Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 3, Issue June, 2025 pp. 2233-2239 http://urj.uin-malang.ac.id/index.php/mij/index

Geopolitik *cyber security*: Strategi menghadapi ancaman siber terhadap keamanan informasi pada era digital

Soraya Bilqis
Program Studi Manajemen, Universitas Islam Negeri Maulana Malik Ibrahim Malang
e-mail: rayaabilqis@gmail.com

Kata Kunci:
Geopolitik; ketahanan nasional; cyber security; strategi keamanan siber; ancaman siber

Keywords:
geopolitics; national resilience; cyber security; cyber security strategy; cyber threats

A B S T R A K

Munculnya serangan-serangan yang membahayakan untuk keamanan informasi dan berakibat pada ketahanan nasional. Penelitian ini mengkaji geopolitik cyber security ancaman-ancaman yang dihadapi negara dalam konteks geopolitik dan strategi menghadapi serangan dalam keamanan siber. Menggunakan metode kualitatif deskriptif dimana ini mengumpulkan data-data yang akurat dari dokumen resmi pemerintah dalam menganalisis geopolitik cyber security. Hasil penelitian indonesia menjadi sasaran terbanyak dalam serangan siber. Pada tahun 2024 lebih dari 330 juta serangan siber terjadi di indonesia. Lemahnya sistem keamanan negara memberikan celah untuk melakukan serangan-serangan pada keamnan informasi negara. Peneliti megharapkan pemerintah dapat melakuakan strategi Penguatan sistem pada Badan Siber dan Sandi Negara (BSSN), menjalin kerja sama luar negeri, peningkatan sumber daya manusia menjadi hal penting dalam menjalankan strategi mengahadapi serangan siber. Penting meningkatkan pertahanan sistem keamanan dalam menghadapi serangan-serangan siber.

A B S T R A C T

The emergence of attacks that are dangerous to information security and have an impact on national resilience. This study examines the geopolitics of cyber security, the threats faced by the country in the context of geopolitics and strategies for dealing with attacks in cyber security. Using a descriptive qualitative method where it collects accurate data from official government documents in analyzing the geopolitics of cyber security. The results of the study Indonesia became the most targeted in cyber attacks. In 2024 more than 330 million cyber attacks occurred in Indonesia. The weakness of the state security system provides a gap for carrying out attacks on the security of state information. Researchers hope that the government can carry out a system strengthening strategy at the National Cyber and Crypto Agency (BSSN), establish foreign cooperation, and increase human resources to be important in implementing a strategy to deal with cyber attacks. It is important to increase the defense of the security system in dealing with cyber attacks.

Pendahuluan

Teknologi informasi semakin berkembang dari masa kemasa dan memiliki pengaruh dalam berbagai aspek kehidupan, termasuk pemerintahan, ekonomi, militer, pertahanan, dan keamanan. Ketergantungan pada teknologi memunculkan ancaman dalam keamanan informas, terutama data strategis negara. Indonesia, sebagai negara yang kaya akan sumber daya alamnya menjadi sasaran dalam serangan cyber security, serangan ini berdampak pada kerugian ekonomi dan reputasi internasional. Serangan

siber dengan perkembangan zaman semakin kompleks dan tersusun dengan baik. Serangan siber menjadi alat strategis dalam perebutan dan pengaruh kekuasaan untuk memperoleh keunggulan global. Kesiapan Indonesia dalam mengahadapi serangan siber masih sangat terbatas.

Serangan siber terjadi karena akses terhadap data yang bersifat rahasia maupum data-data pribadi dibocorkan dan diperjual belikan sehingga disalah gunakan oleh oknum-oknum tak bertanggung jawab. Ketika data pemerintah yang bersifat rahasia ataupun data seseorang disebarluaskan akan berakibat fatal yang merugikan pihak lain bahkan merugikan negara. Di tengah era revolusi seperti saat ini maka banyak negara melakukan upaya yang bernama diplomasi digital yang muncul sebagai alat strategis untuk menghadapi adanya dinamika ini dengan memanfaatkan kerjasama secara internasional serta inovasi teknologi dalam melindungi sistem informasi dan data-data yang bersifat sensitif.

