Aurelia: Jurnal Penelitian dan Pengabdian Masyarakat Indonesia
E-ISSN: 2964-2493 P-ISSN: 2962-0430
Vol. 4 No. 1 Januari 2025

Analisis Hubungan Ancaman Siber dan Strategi Pengamanan Siber pada KTT G20 di Bali Tahun 2022

Abdul Ghofur[1] Priyanto[2] Agus H.S. Reksoprodjo[3]
Universitas Pertahanan Republik Indonesia
Email: abdul.ghofur@sp.idu.ac.id[1]

Abstrak

Konferensi Tingkat Tinggi (KTT) G20 di Bali tahun 2022 menjadi salah satu perhelatan internasional yang memiliki tingkat kerawanan tinggi terhadap ancaman siber. Ancaman siber yang kompleks, seperti peretasan, Phishing, dan Distributed Denial of Service (DDoS), menuntut penerapan strategi pengamanan siber yang menyeluruh dan terintegrasi. Tulisan ini bertujuan untuk menganalisis dinamika ancaman siber pada KTT G20 tahun 2022 dan pola hubungannya dengan strategi pengamanan siber. Metode penelitian yang digunakan adalah kualitatif dengan melakukan wawancara terhadap para narasumber yang terlibat langsung pada pelaksanaan pengamanan siber KTT G20 di Bali tahun 2022. Hasil pembahasan pada tulisan ini menunjukkan jenis-jenis ancaman siber yang dominan, elemen-elemen penting strategi pengamanan siber seta pola hubungan antara ancaman siber dan strategi pengamanan siber pada KTT G20 tahun 2022. Tulisan ini menegaskan bahwa efektivitas strategi pengamanan siber sangat bergantung pada pemahaman mendalam terhadap karakteristik ancaman yang dihadapi serta respons cepat terhadap insiden siber. Temuan ini diharapkan dapat menjadi referensi dalam pengembangan kebijakan keamanan siber untuk acara berskala internasional di masa mendatang.

Kata Kunci: Ancaman Siber, Strategi, Keamanan Siber, KTT G20

PENDAHULUAN

Kemajuan teknologi informasi seperti *Internet of Things* (IoT) dan *Artificial Intelligence* (AI) telah memberikan kemudahan dan efesiensi dalam kehidupan sehari-hari baik yang dilakukan oleh individu maupun organisasi. Kemudahan dan efesiensi tersebut telah mendorong terjadinya tranformasi digital yang sangat masif. Berdasarkan *Digital 2024 Global Overview Report*, jumlah pengguna internet global secara individu telah mencapai 5,35 miliar orang pada Januari 2024. Jumlah tersebut mencapai 66,2% dari populasi global yang totalnya 8,08 miliar orang. Jumlah pengguna internet global secara individu pada Januari 2024 bertambah sekitar 190 juta orang atau naik 3,69% dibanding periode sama tahun lalu yang masih 5,16 miliar orang. Kondisi tersebut menjadi tantangan tersendiri karena semakin meningkat akses terhadap internet, maka potensi kerentanan yang dapat dieksploitasi oleh penyerang siber (*threat actors*) juga semakin meningkat (We Are Social, 2023, 2024). AwanPintar.id, penyedia layanan keamanan siber di Indonesia, merilis laporan yang menyebutkan bahwa tren serangan siber di Indonesia pada semester pertama tahun 2024 meningkat 6 (enam) kali lipat jika dibandingkan pada periode yang sama pada tahun 2023 (AwanPintarid, 2024). Jumlah serangan siber pada semester pertama tahun 2024 mencapai 2.499.486.085 serangan sementara pada semester pertama tahun 2023 berjumlah 347.172.666 serangan. IT Governance, penyedia layanan keamanan siber global menyebutkan bahwa selama periode Januari hingga April 2024 telah terjadi insiden kebocoran data di seluruh dunia sebanyak 35.900.145.035 dengan 9.478 insiden yang diungkapkan ke publik. Sementara, *Check Point Research* merilis tren serangan siber pada kuartal 2 tahun 2024 yang menunjukkan peningkatan 30% jika dibandingkan serangan siber pada periode yang sama

tahun 2023. Berdasarkan data tersebut, dapat diketahui bahwa terjadi tren peningkatan serangan siber dari tahun ke tahun (AwanPintarid, 2024; Check Point Research, 2024; IT Governance, 2024).

Serangan siber tidak hanya menyasar individu dan organisasi strategis, namun juga menyasar acara-acara internasional yang dihadiri oleh individu strategis yang disebut dengan *High Profil Person*/*Very Important Person* (VIP). VIP secara umum merepresentasikan individu yang dianggap memiliki pengaruh, kekuasaan, atau status yang signifikan, sehingga mereka layak mendapatkan layanan atau perlakuan khusus . VIP bisa mencakup tokoh publik seperti selebriti, politisi, eksekutif perusahaan, atau pejabat pemerintah. Crelier (2019) menyebutkan bahwa sejak tahun 2010, aktivitas keamanan siber pada acara internasional terus mengalami peningkatan baik dari sisi jumlah serangan dan kompleksitasnya, jumlah *threat actors* dan jenis peralatan yang digunakan. Salah satu insiden siber yang melibatkan langsung VIP dalam hal ini pemimpin negara adalah insiden siber yang terjadi pada KTT G20 ke-9 tahun 2014 di Brisbane, Australia. Para pemimpin negara peserta KTT G20 mengalami kebocoran data pribadi. Informasi pribadi seperti nomor paspor, tanggal lahir, detil informasi visa dari para pemimpin negara yang menghadiri pertemuan puncak KTT G20 mengalami kebocoran. Insiden berikutnya adalah kelompok *hacktivist* bernama *Dirty Work* memasang kamera CCTV palsu yang diprogram untuk memproyeksikan pesan aktivis yang bertentangan dengan kepentingan G20 secara keseluruhan. Beberapa kamera palsu ditemukan pada menit terakhir, sebelum tokoh-tokoh terkenal seperti presiden dapat melihat pesan yang diproyeksikan.

