Journal of Science and Social Research ISSN 2615 – 4307 (Print)
May 2025, VIII (2): 1748 – 1754 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

PENGUATAN REGULASI PERLINDUNGAN INFRASTRUKTUR KRITIS DI INDONESIA TERHADAP ANCAMAN SERANGAN "DDOS"

Alvin Pradika[1], Adinda Hilda Rachmania[2], Alifia Widianti[3], Pudji Astuti[4]
Universitas Negeri Surabaya, Surabaya
e-mail: [1]alvin.23030@mhs.unesa.ac.id, [2]adinda.23029@mhs.unesa.ac.id,
[3]alifia.23031@mhs.unesa.ac.id, [4]pudjiastuti@unesa.ac.id

Abstract: *Strengthening regulations for the protection of critical infrastructure has become a primary urgency in Indonesia to address the threat of Distributed Denial of Service (DDoS) attacks. Critical infrastructure such as communication networks, financial systems, public services, and energy are increasingly vulnerable to these attacks due to their reliance on digital technologies. This study analyzes the vulnerability of Indonesia's critical infrastructure to DDoS attacks and formulates strategic steps and effective regulatory recommendations. Through a holistic approach that encompasses advanced technologies, adaptive regulations, and cross-sector collaboration, it is expected that Indonesia can enhance national resilience against cyber threats. The application of resilience theory and game theory also supports the development of better mitigation strategies. This research provides a foundation for strengthening cybersecurity regulations to maintain national economic, social, and security stability.*

Keyword: *Regulation, Critical Infrastructure, DDoS, Cybersecurity, National Resilience, Resilience Theory, Game Theory*

Abstrak: Penguatan regulasi perlindungan infrastruktur kritis menjadi urgensi utama di Indonesia untuk menghadapi ancaman serangan Distributed Denial of Service (DDoS). Infrastruktur kritis seperti halnya jaringan komunikasi, sistem keuangan, layanan publik, dan energi semakin rentan terhadap serangan ini akibat ketergantungan pada teknologi digital. Penelitian ini menganalisis tingkat kerentanan infrastruktur kritis Indonesia terhadap serangan DDoS dan merumuskan langkah strategis serta rekomendasi regulasi yang efektif. Dengan pendekatan holistik yang mencakup teknologi canggih, regulasi adaptif, dan kolaborasi lintas sektor, diharapkan Indonesia mampu meningkatkan ketahanan nasional terhadap ancaman siber. Penerapan teori resiliensi dan teori game juga mendukung pengembangan strategi mitigasi yang lebih baik. Penelitian ini memberikan dasar untuk memperkuat regulasi keamanan siber demi menjaga stabilitas ekonomi, sosial, dan keamanan nasional.

Kata kunci: Regulasi, Infrastruktur Kritis, DDoS, Keamanan Siber, Ketahanan Nasional, Teori Resiliensi, Teori Game.

PENDAHULUAN

Kemajuan teknologi saat ini seperti informasi dan komunikasi telah membawa dampak terhadap berbagai aspek kehidupan, termasuk ekonomi, pemerintahan, dan masyarakat secara keseluruhan. Infrastruktur kritis, seperti jaringan telekomunikasi, sistem keuangan, layanan kesehatan, dan transportasi, bergantung pada teknologi digital untuk menjaga operasionalnya tetap berjalan. Pemerintah Indonesia telah memberikan beberapa dukungan dalam akses internet di Indonesia melalui beberapa program dan kebijakan. Pemerintah juga terus mendorong akses internet dan teknologi digital ke seluruh wilayah Indonesia melalui berberapa program seperti Gerakan Nasional 1000 Startup Digital yang merupakan program yang diluncurkan oleh Kementerian

Komunikasi dan Informatika (Kominfo) pada tahun 2016 (Hapsari & Pambayun, 2023). Namun, ketergantungan yang semakin besar terhadap teknologi ini juga meningkatkan risiko terhadap ancaman keamanan siber, termasuk serangan Distributed Denial of Service (DDoS).