Total trafik anomali di Indonesia selama tahun 2024 adalah 330.527.636 anomali dengan jenis trafik anomali tertinggi yaitu Mirai Botnet dengan total sebanyak 81.286.596 aktivitas. Mirai Botnet merupakan salah satu jenis Botnet yang menargetkan perangkat Internet of Things (IoT) dan dibuat untuk melakukan serangan Distributed Denial of Service (DDoS) pada situs web atau layanan online, sehingga mengakibatkan adanya gangguan atau downtime. Pada tahun 2024 Terdapat 2.487.041 aktivitas Advanced Persistent Threat (APT), 514.508 aktivitas Ransomware dan 26.771.610 aktivitas phishing. BSSN telah mengirimkan 1.367 notifikasi indikasi insiden ke stakeholder dengan jenis notifikasi terbanyak dikirimkan adalah Data Breach (BBSN, 2024).

Dalam Forum Grup Discussion sebagai bentuk Upaya Perlindungan serangan Siber menghadapi Geopolitik Indonesia 2045 yang diselenggarakan oleh Lembaga Pertahanan Nasional RI (LEMHANAS RI), Prof. Dr. Ir. Reni Mayerni, M.P., Deputi Bidang Pengkajian Strategik Lemhannas RI menyatakan bahwa keamanan siber kini menjadi isu yang semakin mendesak dalam konteks geopolitik global. Beliau menekankan bahwa menjaga keamanan siber tidak hanya mengandalkan teknologi semata, melainkan juga menjadi aspek kunci dalam menghadapi tantangan di era digital seperti yang sedang kita alami pada masa kini. Dalam pandangannya, perlindungan siber memiliki keterkaitan yang erat dengan pelaksanaan fungsi ketahanan dan keamanan nasional. Disisi lain, Laksda TNI Maman Firmansyah, Wakil Gubernur Lemhannas RI, sebagai pembuka dalam kegiatan Forum Group Discussion (FGD) tersebut, menyampaikan bahwa dalam konteks geopolitik V di Indonesia, transformasi digital menjadi sektor yang sangat signifikan dalam membentuk dinamika pembangunan nasional. Ia menekankan bahwa sektor ini dapat menjadi dasar untuk meningkatkan kapasitas geopolitik Indonesia di tengah arus globalisasi (Alfi et al., 2023).

Dinamika geopolitik internasional menyulitkan tantangan cyber security. Mengingat posisi Indonesia yang strategis dan menjadi negara dengan kekayaan sumber daya alam yang meilimpah menjadikan Indonesia rentan menghadapi konflik siber antar negara besar. Lemahnya sistem keamanan digital di Indonesia membuka celah untuk menyerang keamanan cyber negara. Dengan berbagai ancaman yang

dihadapi, Indonesia membutuhkan pendekatan strategis yang matang dan menyeluruh dalam menghadapi serangan cyber security.

Kajian ini bertujuan mengeksplorasi dimensi geopolitik keamanan siber dengan fokus pada strategi menghadapi ancaman terhadap keamanan informasi di era digital, khususnya dalam konteks Indonesia. Analisis akan mencakup pemetaan aktor-aktor kunci, pola ancaman terkini, serta pendekatan strategis yang dapat diadopsi untuk memperkuat ketahanan siber nasional dalam konteks persaingan geopolitik global.

Metode Penelitian

Penelitian ini menggunakan metode penelitian kualitatif deskriptif yang berfokus pada analisis literatur, karakteristik, metafora, deskripsi suatu hal. Pendekatan kualitatif untuk mendapatkan pemahaman mengenai strategi dalam menghadapi ancaman siber terhadap keamanan informasi, sedangkan pendekatan deskriptif digunakan untuk memberikan gambaran yang detail mengenai hal yang di teliti. Pengumpulan data dipilih yang paling relevan dengan tujuan penelitian. Data yang sesuai dengan tujuan penelitian ditelaah dengan secara mendalam, yang berfokus pada strategi dalam menghadapi ancaman siber, keamanan informasi diera digital.