Berdasarkan KTT G20 ke-15 Riyadh, Indonesia ditetapkan sebagai tuan rumah perhelatan internasional negara-negara G20 atau yang dikenal dengan Presidensi G20 tahun 2022. Sebagai penyelenggara Presidensi G20 tahun 2022, Indonesia bertugas menyelenggarakan berbagai tingkat pertemuan G20 yang berlangsung sejak 1 Desember 2021 hingga kegiatan puncak berupa Konferensi Tingkat Tinggi (KTT) yang diselenggarakan di Bali pada tanggal 15-16 November 2022. Menurut Crelier (2019) yang melakukan penelitian keamanan siber pada acara G20 dan Olimpiade serta menurut Nasser & Al-Dosari (2020) yang melakukan penelitian terhadap keamanan siber *FIFA World Cup* di Qatar tahun 2022, menyebutkan bahwa aspek penting dalam keamanan siber acara-acara internasional adalah pengembangan strategi manajemen risiko keamanan siber yang komprehensif dalam rangka menghalau berbagai jenis ancaman siber. Berdasarkan kondisi-kondisi tersebut, menarik untuk dilakukan analisis, bagaimana dinamika ancaman siber pada KTT G20 di Bali tahun 2022 dan bagaimana hubungan ancaman siber tersebut dengan strategi pengamanan siber KTT G20.

Tinjauan Pustaka

Pengertian Ruang Siber

Ruang siber adalah lingkungan virtual yang tercipta dari interaksi teknologi informasi, data, perangkat digital, jaringan komunikasi, dan penggunanya. Ruang ini tidak memiliki lokasi fisik, tetapi eksis melalui infrastruktur teknologi informasi global yang menghubungkan berbagai perangkat dan sistem. Ruang siber berfungsi sebagai medium untuk berbagai aktivitas, termasuk komunikasi, perdagangan, hiburan, pendidikan, hingga operasi militer. Patrascu (2019) menyebutkan bahwa ruang siber terbentuk dari 3 (tiga) lapisan yang saling terkait, masing-masing mewakili aspek yang berbeda tentang bagaimana interaksi dan operasi digital terjadi. Ketiga lapisan tersebut adalah:

1. Pertama, *Physical Layer* (Lapisan Fisik). Lapisan fisik mencakup seluruh infrastruktur dan perangkat keras yang membentuk dasar ruang siber. Komponen lapisan fisik terdiri dari komponen geografis (tanah, air, udara dan ruang) yang menjadi domain infrastruktur siber dan komponen jaringan fisik terdiri dari infrastruktur jaringan sistem teknologi dan informasi, yang didukung oleh berbagai konektor, termasuk tautan kabel dan nirkabel serta

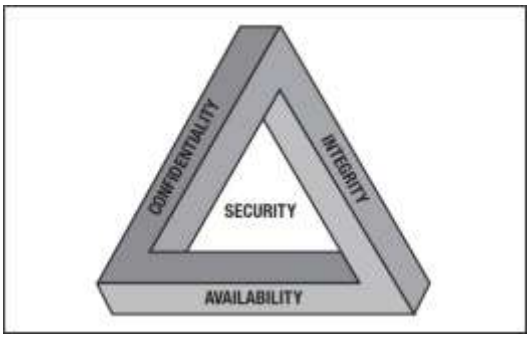
satelit. Lapisan ini sangat penting karena menyediakan infrastruktur yang diperlukan untuk semua komunikasi digital. Keamanan fisik terhadap lapisan fisik ini menjadi perhatian penting, karena kerusakan atau sabotase pada infrastruktur fisik dapat menyebabkan gangguan serius pada ruang siber secara regional maupun global.

2. Kedua, *Logical Layer* (Lapisan Logika). Lapisan logika mencakup perangkat lunak, protokol, dan sistem yang memungkinkan komunikasi antar perangkat dan pengelolaan data. Komponen utamanya meliputi: protokol komunikasi seperti TCP/IP, DNS, dan HTTP, sistem operasi dan aplikasi yang menjalankan perangkat keras, serta arsitektur jaringan yang memungkinkan konektivitas global. Lapisan logika adalah tempat di mana aliran data dikelola dan diorganisasi. Dalam konteks keamanan siber, lapisan ini sering menjadi target serangan siber seperti peretasan, pencurian data, atau manipulasi protokol. Keamanan pada lapisan ini memerlukan penguatan sistem enkripsi, pembaruan perangkat lunak, dan pengelolaan kerentanan sistem.
3. Ketiga, *Cyber-Persona Layer* (Lapisan Cyber-Persona). Lapisan Cyber-Persona adalah representasi digital dari pengguna atau entitas dalam ruang siber, baik melalui nama pengguna, alamat email, profil media sosial, atau identitas lain yang digunakan untuk berinteraksi di dunia maya. Identitas ini tidak hanya terbatas pada individu, tetapi juga mencakup organisasi, lembaga, atau perangkat yang memiliki kehadiran digital. Pada lapisan ini, ancaman siber yang sering terjadi berupa social engineering (rekayasa sosial), *profiling* (pelacakan), propaganda digital, dan manipulasi informasi. Keamanan pada lapisan ini membutuhkan literasi pengguna, kebijakan yang kuat, dan kerja sama antar stakeholder untuk mengelola risiko yang muncul.

Pengelolaan Ruang Siber

Dalam pengelolaan keamanan siber, terdapat 3 (tiga) pilar utama yang saling terhubung satu dengan yang lainnya. Ketiga pilar tersebut adalah: *People*, *Process*, dan *Technology* (Harrell, 2017; Marchewka, 2015). *People* (manusia) adalah aspek penting dalam pengelolaan keamanan siber. Meskipun teknologi terus berkembang, manusia tetap menjadi aktor utama dalam setiap aktivitas di ruang siber. Namun demikian, manusia juga sering menjadi titik lemah yang dapat dieksploitasi oleh *threat actors* sehingga menimbulkan insiden siber yang merugikan individu dan organisasi. *Process* (proses) adalah kerangka kerja yang mengatur pelaksanaan keamanan siber. Proses ini mencakup kebijakan, prosedur, dan standar yang dirancang untuk mengelola risiko, mendeteksi ancaman, dan merespon serangan. Misalnya, penerapan kerangka kerja ISO 27001 dapat membantu organisasi menciptakan sistem manajemen keamanan informasi yang terstruktur. Harrell (2017)menyebutkan bahwa proses yang jelas dan konsisten memungkinkan organisasi untuk mengidentifikasi celah keamanan dan mengambil langkah mitigasi sebelum ancaman menjadi serius. Proses ini juga harus dievaluasi secara berkala untuk menyesuaikan dengan dinamika ancaman yang terus berubah. *Technology* (teknologi) berfungsi menyediakan alat dan solusi untuk melindungi aset digital dari ancaman siber. Teknologi seperti firewall, sistem deteksi intrusi (*Intrusion Detection Systems,* IDS), dan perangkat lunak enkripsi memainkan peran penting dalam menciptakan lapisan pertahanan terhadap serangan. Harrell (2017) menjelaskan bahwa teknologi hanya efektif jika didukung oleh manusia yang memahami cara menggunakannya dan proses yang dirancang dengan baik. Oleh karena itu, organisasi perlu berinvestasi pada teknologi yang tepat dan memastikan bahwa teknologi tersebut dikelola dengan efisien dan optimal. *Information Systems Audit and Control Association* (ISACA) menjelaskan bahwa keamanan siber mencakup tiga prinsip utama yang dikenal sebagai CIA Triad, yaitu: *Confidentiality* (Kerahasiaan), *Integrity* (Integritas), dan *Availability* (Ketersediaan) (ISACA, 2015). Kerahasiaan memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Integritas melindungi data dari perubahan yang

