi ancaman ekstern besar, kondisi ini bisa terjadi jika ketersediaan SDM yang cukup tapi tidak ditopang dengan ketersediaan Matsus yang memadai, maka potensi ancaman yang berasal dari dalam relatif kecil, tapi potensi ancaman dari luar relatif besar. Hal ini disebabkan kesadaran keamanan siber sudah dimiliki masing-masing namun tidak punya kapasitas menghadapi serangan siber dari luar karena kurangnya fasilitas/peralatan.

Timbulnya ancaman/kerawanan dari dalam dan dari luar. Kondisi ini bisa terjadi jika ketersediaan SDM tidak cukup tapi Matsus/fasilitas pendukung memadai. Kondisi ini akan berdampak timbulnya kerawanan dari dalam dan dari luar. Hal ini disebabkan selain kesadaran pengaman intern kurang, kapasitas SDM yang kurang juga tidak bisa menggunakan matsus secara optimal. Sehingga kondisi ini berpotensi menimbulkan kerawanan baik dari dalam maupun dari luar.

Ancaman dari dalam dan dari luar sama sama besar. Kondisi ini bisa terjadi jika ketersediaan SDM dan matsus tidak mencukupi. Kondisi ini merupakan kondisi yang paling parah yang berdampak pada proteksi serangan siber berada pada titik yang paling rendah. Sehingga ancaman serangan siber berada pada titik yang paling berbahaya.

Sumber ancaman Siber pada KTT G20

Sumber ancaman serangan siber pada penyelenggaraan KTT G20 di Indonesia merupakan faktor penting yang perlu dicermati. Ada dua sumber ancaman siber yang berpotensi mengancam penyelenggaran KTT G20, yaitu ancaman dari luar dan ancaman dari dalam (Volti, 2005)

1. Sumber ancaman eksternal. Sumber ancaman yang bersumber dari luar, adalah sumber ancaman serangan siber yang dilakukan oleh aktor-aktor luar negeri. Kemungkinan serangan siber pada penyelenggaraan KTT G20 yang bersumber dari luar negeri dapat disponsori oleh aktor negara (state actor) dan aktor non negara (non state actor). Keduanya mempunyai potensi untuk melakukan serangan siber pada KTT G20 karena mempunyai berbagai kepentingan masing-masing (Suratman, 2017)
   a. State Actor. Serangan siber yang disponsori oleh negara tertentu sangat mungkin terjadi. Hal ini selain didasarkan pada fakta-fakta penyelenggaraan sebelumnya, juga didasarkan atas urgensi kepentingan yang sedang berkembang saat ini. KTT G20 mempunyai posisi sangat penting saat ini, disaat kondisi global sedang mengalami berbagai masalah, khususnya masalah ekonomi akibat dampak covid dan konflik antar negara. Kebutuhan informasi berkaitan dengan berbagai isu global tentu sangat diperlukan oleh beberapa negara, sehingga mendorong negara tersebut berupaya untuk mendapatkan dengan berbagai cara termasuk dengan melakukan serangan siber. Selain ditujukan untuk mendapatkan data, serangan siber yang disponsori oleh negara, kemungkinan juga bisa ditujukan untuk menyerang peserta lain yang selama ini saling bermusuhan.
   b. Non state actor. Serangan siber pada KTT G20 di Indonesia juga berpotensi dilakukan kelompok-kelompok atau perorangan yang berasal dari luar negeri. Berbagai kelompok masyarakat baik yang berupa Lembaga Swadaya Masyarakat, perusahaan-perusahaan, atau kelompok masyarakat lain yang punya kepentingan terkait isu global dan G20 berpotensi sebagai sumber serangan siber pada KTT G20. Selain itu kelompok-kelompok maupun perorangan yang bersifat “peselancar”/petualang dunia siber juga berpotensi melakukan serangan siber pada KTT G20, terutama bertujuan untuk mendapatkankeuntungan finansial dengan menjual data yang berhasil didapatkan dengan melakukan serangan siber.

2. Sumber ancaman internal. Sumber ancaman seangan siber yang berasal dari dalam/internal adalah pelaku-pelaku serangan siber yang berasal dari dalam negeri, potensi ini juga sangat besar terjadi, jika dilihat dari fakta-fakta serangan siber yang terjadi di Indonesia cenderung meningkat dari waktu-kewaktu. Sasaran dan metode yang digunakanpun semakin bervariasi, termasuk aktor pelakunya juga semakin meningkat (Clarke, 2013). Ancaman serangan siber bersumber dari dalam negeri dapat dilakukan secara perorangan maupun secara kelompok yang berasal dari kalangan masyarakat. Selain dari kalangan masyarakat, ancaman serangan siber dan kerawanan terkait denga aktifitas siber juga bisa berasal dari internal penyelenggara itu sendiri (Suratman, 2017)
   a. Sumber Masyarakat. Masyarakat Indonesia bisa menjadi sumber ancaman serangan siber KTT G20 di Indonesia. Berbagai kelompok masyarakat maupun perorangan mempunyai banyak kepentingan terkait penyelenggaraan KTT G20 (van Creveld, 2010). Kepentingan

tersebut, mulai dari upaya coba-coba, upaya pencurian data, penjebolan situs, perusakan sistem sampai melakukan penggalangan dengan menyebarkan konten-konten tertentu melalui internet. Masih banyaknya kelompok oposan yang berbasiskan parpol, ormas, suku dan lainnya, juga berpotensi terlibat dalam upaya melakukan ancaman serangan siber terhadap penyelenggaraan KTT G20 (Coghlan, 2010).