Teknik yang gunakan dalam pengumpulan data penelitian ini adalah triangulasi, dimana menggunakan kombinasi teknik pengumpulan data. Studi pustaka digunakan karena banyaknya informasi dan data mengenai strategi ancaman siber. Pengumpulan data juga berasal dari berbagai jurnal, buku, serta informasi situs/web melalui internet. Dokumen penelitian digunakan untuk menganalisis sumber informs yang tersedia dari dokumen-dokumen resmi seperti dokumen resmi yang dikeluarkan langsung oleh pemerintah.

Pembahasan

Geopolitik Cybersecurity

Geopolitik dapat didefinisikan sebagai kajian tentang faktor-faktor geografis, sejarah, dan ilmu sosial yang dapat mempengaruhi keamanan diruang lingkup siber. Geopolitik menurut bahasa berasal dari kata “geo” yang artinya bumi, dan “politea” berasal dari bahasa Yunani yang artinya urusan. Dalam kamus besar bahasa Indonesia geopolitik adalah kebijakan negara atau bangsa yang disesuaikan dengan posisi geografisnya (Romi Faslah, 2024). Menurut Colin Flint tentang geopolitik yaitu “geopolitics as a study that connects a region's characteristics with its political dynamics” yang dapat diartikan bahwa geopolitik adalah studi yang menghubungkan karakteristik dengan dinamika politiknya. Disimpulkan dari definisi-definisi diatas geopolitik adalah penyelenggaraan suatu negara dengan pemanfaatan wilayah, geografis, dan menggunakan kosep teritorial yang mengunakan kekuatan politik negara tersebut. Perkembangan teknologi mempengaruhi lanskap geopolitik dan membuka persaingan antar negara yang menyerang keamanan informasi. Hal ini terjadi karena interaksi masyarakat yang berbagi informasi yang tidak terkontrol dan tidak terkendali oleh negara berakibat fatal, selain itu informasi-informasi negara jika tidak dijaga dengan baik akan merugikan negara di ranah Internasional (Kristalia & Wibisono, 2024).

Secara khusus, geopolitik adalah metode analisis kebijakan luar negeri yang berusaha memahami, memprediksi, dan menjelaskan perilaku politik internasional dengan mempertimbangkan variable geografis, yang mencakup lokasi geografis suatu negara, ukuran negara, iklim daerahnya, sumber daya alam yang dimiliki, perkembangan teknologi, topografis, dan demografis . Seiring dengan perkembangan zaman kekuatan suatu negara bukan lagi diukur dari ukuran negaranya atau sumber daya alamnya, kekuatan suatu negara juga diukur dengan ketahanan dalam melindungi dan mempertahankan informasi penting negara. Meskipun geopolitik mengalami perubahan menjadi konsep ruang siber tanpa adanya batas teriorial yang jelas (Kristalia & Wibisono, 2024).Serangan siber yang dapat menyerang dalam berbagi bentuk seperti pencurian data penting negara yang mengakibatkan krisis ekonomi. Serangan siber ini dapat dilakukan secara individu ataupun kelompok, seperti kelompok teroris maupun kelompok kriminal. Negara berperan penting pada konsep geopolitik yang memiliki kepentingan untuk melindungi dan mempertahankan informasi penting negara dari ancaman dan serangan-serangan luar.