tidak sah, memastikan bahwa informasi yang diterima adalah akurat dan utuh. Ketersediaan menjamin bahwa informasi dan sistem dapat diakses oleh pengguna yang sah kapan pun diperlukan.



Gambar 1. Prinsip Utama Keamanan Siber
Sumber: (ISACA, 2015)

Dalam kerangka kerja *National Institute of Standards and Technology* (NIST), terdapat 5 (lima) aktivitas utama keamanan siber, yaitu: *Identify, Protect, Detect, Respond*, dan *Recover* (NIST, 2018).

Gambar 2. Kerangka Kerja NIST
Sumber: (NIST, 2018)

Identify (Identifikasi) merupakan upaya mengembangkan pemahaman organisasi untuk mengelola risiko keamanan siber terhadap sistem, orang, aset, data, dan kemampuan siber. Aktivitas dalam fungsi Identifikasi merupakan pondasi penggunaan kerangka kerja secara efektif. Memahami konteks bisnis, sumber daya yang mendukung fungsi kritis, dan risiko keamanan siber terkait memungkinkan organisasi fokus dan memprioritaskan upaya pengamanan siber sesuai dengan strategi manajemen risiko dan kebutuhan organisasi. *Protect* (Proteksi) merupakan upaya mengembangkan dan melaksanakan keamanan yang sesuai untuk memastikan kesinambungan layanan penting. Fungsi Proteksi mencakup penerapan langkah-langkah pengamanan untuk melindungi data dan sistem kritis. Aktivitas Proteksi melibatkan pengendalian akses, enkripsi data, dan pelatihan staf untuk meningkatkan kesadaran keamanan siber. *Detect* (Deteksi) merupakan upaya mengembangkan dan melaksanakan kegiatan yang sesuai untuk mengidentifikasi insiden siber. Fungsi Deteksi memungkinkan ditemukannya insiden siber secara tepat waktu. Aktivitas Deteksi melibatkan pemantauan aktivitas jaringan dan analisis anomali. Teknologi seperti analitik *Big Data* dan kecerdasan buatan semakin sering digunakan untuk mengidentifikasi pola serangan sebelum menjadi ancaman besar. *Respond* (Respon) upaya mengembangkan dan melaksanakan kegiatan yang sesuai untuk mengambil tindakan mengenai insiden keamanan siber yang terdeteksi. Fungsi

Respons mendukung kemampuan untuk memitigasi dampak insiden siber. Aktivitas Respons meliputi analisis insiden, mitigasi dampak, dan komunikasi kepada pihak terkait. *Recover* (Pemulihan) upaya mengembangkan dan melaksanakan kegiatan yang sesuai untuk mempertahankan rencana ketahanan dan mengembalikan kemampuan atau layanan yang terganggu karena insiden siber. Aktivias Pemulihan fokus pada pemulihan sistem dan layanan yang terganggu akibat insiden siber. Langkah Pemulihan mencakup perbaikan infrastruktur teknologi dan peningkatan proses untuk mencegah insiden serupa di masa depan.

Jenis Ancaman Siber

Mhara et al. (2024) menjelaskan jenis-jenis utama ancaman siber, yaitu:

1. *Hacking. Hacking* (peretasan) adalah akses tidak sah ke dalam sistem komputer, jaringan atau data. Peretasan dilakukan melalui beberapa teknik, diantaranya: *Social Engineering*, *Exploitation of Vulnerabilities*, *Credential Stuffing* dan *Distributed Denial of Service*. *Social Engineering* adalah teknik manipulasi psikologis yang digunakan oleh penyerang untuk mengecoh individu agar memberikan informasi rahasia, seperti kredensial login, data keuangan, atau akses ke sistem yang aman. Berbeda dengan serangan teknis yang bergantung pada eksploitasi kelemahan perangkat lunak atau sistem, *Social Engineering* mengeksploitasi kelemahan manusia, seperti kepercayaan, ketidaktahuan, atau rasa takut. *Exploitation of Vulnerabilities* (eksploitasi kerentanan) adalah proses di mana penyerang mengeksploitasi kelemahan atau celah keamanan perangkat lunak, sistem operasi, atau infrastruktur jaringan untuk mendapatkan akses yang tidak sah, mencuri data, atau menyebabkan gangguan pada sistem. *Credential Stuffing* adalah jenis serangan siber di mana penyerang menggunakan kombinasi *username* dan *password* yang telah bocor dari satu layanan untuk mencoba mendapatkan akses ke akun di layanan lain. Serangan ini terjadi karena banyak pengguna menggunakan kata sandi yang sama di berbagai platform, sehingga jika satu akun mereka bocor, semua akun yang menggunakan kredensial serupa menjadi rentan. *Distributed Denial of Service* (DDoS) adalah serangan siber yang bertujuan untuk melumpuhkan layanan atau sistem dengan membanjiri jaringan, server, atau aplikasi dengan lalu lintas dalam jumlah besar yang berasal dari berbagai sumber yang tersebar di seluruh dunia. Serangan ini bertujuan untuk membuat layanan menjadi tidak tersedia bagi pengguna yang sah, menyebabkan gangguan operasional, dan dalam beberapa kasus, menimbulkan kerugian finansial. Peretas dapat berupa individu atau kelompok terorganisir, dan mempunyai motivasi berkisar dari keuntungan finansial hingga aktivitas politik.
2. *Malware. Malware* adalah perangkat lunak berbahaya yang dirancang untuk merusak, menyusup, atau mencuri informasi dari sistem komputer atau jaringan. Jenis-jenis *Malware* meliputi *Virus, Ransomware, Spyware, Worm*, dan *Trojan*. *Virus* menempel pada file atau program yang sah dan menyebar saat dijalankan, *Ransomware* mengenkripsi data dan meminta pembayaran untuk kunci dekripsi, *Spyware* secara diam-diam mengumpulkan dan mengirimkan data pengguna tanpa izin, *Worm* menyebar ke seluruh jaringan tanpa memerlukan tindakan manusia, *Trojan* menyamar sebagai perangkat lunak yang sah tetapi menjalankan operasi berbahaya setelah diinstal.
3. *Targeted Attacks. Targeted Attacks* adalah operasi siber yang disengaja dan ditujukan terhadap orang, kelompok, atau sistem tertentu. Serangan ini direncanakan dan dilakukan dengan hati-hati dengan tujuan tertentu, seperti memperoleh data sensitif, mengganggu proses bisnis, atau mencuri kekayaan intelektual. Serangan ini sering menggunakan teknik canggih, seperti *spear-phishing* dan eksploitasi *zero-day*.
4. *Electronic Espionage. Electronic Espionage* adalah akuisisi data yang tidak sah, biasanya dilakukan oleh aktor yang disponsori negara atau kelompok kriminal terorganisir. Tujuannya adalah untuk mendapatkan keuntungan strategis, finansial, atau politik. Jenis