b. Internal penyelenggara. Sumber ancaman serangan siber bisa juga berasal dari personel penyelenggara KTT G20 itu sendiri. Potensi ini dapat terjadi karena faktor kecerobohan dan faktor penyusupan (Doeser & Eidenfalk, 2013). Faktor kecerobohan yang disebabkan kurangnya kapasitas personel, rendahnya kedisiplinan dan kurangnya kesadaran keamanan dapat berpotensi terjadinya serangan siber yang bersumber dari dalam/internal penyelenggara . Selain kecerobohan, serangan siber yang berasal dari internal penyelenggara bisa disebabkan karena adanya penyusupan pihak tertentu secara langsung maupun menggunakan personel lain (Warner, 2001).

CONCLUSION

Berdasarkan hasil penelitian dan analisis di atas, dapat disimpulkan bahwa dalam mencermati berbagai fakta dan analisa peta ancaman serangan siber pada penyelenggaraan KTT G20 di Indonesia, menunjukkan bahwa potensi serangan siber pada event KTT G20 relatif besar. Hal ini didasarkan pada fakta-fakta dan data tentang penyelenggaraan sebelumnya dan perkembangan ancamanan siber saat ini. Selain itu kecenderungan meningkatnya serangan siber dan belum kondusifnya situasi global serta banyaknya kepentingan negara-negara tertentu terhadap negara lain, juga menjadi dasar perkiraan potensi ancaman serangan siber pada penyelenggaraan KTT G20 yang relatif besar. Faktor-faktor yang berpengaruh terhadap peluang ancaman serangan siber pada KTT G20 perlu mendapatkan perhatian khusus, agar deteksi dini dan cegah dini terhadap setiap ancaman serangan siber KTT G20 dapat dilaksanakan secara maksimal.

REFERENCES

Astuti, W. R. D., & Fathun, L. M. (2020). Diplomasi Ekonomi Indonesia di Dalam Rezim Ekonomi G20 Pada Masa Pemerintahan Joko Widodo. *Intermestic: Journal of International Studies*, *5*(1), 47–68. Google scholar

Clarke, G. (2013). *Civil society in the Philippines: Theoretical, methodological and policy debates*. Routledge. Google scholar

Coghlan, D. (2010). War And The strategist of the twenty-first century. *Australian Army Journal*, *7*(1), 165–172. Google scholar

Dewi, I. G. A. K. I. (2022). Peran Human Capital Dan Teknologi Informasi Pada Organizational Performance Dalam Persiapan Presidensi G20. *Jurnal Ekonomi, Manajemen, Bisnis, Dan Sosial (Embiss)*, *2*(4), 646–653. Google scholar

Doeser, F., & Eidenfalk, J. (2013). The importance of windows of opportunity for foreign policy change. *International Area Studies Review*, *16*(4), 390–406. Google scholar

Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT: Information Communication & Technology*, *20*(1), 42–52. Google scholar

Islami, M. J. (2017). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *8*(2), 137–144. Google scholar

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, *1*(2), 85–92. Google scholar

Prananda, A. (2021). Sinergi Lembaga Intelijen Dalam Menghadapi Ancaman Siber Di Indonesia. *Peperangan Asimetris*, *7*(1), 51–71. Google scholar

Putra, R. D., Supartono, S., & Deni, D. A. R. (2018). Ancaman Siber Dalam Persfektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta). *Peperangan Asimetris*, *4*(2). Google scholar

Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. *Media Informasi Ditjen Pothan Menhan*, 31–35. Google scholar

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber Dan Sandi Negara (Bssn) Dalam Menghadapi Ancaman Siber Di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 157–178. Google scholar

Suratman, Y. P. (2017). Penggunaan Strategi Operasi Kontra Intelijen dalam Rangka Menghadapi Ancaman Siber Nasional. *Jurnal Pertahanan & Bela Negara*, *7*(2), 1–18. Google scholar

van Creveld, M. (2010). *Technology and war: From 2000 BC to the present*. Simon and Schuster. Google scholar

Volti, R. (2005). *Society and technological change*. Macmillan. Google scholar

Warner, M. (2001). *Central Intelligence: Origin and Evolution*. Central Intelligence Agency. Google scholar