Ancaman *Cyber Security* pada Era Digital

Indonesia menjadi salah satu target yang banyak dituju dalam serangan siber, menurut Kominfo data yang dicuri mencapai jutaan setiap tahunya. Berdasarkan data dari BSSN (Badan Siber dan Sandi Negara) menujukan laporan serangan siber atau trafik anomali pada tahun 2024 sebanyak 330.572.636 anomali. Anomali trafik tertinggi terjadi pada bulan Desember yaitu mencapai 112.085.045 anomali, dan trafik terendahnya pada bulan Mei yaitu 12.273.078 anomali (BSSN,2024). Jumlah ini lebih rendah jika dibandingkan tahun 2023 yang mencapai 403.990.813 anomali. Hal ini dapat berdampak pada penurunan performa perangkat dan jaringan, pencurian data sensitive, hingga perusakan reputasi, dan penurunan kepercayaan terhadap sutau organisasi (BSSN,2024).

Pada pemilu 2024, dari 514 kota/kabupaten di Indonesia 116 diantaranya mengalami serangan siber. Berdasarkan pernyataan Puadi (Komisioner Bawaslu RI), pihaknya menerima 7.650 laporan serangan siber terhadap sistem informasi milik Bawaslu di daerah. Berdasarkan laporan serangan siber yang diterima, di antaranya upaya pencurian data rahasia milik Bawaslu, data penyelesaian sengketa proses pemilu, data pelanggaran administrasi, hingga usaha pencurian data pemilih (Alfi et al., 2023). Pencurian ini menimbulkan rasa ketidak percayaan masyarakat dan mempengaruhi pikiran adanya kecurangan dari pemilu tersebut. Pencurian data-data pribadi yang berakhir disalah gunakan atau dijual yang merugikan diri kita sendiri. Pakar keamanan siber dari Cissrec, Pratama Persadha, mengatakan bahwa serangan siber dan ancaman peretasan ini terjadi berkali-kali dalam satu bulan, hal ini yang menyebabkan keamanan siber di Indonesia dalam tahap Red Alert atau tahap berbahaya (Vimy et al., 2022).

Perkembangan digital yang terus meningkat ancaman siber lagi hal yang dapat dianggap sepele, hal ini berkaitan dengan pertahanan dan keamanan Indonesia. Ancaman siber dapat juga berupa orang yang mempunyai kepentingan politik tertentu seperti halnya pada pencurian data pemilu 2024. Pada tahun 2018 terjadi kasus pencurian data melalui mesin ATM yang menyebabkan nasabah kehilangan uang

direkeningnya dan data pribadinya digunakan transaksi illegal di luar negeri (Afwadzi & Djalaluddin, 2024). Berdasarkan data dari Badan Siber dan Sandi Negara bahwasanya sector keuangan Indonesia mengalami serangan siber paling banyak dari sector lain yaitu mencapai 361 juta ditahun 2023 (OJK, n.d.).

Pemerintah sebagai pemangku kepentingan penting utntuk menyadari ancaman siber yang merusak pertahanan dan keamanan informasi penting negara atau individu, sehingga dapat dibentuk sistem keamanan yang lebih baik dan kompeten melalui BSSN. Minimnya pengetahuan masyarakat tentang ancaman siber semakin mengancan keamanan informasi di Indonesia. Pemberian wawasan melalui seminar atau pameran dapat menambah pengetahuan tentang ancaman siber. Walaupun serangan siber banyak menyerang pemerintah pemberian wawasan pada masyarakat penting bagi mereka agar lebih berhati-hati dlam menggunakan data pribadinya.

Strategi Menghadapi Ancaman Siber Dalam Konteks Geopolitik

Indonesia menduduki tingkatan kedua dalam konteks kejahatan siber, bebagai ancaman siber semakin mengkhawatirkan sehingga pemerintah dituntut untuk menguatkan keamanan informasi dari serangan siber melalui Badan Siber dan Sandi Negara (BSSN) serta berpartisipasi aktif dalam kemanan siber regional maupun internasional (Chamidy, n.d.). Perkembangan keamanan siber di Indonesia sudah berkembang sejak tahun 1990-an. Namun, Indonesia terlambat dalam proses penegakan hokum tentang keamanan siber dibandingkan dengan Negara tetangga yaitu Malaysia dan singapura (Yustika Citra & Ni Komang Desy, 2023). Ancaman siber terus meningkat dan dengan perkembangan teknologi serangan yang di hadapi juga semakin berbahaya. Penangulangan ancaman siber membutuhkan cara yang komprehensif dan kebijakan yang matang.