serangan ini ditandai dengan kecanggihan dan nilai tinggi dari informasi yang ditargetkan. IBM Cloud Team (2024) menyebutkan jenis-jenis ancaman siber yang umum terjadi, yaitu: *Malware*, Rekayasa Sosial dan *Phising*, *Man in The Middle, Denial of Service* (DoS), Eksploitasi *Zero Day*, Serangan Kata Sandi, Serangan *Internet of Things*, Serangan Injeksi.

Pengertian Strategi

Pengertian strategi secara umum diartikan sebagai upaya individu atau kelompok untuk membuat skema guna mencapai target sasaran yang hendak dituju. Dengan kata lain, strategi adalah seni bagi individu ataupun kelompok untuk memanfaatkan, kemampuan dan sumber daya yang dimiliki guna untuk mencapai target sasaran melalui tata cara yang dianggap efektif dan efisien untuk mencapai sasaran yang telah diharapkan (Novi V, n.d.). Gray (1999) mendefinisikan strategi sebagai seni dan ilmu yang mengintegrasikan *Ends* (tujuan), *Ways* (cara), dan *Means* (sarana) untuk mencapai hasil yang diinginkan. Kerangka ini menawarkan pendekatan holistik yang relevan dalam menganalisis dan merancang strategi keamanan siber, khususnya dalam konteks serangan siber pada kegiatan internasional seperti KTT G20 di Bali. Gray juga menjelaskan bahwa strategi bersifat multidimensional dan melibatkan berbagai faktor, termasuk dimensi politik, militer, ekonomi, sosial, dan teknologi. Kerangka kerja *Ends, Ways, and Means* menjadi dasar untuk menganalisis strategi pengamanan siber pada KTT G20. Tujuan (*Ends*) pengamanan siber KTT G20 adalah memastikan perlindungan maksimal terhadap penyelenggaraan KTT G20. Dalam konteks operasional yang lebih spesifik, *Ends* pengamanan siber KTT G20 dapat berupa: proteksi serangan siber terhadap infrastruktur penting, mengamankan data strategis VIP dan organisasi, serta menjamin keberlangsungan kegiatan KTT G20. Cara (*Ways*) merujuk pada metode, pendekatan, atau konsep strategis yang digunakan untuk memanfaatkan sumber daya (*means*) dalam mencapai tujuan akhir (*Ends*). *Ways* mencakup bagaimana strategi dirancang dan diimplementasikan melalui taktik, kebijakan, atau operasi yang terkoordinasi. Dalam konteks keamanan siber, *Ways* dapat berupa penerapan sistem deteksi dini, penguatan protokol enkripsi data, atau pelatihan tim keamanan untuk menghadapi dinamika ancaman siber. Kemudian *Means* adalah sumber daya yang tersedia dan digunakan untuk mendukung implementasi *Ways* demi mencapai tujuan akhir (*Ends*). Gray mengidentifikasi bahwa means meliputi elemen-elemen seperti personel, teknologi, infrastruktur, anggaran, dan kapasitas organisasi. Dalam keamanan siber, *Means* dapat berupa: perangkat lunak keamanan, infrastuktur teknologi informasi, dan tenaga ahli keamanan siber.

METODE PENELITIAN

Dalam menyusun tulisan ini, penulis menggunakan metode kualitatif dengan teknik pengumpulan data melalui wawancara, observasi dan studi dokumen. Pendekatan kualitatif dipilih karena memungkinkan eksplorasi yang mendalam terhadap fenomena ancaman dan strategi pengamanan siber pada KTT G20 di Bali tahun 2022. Wawancara mendalam dilakukan terhadap narasumber yang terlibat langsung pada pelaksanaan pengamanan siber KTT G20 tahun 2022. Para narasumber tersebut adalah:

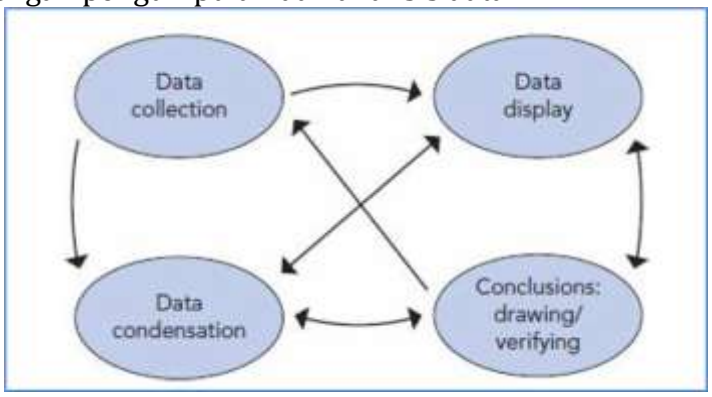
a. Deputi Bidang Operasi Keamanan Siber dan Sandi Badan Siber dan Sandi Negara (BSSN);
b. Kepala Pusat Data dan Teknologi Informasi Komunikasi BSSN;
c. Wakil Komandan Satuan Siber TNI;
d. Tim Siber Direktorat Tindak Pidana Siber Bareskrim Polri.