Distributed Denial of Service Attack (DDoS) merupakan serangan dengan mengkompilasi beberapa sistem di internet dengan zombie/agen yang terinfeksi dan membentuk jaringan botnet. Serangan DDoS mengakibatkan kerugian finansial, hilangnya produktivitas, kerusakan merek, penurunan peringkat kredit dan asuransi serta terganggunya hubungan pelanggan, dan pemasok (Purba et al., 2022). Serangan ini tidak hanya berdampak pada kerugian finansial yang besar tetapi juga mengancam kestabilan sosial dan keamanan nasional, terutama jika infrastruktur kritis menjadi target utama. Indonesia, sebagai negara dengan pertumbuhan teknologi yang pesat, tidak luput dari ancaman serangan DDoS. Berbagai sektor, mulai dari perbankan, layanan publik, hingga sektor energi, telah menjadi target potensial serangan tersebut. Ketergantungan yang tinggi terhadap teknologi digital membuat infrastruktur kritis di Indonesia rentan terhadap gangguan operasional yang dapat merugikan masyarakat luas.

Ada banyak alat di Internet dengan skrip PHP dan Perl, jadi tidak sulit untuk mengimplementasikan serangan ini. Banyak PC zombie berpartisipasi dalam serangan ini dan melakukan serangan DoS. Individu atau kelompok yang tidak bermoral dapat menggunakan Internet untuk memblokir atau menghapus situs web, mengalihkan router, dan menolak akses ke orang lain (Julda Alhafiz et al., 2023). Sayangnya, perlindungan terhadap infrastruktur kritis di Indonesia masih menghadapi berbagai tantangan. Salah satunya adalah kurangnya regulasi yang komprehensif dan terintegrasi dalam menangani ancaman siber, termasuk serangan DDoS.

Meskipun sudah ada beberapa peraturan terntang keamanan siber, seperti Undang- Undang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), kerangka regulasi ini belum secara spesifik mengatur perlindungan terhadap infrastruktur kritis dari ancaman DDoS. Di tingkat global, banyak negara telah mengembangkan regulasi khusus untuk melindungi infrastruktur kritis mereka dari serangan siber. Misalnya, Amerika Serikat memiliki Critical Infrastructure Protection Plan yang mencakup langkah-langkah mitigasi ancaman DDoS, sementara Uni Eropa mengadopsi Network and Information Security Directive (NIS Directive) yang mewajibkan negara anggota untuk mengimplementasikan langkah-langkah perlindungan terhadap infrastruktur penting. Hal ini menunjukkan pentingnya regulasi yang terfokus dan terarah dalam menghadapi ancaman siber yang terus berkembang.

Denial of Service (DoS) Attack, yang mana DoS Attack ini merupakan bentuk akhir dari tindakan cracking, yang mana mempunyai dampak yang sangat buruk terhadap suatu sistem. Cracking adalah proses bagaimana seseorang menyusup ke dalam sistem milik orang lain, dengan tujuan untuk merusak sistem tersebut (Cheny Berlian, 2022). Dalam konteks Indonesia, urgensi untuk memiliki regulasi perlindungan infrastruktur kritis dari ancaman DDoS menjadi semakin nyata. Regulasi ini tidak hanya bertujuan untuk melindungi sistem dan layanan yang menjadi tulang punggung masyarakat, tetapi juga untuk meningkatkan ketahanan nasional terhadap ancaman siber. Dengan adanya regulasi yang jelas, diharapkan pemerintah, sektor swasta, dan masyarakat dapat bersinergi secara efektif untuk mengidentifikasi, mencegah, dan merespons serangan DDoS. Selain itu, pengembangan regulasi ini juga perlu mempertimbangkan perkembangan teknologi dan dinamika ancaman siber. Serangan DDoS terus berevolusi dengan memanfaatkan teknologi baru seperti

Internet of Things (IoT) yang merupakan teknologi yang dirancang untuk memudahkan kita dengan memungkinkan koneksi dengan berbagai perangkat melalui internet. Dengan IoT, pekerjaan sehari-hari menjadi lebih mudah dan efisien (Junaidi & Ramadhani, 2024). Oleh karena itu, regulasi yang dirancang harus bersifat adaptif dan mampu menghadapi tantangan di masa depan.