Pengembangan aspek hukum dan regulasi penting dalam menghadapi ancaman siber. Penambahan undang-undang khusus tentang keamanan siber yang dapat memberikan sanksi tegas kepada pelanggar yang melakukan kejahatan siber. Di Indonesia sudah ada beberapa regulasi seperti UU ITE, tetapi hal tersebut masih kurang karena tidak adanya undang-undang khusus tentang keamanan siber yang dapat mengatur kejahatan siber secara speksifik. Hingga saat ini Indonesia masih menggunakan regulasi seperti undang-undang ITE dalam merespon permasalahan siber yang masih sangat kurang untuk menangani permasalahan kejahatan siber. Penyunan perundang-undangan harus dilakukan secara berkelanjutan agar mampu mengikuti perkembangan ancaman siber (Yustika Citra & Ni Komang Desy, 2023)

Badan siber dan sandi Negara (BSSN) sebagai oraganisasi Negara yang bertanggung jawab dalam keamanan siber di Indonesia diharapkan dapat memberikan solusi dalam anacaman-ancaman siber. Badan Siber dan Sandi Negara dibentuk berdasarkan Peraturan Presiden No.53/2017, merupakan lembaga pemerintah non-kementerian yang langsung berada di bawah presiden (Yustika Citra & Ni Komang Desy, 2023). BSSN menerbitkan strategi yang komprehensif dalam memperkuat keamanan dan ketahanan siber nasional, BSSN menekankan pentingnya pembangunan ketahanan siber berlapis yang mampu melindungi infrastruktur informasi vital, serta memperkuat kemampuan deteksi, respons, dan pemulihan terhadap insiden siber. Strategi ini juga

mencakup kolaborasi lintas sektor, baik nasional maupun internasional, untuk pertukaran informasi intelijen dan penguatan koordinasi antar pemangku kepentingan, termasuk pemerintah, sektor swasta, akademisi, dan masyarakat (Sudarmadi & Runturambi, 2019). Dalam penyelenggaraan strategi dibutuhkan sumber daya yang unggul, dengan pelatihan, pendidikan yang tinggi, dan literasi siber akan menghasilkan sumber daya yang unggul.

Ancaman siber yang bersifat luas tidak hanya kawasan Indonesia tetapi juga internasional menjadikan hal ini sebagai alat dalam persaingan geopolitik. Indonesia memerlukan kolaborasi dengan Negara-negara tetangga, sehingga Indonesia perlu aktif dan berpartisipasi dalam kerja sama regional maupun internasional yang dapat memperkuat keamanan siber. Indonesia berkolaborasi melalui ASEAN dan lembaga internasional. Kerja sama Indonesia dengan lembaga internasional berupaya untuk meningkatkan keamanan siber (Kristiani Virgi Kusuma Putri, 2021).

Mengembangkan infrastruktur digital dalam negeri dan mengurangi ketergantungan layanan digital internasional, hal ini dilakukan agar Negara memiliki kendali penuh terhadap terhadap data-data negara. Membanfun system keamanan yang responsive atau cepat tanggap, penguatan sistem elektronik, menerapkan sistem keamanan yang yang ketat hal-hal tersebut dapat menjadi cara dalam melindungi data-data negara (Hoshmand & Ratnawati, 2023). Negara patut mendorong tentang riset dan penelitian teknologi informasi untuk menjaga keamanan informsi tetap terjaga. Berfokus pada pengembangan sistem keamanan untuk memperkuat geopolitik keamanan Indonesia dari serangan siber.