Data dalam tulisan ini dianalisis menggunakan model Miles and Huberman melalui aktivitas yang terdiri dari: *Data Condensation, Data Display, Drawing and Verifying Conclusions.* (Miles et al., 2014) *Data Condensation* adalah proses memilih, memfokuskan,

menyederhanakan, mengabstraksi, dan mentransformasi data mentah dari lapangan. Tujuannya untuk mengorganisasi data agar lebih mudah dianalisis. Kegiatan pada tahap ini adalah:

a. Seleksi, yaitu: memilih data yang relevan sesuai fokus penelitian.
b. *Coding* (Koding), yaitu: memberi label atau kode untuk mengelompokkan data berdasarkan tema tertentu.
c. Kategorisasi, yaitu: mengelompokkan data ke dalam kategori untuk menemukan pola atau hubungan.
d. Reduksi, yaitu: menyederhanakan data tanpa menghilangkan esensi pentingnya.

Data Display adalah proses mengorganisasi data yang telah dikondensasi ke dalam format yang terstruktur, sehingga memudahkan untuk memahami dan menarik kesimpulan. *Data Display* (penyajian data) dapat dalam bentuk matriks, bagan atau diagram, jaringan (network), atau narasi deskriptif. *Drawing and Verifying Conclusions* adalah proses interpretasi data untuk menemukan makna, pola, hubungan, atau teori. Penarikan kesimpulan dilakukan secara iteratif (berulang), seiring dengan pengumpulan dan analisis data.

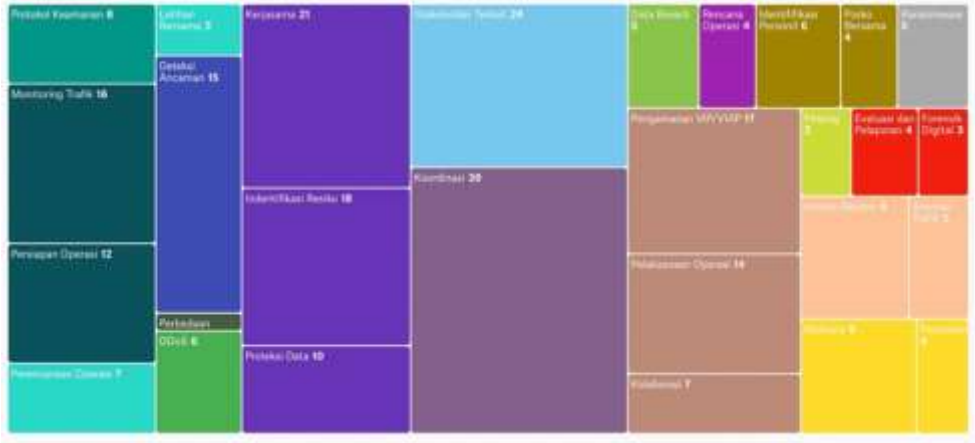


Gambar 3. Analisis Model Miles dan Huberman
Sumber: (Miles et al., 2014)

HASIL PENELITIAN DAN PEMBAHASAN

Hasil Kategorisasi

Berdasarkan hasil wawancara dengan para narasumber, penulis memberikan label/kode yang merepresentasikan esensi dari suatu segmen data dan kemudian mengkategorikannya dalam suatu kelompok/grup. Berikut adalah distribusi kode hasil wawancara dengan para narasumber:



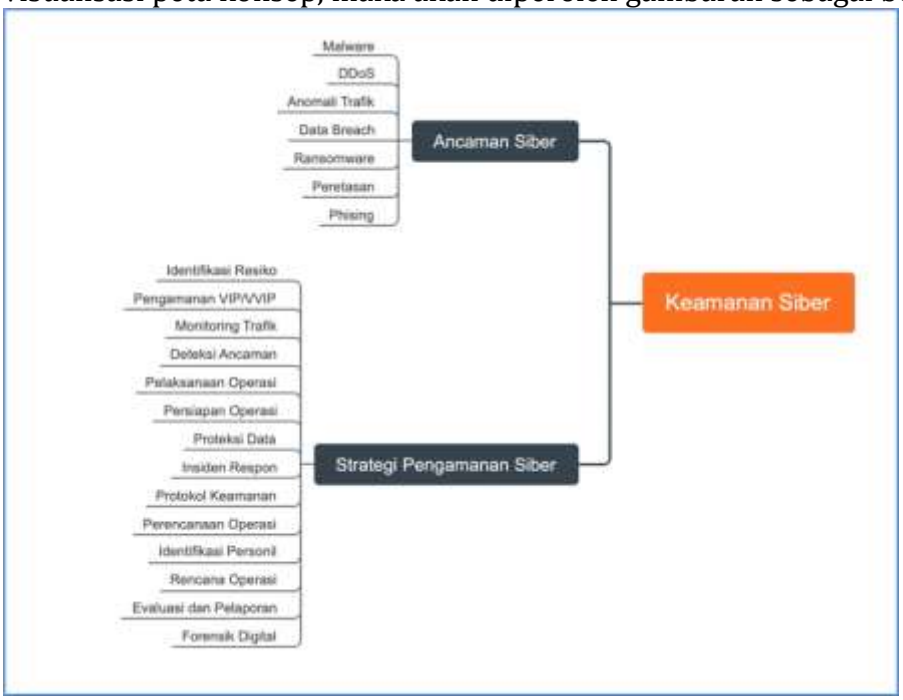
Gambar 4. Distribusi Kode
Sumber: Atlasti.com (2025)

Berdasarkan hasil distribusi kode tersebut, terdapat 7 (tujuh) kode yang terkait dengan kategori/tema Ancaman Siber dan 14 (empat belas) kode yang terkait dengan kategori/tema Strategi Pengamaman Siber. Kode-kode tersebut adalah:

Tabel 1. Kategorisasi Kode

No.	Kode	Kategori/Tema	Frekeunsi	Persentase
1.	Malware	Ancaman Siber	9	3,23%
2.	DDoS		6	2,15%
3.	Anomali Trafik		5	1,79%
4.	Data Breach		5	1,79%
5.	Ransomware		5	1,79%
6.	Peretasan		4	1,43%
7.	Phising		3	1,08%
			37	13,26%
1.	Identifikasi Resiko	Strategi Pengamanan Siber	18	6,45%
2.	Pengamanan VIP/VVIP		17	6,09%
3.	Monitoring Trafik		16	5,73%
4.	Deteksi Ancaman		15	5,38%
5.	Pelaksanaan Operasi		14	5,02%
6.	Persiapan Operasi		12	4,30%
7.	Proteksi Data		10	3,58%
8.	Insiden Respon		9	3,23%
9.	Protokol Keamanan		8	2,87%
10.	Perencanaan Operasi		7	2,51%
11.	Identifikasi Personel		6	2,15%
12.	Rencana Operasi (RO)		4	1,43%
13.	Evaluasi dan Pelaporan		4	1,43%
14.	Forensik Digital		3	1,08%
			143	51,25%