Kolaborasi internasional juga menjadi aspek penting dalam menghadapi ancaman global ini, mengingat sifat serangan DDoS yang tidak mengenal batas wilayah. Dalam upaya menyusun regulasi perlindungan infrastruktur kritis dari ancaman DDoS, pendekatan holistik yang mencakup aspek teknis, hukum, dan sosial perlu diambil. Langkah ini mencakup identifikasi aset kritis, analisis risiko, penerapan standar keamanan, peningkatan kapasitas sumber daya manusia, serta peningkatan kesadaran masyarakat tentang pentingnya perlindungan infrastruktur kritis. Dengan demikian, regulasi ini tidak hanya menjadi instrumen hukum, tetapi juga menjadi pedoman strategis untuk memperkuat keamanan dan ketahanan nasional di era digital. Melalui dokumen ini, akan dibahas secara mendalam mengenai pentingnya regulasi perlindungan infrastruktur kritis dari ancaman DDoS, tantangan yang dihadapi, serta beberapa langkah strategis yang dapat diambil untuk mewujudkan regulasi yang efektif dan komprehensif. Dengan pemahaman yang lebih baik tentang ancaman dan solusi yang dapat diimplementasikan, diharapkan Indonesia dapat meningkatkan kesiapan dan kapasitasnya dalam menghadapi serangan DDoS dan ancaman siber lainnya.

Tujuan dari penelitian ini adalah untuk:

1. Mengidentifikasi tantangan yang dihadapi dalam perlindungan infrastruktur kritis di Indonesia dari ancaman DDoS.
2. Menganalisis kebijakan dan regulasi yang sudah ada terkait keamanan siber di Indonesia.
3. Memberikan rekomendasi strategis
4. untuk pengembangan regulasi perlindungan infrastruktur kritis yang efektif, komprehensif, dan adaptif terhadap ancaman DDoS.
5. Meningkatkan pemahaman tentang pentingnya kolaborasi antar sektor dan lintas negara dalam menghadapi ancaman DDoS secara global.

Melalui dokumen ini, akan dibahas secara mendalam mengenai pentingnya regulasi perlindungan infrastruktur kritis dari ancaman DDoS, tantangan yang dihadapi, serta beberapa langkah strategis yang dapat diambil untuk mewujudkan regulasi yang efektif dan komprehensif. Dengan pemahaman yang lebih baik tentang ancaman dan solusi yang dapat diimplementasikan, diharapkan Indonesia dapat meningkatkan kesiapan dan kapasitasnya dalam menghadapi serangan DDoS dan ancaman siber lainnya.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif-analitis untuk menganalisis kondisi keamanan infrastruktur kritis di Indonesia terhadap ancaman Distributed Denial of Service (DDoS). Data dikumpulkan melalui beberapa studi literatur yang mencakup jurnal ilmiah, peraturan hukum, dan publikasi resmi, serta analisis dokumen kebijakan seperti UU ITE dan PP PSTE yang dibandingkan dengan regulasi internasional, seperti Critical Infrastructure Protection Plan di AS dan NIS Directive di Uni Eropa. Pendekatan holistik digunakan untuk mengkaji aspek teknis, hukum, dan sosial, guna memahami tantangan dan merumuskan langkah strategis. Analisis komparatif dilakukan untuk menemukan kesenjangan dan peluang peningkatan kerangka regulasi di Indonesia. Hasil penelitian ini bertujuan merumuskan rekomendasi kebijakan regulasi yang efektif dan komprehensif untuk

meningkatkan perlindungan infrastruktur kritis dari ancaman DdoS

HASIL DAN PEMBAHASAN

Keamanan Siber dan Infrastruktur Kritis

Keamanan siber adalah bidang yang bertujuan melindungi sistem informasi, jaringan, dan data dari ancaman digital untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi. Menurut National Institute of Standards and Technology (NIST), keamanan siber juga berkaitan erat dengan keamanan infrastruktur kritis, yaitu aset fisik dan virtual yang menopang fungsi vital masyarakat, seperti energi, transportasi, komunikasi, dan sektor keuangan. Gangguan pada infrastruktur ini dapat menyebabkan dampak besar terhadap ekonomi, keamanan nasional, dan kesejahteraan publik.

Untuk melindungi infrastruktur kritis, diperlukan strategi keamanan yang efektif. Langkah pertama adalah memantau jaringan secara menyeluruh menggunakan sistem log untuk mendeteksi aktivitas mencurigakan, seperti login gagal atau transfer data ilegal. Kedua, gunakan teknologi canggih seperti sistem deteksi intrusi, pemindai malware, dan analisis perilaku untuk mendeteksi ancaman dengan cepat. Ketiga, susun kebijakan tanggap darurat keamanan siber yang jelas dan latih staf agar siap menghadapi serangan siber dengan tepat (Laksana & Mulyani, 2024).