Kesimpulan dan Saran

Pada penelitian ini, diketahui ancaman serangan siber di Indonesia meningkat dengan berbagai macam model serangan. Dengan dilakukan identifikasi pada berbagai serangan. Hasil penelitian menunjukan berbagai strategi digunakan untuk menyelesaikan persoalan serangan siber. strategi ini dilakukan untuk meminimalisir berbagai bentuk serangan dan cara menghadapi serangan di masa depan. Indonesia ada diurutan kedua dalam konteks kejahatan siber. Badan Siber dan Sandi Negara menekankan pentingnya sistem keamanan berlapis untuk melindungi keamanan informasi. Berpartisipasi dalam kerja sama regional maupun internasional dapat mengurangi kasus kejahatan siber di Indonesia. Mengurangi ketergantungan pada sistem digital internasional melindungi dari serangan siber dan negara dapat mengakses data rahasia dengan lebih leluasa.

Melalui temuan yang diperoleh pada studi ini, diperlukan cara yang koherensif dan bijak dalam menyusun strategi keamanan informasi. Pengesahan undang-undang yang khusus membahas tentang kejahatan siber penting utntuk diperhatikan pemerintah. BSSN sebagai pemangku kepentingan terhadap serangan siber mengupayakan keamanan berlapis untuk data-data atau informasi penting. Menjalin kerjasama pada taraf regional maupum internasional dapat mengurangi serangan siber di Indonesia. Hal ini perlu didorang dengan sumber daya manusia yang unggul. Pemerintah perlu memperhatikan kualitas tenaga ahli dlam bidang keamanan siber.

Daftar Pustaka

Afwadzi, B., & Djalaluddin, A. (2024). PENGEMBANGAN EKONOMI BERBASIS SYARIAH DI ERA DIGITAL: ANTARA PELUANG, TANTANGAN, DAN KENDALA. *Journal of Sharia Economics*, *5*(1), 70–86. http://repository.uin-malang.ac.id/19072/

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). *Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia*. 6(2).https://scholarhub.ui.ac.id/jkskn/vol6/iss2/5/

BBSN. (2024). *LANSKAP KEAMANAN SIBER INDONESIA 2024*.

Chamidy, D. T. (n.d.). *Teknologi Informasi: Masa Depan atau Masa Lalu?*http://repository.uin-malang.ac.id/16343/

Hoshmand, M. O., & Ratnawati, S. (2023). *Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity*. 5(2).http://ejournal.sisfokomtek.org/index.php/saintek/article/view/2347

Kristalia, B. Y. Y., & Wibisono, I. W. (2024). ANCAMAN SIBER DAN PENGUATAN KEDAULATAN DIGITAL INDONESIA DARI PERSPEKTIF GEOPOLITIK DIGITAL. *Jurnal Ilmiah Multidisiplin*, *3*(02), 83–93. https://doi.org/10.56127/jukim.v3i02.1584

Kristiani Virgi Kusuma Putri. (2021). *KERJA SAMA INDONESIA DENGAN ASEAN MENGENAI CYBER SECURITY DAN CYBER RESILIENCE DALAM MENGATASI CYBER CRIME*. 2.

OJK. (n.d.). *Pedoman Keamanan Siber Bagi Penyelenggara Inovasi Teknologi Sektor Keuangan (ITSK)*.

Romi Faslah. (2024). *IDENTITAS NASIONAL, GEOSTRATEGI, DAN GEOPOLITIK: Membangun Keberlanjutan dan Kedaulatan* (1st ed.). PT.Literasi Nusantara Abadi Grup.http://repository.uin-malang.ac.id/20872/

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). *Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia*. 2(2). https://scholarhub.ui.ac.id/jkskn/vol2/iss2/7/

Vimy, T., Wiranto, S., Widodo, P., & Suwarno, P. (2022). *ANCAMAN SERANGAN SIBER PADA KEAMANAN NASIONAL INDONESIA*. 6(1).

Yustika Citra & Ni Komang Desy. (2023). *STRATEGI PENANGANAN KEAMANAN SIBER (CYBER SECURITY) DI INDONESIA*. *Volume 6*. https://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/20659