Kode-kode dalam kategori Ancaman Siber dan Strategi Pengamanan Siber jika disajikan dalam bentuk visualisasi peta konsep, maka akan diperoleh gambaran sebagai berikut:



Gambar 5. Visualisasi Peta Konsep
Sumber: Penulis (2025)

Dalam rangka menggali makna yang lebih dalam hasil dari proses kategorisasi tersebut, maka penulis memberikan penjelasan setiap kode atau frasa yang memuat esensi dari segmen data hasil wawancara dengan mempertimbangkan konteks tema pembahasan tulisan dan perspektif narasumber.

Ancaman Siber

1. Malware. *Malware* adalah perangkat lunak berbahaya yang dirancang untuk merusak, menyusup, atau mencuri informasi dari sistem komputer atau jaringan. Jenis-jenis *Malware* meliputi *virus, worm, trojan, ransomware,* dan *spyware*, masing-masing dengan tujuan dan metode serangan yang berbeda. Serangan *Malware* sering kali menggunakan teknik seperti *Social Engineering*, eksploitasi kerentanan perangkat lunak, atau penggunaan lampiran berbahaya dalam email.
2. DdoS. Serangan *Distributed Denial of Service* (DDoS) adalah upaya untuk melumpuhkan layanan atau jaringan dengan membanjiri sistem target dengan lalu lintas dalam jumlah besar dari berbagai sumber yang tersebar. Serangan tersebut bertujuan untuk membuat layanan tidak tersedia bagi pengguna sah, sehingga mengganggu operasional bisnis atau menyebabkan kerugian finansial. Serangan DDoS biasanya dilakukan menggunakan botnet, yaitu jaringan perangkat yang telah dikompromikan dan dikendalikan oleh penyerang.
3. Anomali Trafik. Anomali trafik dalam konteks pengamanan siber merujuk pada pola lalu lintas jaringan yang tidak biasa atau mencurigakan yang dapat menunjukkan adanya ancaman keamanan. Anomali ini bisa berupa lonjakan trafik yang tiba-tiba, perubahan pola akses, atau penggunaan bandwidth yang tidak normal. Deteksi anomali trafik merupakan langkah penting dalam strategi keamanan proaktif, di mana metode seperti *Intrusion Detection Systems* (IDS) digunakan untuk mendeteksi pola yang menyimpang dari *baseline* normal.
4. Data Breach. *Data Breach* (kebocoran data) adalah insiden keamanan di mana informasi sensitif, seperti data pribadi atau rahasia bisnis, diakses, dicuri, atau diungkapkan oleh pihak yang tidak berwenang. Insiden ini sering kali disebabkan oleh kelemahan dalam sistem keamanan, serangan siber yang terkoordinasi, atau kelalaian pengguna dalam menjaga keamanan informasi. Konsep CIA Triad (*Confidentiality, Integrity, Availability*) menjadi dasar dalam melindungi data dari kebocoran yang dapat berdampak serius bagi individu dan organisasi.
5. Ransomware. *Ransomware* adalah jenis malware yang mengenkripsi data korban dan menuntut pembayaran tebusan (ransom) untuk mengembalikan akses ke data tersebut. Biasanya, penyerang menginfeksi sistem dengan *Ransomware* melalui email *Phishing*, eksploitasi kerentanannya, atau melalui website berbahaya. Setelah terinfeksi, file-file penting yang ada dalam sistem korban akan dienkripsi dengan algoritma yang kuat, dan korban diancam dengan kehilangan data secara permanen jika tidak membayar tebusan. Salah satu contoh terkenal dari serangan ransomware adalah serangan *WannaCry* yang menginfeksi ratusan ribu komputer di seluruh dunia pada tahun 2017.
6. Peretasan. *Hacking* (peretasan) adalah aktivitas yang dilakukan untuk mendapatkan akses tidak sah ke sistem komputer, jaringan, atau data dengan tujuan tertentu, seperti pencurian informasi, sabotase, atau eksploitasi sumber daya. Peretasan dapat dilakukan oleh individu atau kelompok yang disebut sebagai *threat actors*, yang dapat berupa *hacker* etis, kriminal siber, atau bahkan aktor negara.
7. Phising. *Phishing* adalah metode serangan rekayasa sosial di mana penyerang menyamar sebagai entitas tepercaya untuk menipu korban agar memberikan informasi sensitif seperti kredensial login atau data finansial. Serangan ini biasanya dilakukan melalui email atau

pesan palsu yang mengandung tautan berbahaya. *Phising* juga sering kali memanfaatkan *Social Engineering*, di mana penyerang mengeksploitasi kepercayaan dan emosi korban.