Serangan DDoS: Definisi dan Dampaknya

Serangan Distributed Denial of Service (DDoS) adalah salah satu bentuk ancaman dunia maya yang serius di mana penyerang berusaha untuk memblokir akses ke layanan, server, atau aplikasi dengan membanjiri target dengan lalu lintas internet yang sangat besar, sehingga menyebabkan kelumpuhan atau penurunan kinerja layanan tersebut, yang dilakukan melalui jaringan perangkat yang terinfeksi malware (botnet) yang dikendalikan dari jarak jauh, dan dampaknya tidak hanya merugikan secara finansial karena gangguan operasional yang menyebabkan kerugian akibat tidak dapat mengakses layanan atau situs web penting, tetapi juga menimbulkan kerusakan lebih lanjut pada infrastruktur teknologi yang ada, dengan dampak operasional yang signifikan seperti hilangnya produktivitas dari sistem yang terganggu, yang pada gilirannya menyebabkan gangguan pada kegiatan bisnis dan menyebabkan waktu henti yang merugikan reputasi perusahaan atau organisasi yang menjadi target.

Serangan siber tidak hanya bertujuan untuk merusak sistem komputer, tetapi juga menyasar aspek ekonomi, sosial, maupun pemerintahan. Serangan ini tidak terbatas oleh letak geografis karena perangkat komputer tidak terpengaruh oleh jarak atau lokasi wilayah tertentu. Hal inilah yang membuat potensi serangan siber jauh lebih luas dan lebih beragam dibandingkan dengan serangan konvensional. Sehingga perlu adanya Cyber security, yang merupakan tindakan untuk melindungi operasi sistem komputer atau integrasi data di dalamnya dari aksiaksi kejahatan Konsep cyber security merujuk kepada persepsi ancaman yang dihadapi mengingat aktivitas yang terhubung melalui internet adalah borderless (Weu, 2020).

Rancangan Regulasi Serangan Siber DDoS

Regulasi dan standar keamanan siber dirancang untuk melindungi data serta sistem informasi dari ancaman siber dengan memastikan pemenuhan persyaratan seperti kerahasiaan, integritas, dan ketersediaan informasi. Regulasi ini mencakup berbagai kebijakan, seperti penggunaan enkripsi, kontrol akses, pemantauan, audit, dan pedoman internasional seperti GDPR dan ISO/IEC 27001, yang berfokus pada pengelolaan

data pribadi dan manajemen risiko keamanan informasi.

Terkait serangan siber Distributed Denial of Service (DDoS), regulasi menetapkan kewajiban bagi pemangku kepentingan untuk menerapkan langkah-langkah pencegahan, seperti penggunaan firewall, sistem deteksi intrusi (IDS), dan teknologi mitigasi DDoS. Selain itu, regulasi mewajibkan pemberian edukasi kepada pengguna, deteksi dini, serta pelaporan dan penanggulangan serangan secara cepat melalui koordinasi dengan pihak berwenang dan tim tanggap darurat keamanan siber

Pelanggaran terhadap regulasi ini dapat dikenakan sanksi administratif, perdata, atau pidana, dan penyelesaian sengketa dilakukan melalui musyawarah, mediasi, atau pengadilan. Pemerintah memantau implementasi regulasi ini melalui badan pengawas keamanan siber dan melakukan evaluasi berkala untuk memastikan efektivitasnya. Regulasi dapat diperbarui sesuai perkembangan teknologi dan disosialisasikan kepada masyarakat guna meningkatkan kesadaran akan ancaman siber.

Pendekatan Holistik dalam Perlindungan Infrastruktur Kritis

Pendekatan holistik dalam melindungi infrastruktur kritis dari serangan DDoS melibatkan strategi terintegrasi yang mencakup pencegahan, deteksi, respons, dan pemulihan. Teknologi canggih seperti sistem pencegahan intrusi (IPS), pemantauan lalu lintas jaringan real-time, firewall adaptif, dan penggunaan kecerdasan buatan (AI) serta pembelajaran mesin (ML) berperan penting dalam mengidentifikasi dan mengantisipasi pola serangan. Strategi ini dipadukan dengan kebijakan redundansi dan cadangan untuk memastikan kelangsungan operasional meskipun terjadi serangan, serta audit keamanan reguler untuk menguji kerentanan sistem. Peran pemerintah dan badan pengatur juga krusial dalam menetapkan pedoman keamanan dan standar bagi operator infrastruktur kritis.