Strategi Pengamanan Siber

1. Identifikasi Risiko. Identifikasi risiko adalah langkah awal dalam pengamanan siber yang bertujuan untuk mengidentifikasi ancaman potensial yang dapat mempengaruhi aset organisasi. Proses ini mencakup penilaian terhadap kerentanan sistem, kemungkinan ancaman, serta dampak yang dapat ditimbulkan jika risiko tersebut terjadi.
2. Pengamanan VIP/VVIP. Pengamanan VIP/VVIP dalam konteks siber merujuk pada langkah-langkah perlindungan khusus yang diberikan kepada individu dengan tingkat risiko tinggi, seperti pejabat pemerintah, eksekutif perusahaan, atau tokoh publik. Ancaman terhadap VIP/VVIP dapat berupa serangan siber yang menargetkan identitas digital, perangkat pribadi, atau komunikasi mereka.
3. Monitoring Trafik. Monitoring trafik adalah proses pengawasan lalu lintas data yang melewati jaringan organisasi untuk mendeteksi aktivitas mencurigakan atau tidak sah. Dengan menggunakan alat seperti *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS), organisasi dapat menganalisis pola lalu lintas jaringan untuk mengidentifikasi tanda-tanda serangan seperti DDoS atau aktivitas *Malware*.
4. Deteksi Ancaman. Deteksi ancaman adalah proses identifikasi potensi serangan siber yang dapat mengganggu operasional organisasi. Kemampuan mendeteksi ancaman dengan cepat sangat penting dalam mencegah serangan yang dapat menyebabkan kerugian besar.
5. Pelaksanaan Operasi. Pelaksanaan operasi dalam pengamanan siber adalah implementasi dari rencana dan strategi yang telah disusun untuk melindungi sistem informasi organisasi dari ancaman siber. Proses ini mencakup penerapan kontrol keamanan, pemantauan berkelanjutan, serta respons terhadap insiden yang terjadi.
6. Persiapan Operasi. Persiapan operasi adalah tahap sebelum pelaksanaan operasional keamanan siber yang bertujuan untuk memastikan kesiapan sumber daya, infrastruktur, dan prosedur yang akan digunakan. Persiapan ini mencakup pengujian sistem keamanan, pelatihan tim, serta penyusunan prosedur operasi standar (SOP) untuk menangani berbagai skenario ancaman.
7. Proteksi Data. Proteksi data adalah upaya untuk menjaga kerahasiaan, integritas, dan ketersediaan data dari akses yang tidak sah atau manipulasi yang berbahaya. Strategi proteksi data mencakup implementasi enkripsi, kontrol akses berbasis peran, serta pencadangan data yang dilakukan secara rutin untuk mencegah kehilangan akibat insiden siber.
8. Insiden Respon. Insiden Respon adalah rangkaian tindakan yang diambil untuk menangani dan memitigasi dampak dari insiden keamanan siber yang terjadi pada organisasi. Kerangka kerja NIST memberikan panduan mengenai tahap-tahap dalam respons insiden, mulai dari deteksi, analisis, penanggulangan, hingga pemulihan.
9. Protokol Keamanan. Protokol keamanan adalah serangkaian aturan dan prosedur yang dirancang untuk melindungi sistem informasi dari ancaman siber. Protokol ini mencakup enkripsi data, autentikasi pengguna, dan prosedur respons insiden yang terstruktur. Protokol Keamanan memastikan bahwa proses komunikasi data dilakukan dengan cara yang aman, menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi.
10. Perencanaan Operasi. Perencanaan operasi keamanan siber adalah proses penyusunan strategi dan taktik yang bertujuan untuk melindungi aset informasi organisasi. Perencanaan ini mencakup identifikasi ancaman, alokasi sumber daya, serta penentuan metode respon

yang akan diterapkan jika terjadi insiden keamanan. Prinsip perencanaan ini mengikuti standar seperti NIST yang menetapkan kontrol keamanan yang harus diterapkan dalam lingkungan teknologi informasi.

11. Identifikasi Personil. Identifikasi personil dalam konteks keamanan siber adalah proses menentukan siapa saja individu yang memiliki akses ke sistem dan data sensitif organisasi. Prinsip *Least Privilege Access* menekankan bahwa setiap individu hanya boleh memiliki akses yang diperlukan untuk menjalankan tugasnya guna meminimalkan risiko pelanggaran keamanan.
12. Evaluasi dan Pelaporan. Evaluasi dan pelaporan dalam keamanan siber merupakan langkah penting untuk menilai efektivitas strategi keamanan yang diterapkan serta mengidentifikasi area yang perlu ditingkatkan. Laporan yang dihasilkan dari evaluasi ini dapat digunakan sebagai dasar untuk perbaikan strategi keamanan, penyusunan anggaran, dan pelaporan kepada pimpinan serta dapat digunakan sebagai pembelajaran untuk kegiatan yang serupa.
13. Rencana Operasi. Rencana Operasi adalah dokumen yang merinci langkah-langkah yang harus diambil untuk memastikan keamanan informasi dan kelangsungan operasional organisasi. Rencana ini mencakup strategi pencegahan, prosedur respon insiden, serta mekanisme pemulihan yang harus diikuti dalam situasi darurat.
14. Forensik Digital. Forensik Digital adalah proses pengumpulan, analisis, dan interpretasi bukti elektronik untuk menyelidiki insiden keamanan siber. Proses ini penting dalam mengidentifikasi penyebab serangan, metode yang digunakan oleh penyerang, serta dampak yang ditimbulkan terhadap sistem organisasi. Prinsip dasar dalam forensik digital mengacu pada framework seperti *Digital Forensics and Incident Response* (DFIR) yang dirilis oleh NIST.

Pembahasan

Berdasarkan hasil analisis data sesuai dengan Tabel 1 tentang Kategorisasi Kode dan Gambar tentang Visualisasi Peta Konsep, dapat diketahui bahwa pada tema/kategori Ancaman Siber terdapat 7 (tujuh) kode, yaitu : Anomali Trafik, *Data Breach*, *DDoS, Malware,* Peretasan, *Phising, Ransomware.* Dari ke-7 kode tersebut, yang termasuk jenis ancaman siber adalah: *Malware, DDoS, Ransomware, Phising* dan Peretasan. Sehingga dapat disimpulkan bahwa jenis serangan siber yang terjadi pada KTT G20 tahun 2022 adalah: *Malware, DDoS, Ransomware, Phising* dan Peretasan. Dari jenis-jenis ancaman tersebut, *Malware* adalah jenis serangan yang paling dominan pada KTT G20 tahun 2022. Jumlah kode tertinggi dari kategori Strategi Pengamanan Siber adalah Identifikasi Risiko. Namun jika dilihat secara keseluruhan, sebaran jumlah masing-masing kode pada kategori Strategi Pengamanan Siber cenderung merata. Oleh karena itu, penulis memutuskan untuk memilih kode dengan jumlah frekuensi ≥ 10 sebagai elemen penting dalam kategori Strategi Pengamanan Siber. Kode-kode tersebut adalah: Identifikasi Risiko, Pengamanan VIP/VVIP, Monitoring Trafik, Deteksi Ancaman, Pelaksanaan Operasi, Persiapan Operasi, dan Proteksi Data. Jika dikaitkan dengan kerangka kerja NIST, maka kode-kode pada kategori Strategi ditabulasikan sebagai berikut:

NIST	Kode	Frek	%
IDENTIFY	Identifikasi Resiko	18	40,17%
	Persiapan Operasi	12	
	Perencanaan Operasi	7	
	Identifikasi Personil	6	
	Rencana Operasi	4	
		47	
PROTECT	Pengamanan VIP/VVIP	17	23,08%

	Proteksi Data	10	
		27	
DETECT	Monitoring Trafik	16	26,50%
	Deteksi Ancaman	15	
		31	
RESPOND	Insiden Respon	9	7,69%
RECOVER	Forensik Digital	3	2,56%
		117	

Berdasarkan pola hubungan antara kode-kode pada kategori Ancaman Siber dan kategori Strategi Pengamanan Siber, diperoleh relasi sebagai berikut:

	Anomali Trafik	Data Breach	DDoS	Malware	Peretasan	Phising	Ransomware
Deteksi Ancaman	0	0	1	2	2	1	1
Evaluasi dan Pelaporan	0	0	0	0	0	0	0
Forensik Digital	0	0	0	0	0	0	0
Identifikasi Personil	0	0	0	0	0	0	0
Indentifikasi Resiko	0	0	1	1	0	0	0
Insiden Respon	0	0	0	0	0	0	0
Monitoring Trafik	4	0	3	2	0	0	0
Pelaksanaan Operasi	0	1	0	0	1	0	0
Pengamanan VIP/VVIP	0	0	0	1	0	0	1
Perencanaan Operasi	0	0	0	0	0	0	0
Persiapan Operasi	0	1	0	0	1	0	0
Proteksi Data	0	2	0	0	0	0	0
Protokol Keamanan	0	0	0	0	0	0	0
Rencana Operasi	0	0	0	0	0	0	0

Gambar 6. Relasi Ancaman Siber dan Strategi Pengamanan Siber
Sumber: Atlasti.com (2025)

Berdasarkan relasi antara kategori Ancaman dengan Strategi Pengamanan Siber dapat diketahui bahwa terdapat beberapa kode pada kategori Ancaman yang mempengaruhi kode-kode pada Strategi Pengamanan Siber dan begitu pula sebaliknya, beberapa kode pada Strategi Pengamanan Siber mempengaruhi kode-kode pada Ancamanan Siber. Dalam relasi tersebut, kategori Ancaman yang paling menonjol adalah *Malware* dengan frekuensi sebanyak 6 (enam), sementara kategori Strategi Pengamanan Siber yang paling menonjol adalah Monitoring Trafik dengan frekuensi sebanyak 9 (sembilan).

KESIMPULAN

Berdasarkan pembahasan dari bagian sebelumnya, terkait dengan dinamika ancaman siber dan hubungannya dengan strategi keamanan siber, dapat disimpulkan hal-hal sebagai berikut: *Pertama*, pelaksanaan pengamanan siber kegiatan KTT G20 tahun 2022 berjalan dengan aman, karena ancaman siber yang terjadi yaitu: Anomali Trafik, *Data Breach*, *DDoS, Malware,* Peretasan, *Phising, Ransomware* tidak menyebabkan peristiwa terjadinya insiden siber. Ancaman siber yang dominan adalah *Malware*, sementara langkah-langkah mitigasi ancaman siber pada KTT G20 tahun 2022 didominasi oleh aktivitas Monitoring Trafik. *Kedua*, elemen penting dalam strategi pengamanan siber VIP/VVIP KTT G20 adalah: Identifikasi

Risiko, Pengamanan VIP/VVIP, Monitoring Trafik, Deteksi Ancaman, Pelaksanaan Operasi, Persiapan Operasi, dan Proteksi Data. Jika dikaitkan dengan kerangka kerja NIST, strategi pengamanan siber KTT G20 lebih dominan pada aktivitas Identifikasi (40,7%), Deteksi (26,50%) dan Proteksi (23,08%). Dengan demikian, strategi pengamanan siber KTT G20 tahun 2022 lebih didominasi aktivitas pencegahan terjadinya insiden siber. *Ketiga*, ancaman siber dan strategi pengamanan siber pada pelaksanaan kegiatan KTT G20 tahun 2022 mempunyai pola hubungan yang saling mempengaruhi. Dengan kata lain, hubungan antara ancaman siber dan strategi pengamanan siber dapat digambarkan sebagai hubungan sebab-akibat yang dinamis. Ketika ancaman siber semakin kompleks, maka strategi pengamanan siber pun harus berkembang menjadi lebih canggih dan proaktif.

DAFTAR PUSTAKA

AwanPintarid. (2024). AwanPintar.id | Indonesia Waspada - Laporan Ancaman Digital di Indonesia Semester 1 Tahun 2024.

Check Point Research. (2024, June 16). Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks. https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

Crelier, A. (2019). Trend Analysis Cybersecurity at Big Events. www.css.ethz.ch

Harrell, M. N. (2017). Synergistic Security: A Work System Case Study of the Target Breach. Journal of Cybersecurity Education, Research and Practice, 2. https://digitalcommons.kennesaw.edu/jcerpAvailableat:https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss2/4Practice:https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss2/4

IBM Cloud Team. (2024, March 25). Jenis-jenis ancaman siber. https://www.ibm.com/id-id/think/topics/cyberthreats-types

ISACA. (2015). Cybersecurity Fundamentals. www.isaca.org/cyber

IT Governance. (2024, May 2). Global Data Breaches and Cyber Attacks in 2024. https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024

Marchewka, J. T. (2015). Information Technology Project Management (5th ed.). Wiley.

Mhara, M. A. O. A., Abdulrahman, A. A. A., & Baroud, A. A. S. (2024). Cyber Attacks And Threats: Study Of The Types Of Cyber Attacks: Hacking, Viruses, Targeted Attacks, And Electronic Espionage. Int. J. Electr. Eng. and Sustain., 38–47.

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). Qualitative Data Analysis: A Methods Sourcebook (3rd ed.). Sage.

Nasser, K., & Al-Dosari, K. A. (2020). Identification and Prevention of Expected Cybersecurity Threats During 2022 Fifa World Cup In Qatar. Journal of Poverty, Investment and Development, 5(1), 49–84. www.iprjb.org

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018

Novi V. (n.d.). Pengertian Strategi serta Jenis, Tujuan, Dan Contohnya. Retrieved August 12, 2024, from https://www.gramedia.com/literasi/pengertian-strategi/

Patrascu, P. (2019). Missions and Actions Specific to Cyberspace Operations. International Conference Knowledge-Based Organization, 25(3), 51–56. https://doi.org/10.2478/kbo-2019-0117

We Are Social. (2023). Digital 2023 Global Overview Report.

We Are Social. (2024). Digital 2024 Global Overview Report.