Kolaborasi lintas sektor menjadi elemen kunci, dengan melibatkan penyedia layanan internet (ISP), organisasi keamanan siber, dan pemangku kepentingan lainnya dalam berbagi informasi dan sumber daya. Kerjasama ini mencakup pengelolaan risiko melalui analisis dampak serangan terhadap operasi, prioritas perlindungan aset vital, dan koordinasi respons lintas batas negara. Pendekatan ini menekankan perlindungan yang tidak hanya reaktif tetapi juga proaktif, mendukung pengembangan sistem yang inovatif, dan mempromosikan keamanan nasional yang lebih kuat di tengah ancaman siber yang semakin kompleks.

Teori Resilensi Sistem

Teori resiliensi sistem menurut Van Breda (2013) merupakan sebuah kekuatan dan sebuah sistem yang memungkinkan individu untuk terus kuat berada di sebuah keterpurukan (Syah et al., 2023), khususnya infrastruktur kritis, untuk mengadaptasi, menyerap, dan pulih dari gangguan atau gangguan besar dengan memastikan kelangsungan operasional melalui proses persiapan yang matang, respons yang cepat terhadap ancaman yang muncul, dan pemulihan yang efisien, di mana dalam konteks keamanan informasi, model CIA (Confidentiality, Integrity, Availability) menjadi dasar fundamental yang menuntut perlindungan informasi dari akses yang tidak sah atau kebocoran (Confidentiality), memastikan bahwa data tetap akurat, konsisten, dan bebas dari perubahan yang tidak sah yang dapat merusak proses atau pengambilan keputusan (Integrity), serta menjamin aksesibilitas informasi dan layanan penting kapan saja dan tanpa hambatan, meskipun menghadapi potensi serangan atau gangguan, dengan tujuan untuk menjaga keberlanjutan operasional, mencegah kerugian yang lebih besar, dan memastikan sistem tetap dapat berfungsi secara optimal bahkan setelah terjadi serangan, bencana alam, atau kegagalan teknis yang tak terduga, yang semakin penting seiring dengan

meningkatnya ketergantungan pada teknologi dan interkonektivitas di berbagai sektor, mulai dari energi, transportasi, kesehatan, hingga keuangan, yang menjadikan resiliensi sebagai salah satu aspek penting dalam pengelolaan risiko dan kebijakan keamanan siber, karena sistem yang memiliki tingkat resiliensi tinggi dapat lebih cepat pulih dan meminimalkan dampak negatif pada masyarakat, ekonomi, dan negara, sehingga menciptakan landasan yang kokoh untuk menjaga kestabilan serta integritas dari berbagai layanan yang menyentuh kehidupan sehari-hari masyarakat.

Teori Game

Teori game adalah pendekatan matematis untuk menganalisis persaingan dan konflik antara berbagai kepentingan. Dalam konteks keamanan siber, teori ini digunakan untuk memodelkan interaksi antara penyerang dan defender. Penyerang berupaya mengeksploitasi kerentanan sistem, sementara defender bertujuan mencegah, mendeteksi, dan merespons ancaman. Model zero-sum sering digunakan, di mana keuntungan satu pihak berarti kerugian bagi pihak lain. Contohnya, defender dapat mengalokasikan sumber daya untuk perlindungan dengan mempertimbangkan adaptasi strategi dari penyerang, seperti DDoS, phishing, atau ransomware (Natasya, 2022).

Pendekatan teori game dalam keamanan siber mencakup strategi seperti Nash equilibrium, yang menggambarkan situasi di mana kedua pihak tidak dapat meningkatkan hasil mereka dengan mengubah strategi secara sepihak. Defender yang mampu memprediksi langkah penyerang dapat mencapai hasil optimal, sedangkan penyerang yang menemukan kelemahan baru dapat memperoleh keunggulan. Penerapan model non-zero-sum juga relevan dalam situasi di mana kedua pihak saling bereaksi dan menyesuaikan strategi berdasarkan pengalaman dan pengetahuan dari interaksi sebelumnya. Teori game dalam keamanan siber semakin efektif dengan bantuan kecerdasan buatan (AI) dan pendekatan berbasis data. Defender dapat memanfaatkan simulasi dan model probabilistik untuk memprediksi jenis serangan yang mungkin terjadi dan merancang langkah mitigasi yang efisien. Strategi seperti penggunaan honeypots atau perangkap bertujuan mengalihkan perhatian penyerang dari target utama. Dengan pemahaman ini, organisasi dapat berpikir lebih strategis, mengantisipasi langkah penyerang, dan memperkuat kebijakan keamanan mereka dalam menghadapi ancaman yang terus berkembang (Natasya, 2022).

SIMPULAN

Penelitian ini berhasil mengidentifikasi tantangan utama yang dihadapi dalam melindungi infrastruktur kritis di Indonesia dari ancaman serangan DDoS, menganalisis regulasi yang ada, dan memberikan rekomendasi strategis untuk memperkuat perlindungan terhadap ancaman siber. Dengan pendekatan kualitatif yang holistik, penelitian ini mengungkapkan bahwa tantangan perlindungan infrastruktur kritis di Indonesia tidak hanya mencakup aspek teknis tetapi juga melibatkan keterbatasan regulasi, kolaborasi lintas sektor, dan kesenjangan antara standar internasional dan kebijakan lokal. Analisis ini menyoroti pentingnya adopsi teknologi canggih seperti kecerdasan buatan dan pembelajaran mesin, penguatan kerangka hukum, serta pembentukan budaya keamanan siber yang tangguh dan inklusif. Melalui pembenaran ilmiah berbasis teori resilien sistem dan teori game, penelitian ini memberikan wawasan bahwa perlindungan infrastruktur kritis bukan sekadar soal reaksi terhadap serangan, melainkan juga tentang membangun kapasitas adaptasi, respons cepat, dan pemulihan yang efisien untuk memastikan kontinuitas operasional. Penelitian ini memperkuat pengetahuan terkini dengan

mengintegrasikan pendekatan teknis, hukum, dan sosial, serta menekankan perlunya kolaborasi lintas batas negara dalam menghadapi ancaman yang bersifat global. Dengan demikian, penelitian ini berkontribusi pada pengembangan kerangka regulasi yang lebih efektif, adaptif, dan komprehensif, yang tidak hanya relevan untuk Indonesia tetapi juga menjadi model yang dapat diterapkan di negara lain yang menghadapi tantangan serupa dalam keamanan siber.

DAFTAR PUSTAKA

Cheny, Berlian. (2022). Dos Attack Sebagai Tindak Pidana Siber Dalam Pengaturan Hukum Di Indonesia. Journal Equitable, 7(1), 1–25. https://doi.org/10.37859/jeq.v7i1.3686

Hapsari, R. D., & Pambayun, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis. Jurnal Konstituen, 5(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208 Julda Alhafiz, M., Fauzi, A., Dwiansyah, A.,

Revana Indriani, B., Maulana Andhito Putra, F., & Ridho Ridwani, R. (2023). Dampak Denial of Service pada Perusahaan Perbankan di Indonesia. Jurnal Ilmu Multidisplin, 2(1), 114–120. https://doi.org/10.38035/jim.v2i1.233

Junaidi, J., & Ramadhani, K. (2024). Efektivitas Internet of Things (Iot) Pada Sektor Pertanian. Jurnal Teknisi, 4(1), 12. https://doi.org/10.54314/teknisi.v4i1.1793

Kusumoningtyas A.A & Puspitasari. (2020). Dilema Hak Perlindungan Data Pribadi Dan Pengawasan Siber: Tantangan Di Masa Depan. Legislasi Indonesia, 17(2), 234–250.

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan. Jurnal Ilmiah Multidisiplin, 3(01), 109–122. https://doi.org/10.56127/jukim.v3i01.1143

Natasya, C. (2022). KENALAN LEBIH DEKAT DENGAN GAME THEORY. Student-Activity.Binus. https://student-activity.binus.ac.id/himmat/2022/04/kenalan-lebih-dekat-dengan-game-theory/

Purba, R., Lestari, W. S., & Ulina, M. (2022). Deteksi Serangan DDoS Mengunakan Deep Q-Network. Jurnal Teknik Informatika Dan Sistem Informasi, 9(1), 648–658. http://jurnal.mdp.ac.id

Syah, A. M., Alfarras, M. B., Rizkiya, A. N., Ruslina, E., & Gustini, D. R. (2023).

Resiliensi Perekonomian Indonesia Di masa Endemic Covid-19. Das Sollen, 1(1), 1–14. https://doi.org/10.11111/moderasi.xxxx xxx

Weu, M. R. (2020). Kerjasama Pemerintah Indonesia Dan Pemerintah Kerajaan Inggris Dalam Bidang Keamanan Siber. Global Political Studies Journal, 4(2), 154–169. https://doi.org/10.34010/gpsjournal.v4i 2.5879