JURNAL MEDIA AKADEMIK (JMA)
Vol.3, No.6 Juni 2025
e-ISSN: 3031-5220; DOI: 10.62281, Hal XX-XX
PT. Media Akademik Publisher
AHU-084213.AH.01.30.Tahun 2023

CYBER SECURITY DAN KETAHANAN NASIONAL: TANTANGAN DAN SOLUSI DI ERA DIGITAL

Oleh:

Alvin Sudiatma Syawaluddin[1]
Achmad Fadhilah Putra H[2]
Mayzen Putra A[3]

Universitas Muhammadiyah Surabaya
Alamat: JL. Raya Sutorejo No.59, Dukuh Sutorejo, Kec. Mulyorejo, Surabaya, Jawa Timur (60113).
Korespondensi Penulis: anugrahmayzen@gmail.com

Abstract. *The development of digital technology has had a significant impact on various aspects of life, including the national defense and security system. In the digital era, cyber threats have become a strategic challenge that is not only technical in nature, but also has a direct impact on the political, economic, and social stability of a country. Indonesia as a developing country is facing an increasing number of cyber incidents targeting vital infrastructure such as government data, the banking sector, and public services. One example is the ransomware attack on the Temporary National Data Center (PDSN) which shook public trust in the country's digital system. Weak infrastructure, lack of competent human resources, and minimal regulation and coordination between institutions are the main obstacles in building strong national resilience in cyberspace. This study aims to identify the most significant types of cyber threats, analyze cybersecurity challenges in Indonesia, and formulate concrete strategies and solutions that can be implemented to strengthen the digital defense system. Strengthening governance, human resource development, and increasing collaboration with multi-ethnics are the keys to overcoming the growth of cyber threats.*

Keywords: *Cybersecurity, National Resilience, Digital Threats.*

Received June 14, 2025; Revised June 20, 2025; June 28, 2025
*Corresponding author: *anugrahmayzen@gmail.com*

CYBER SECURITY DAN KETAHANAN NASIONAL: TANTANGAN DAN SOLUSI DI ERA DIGITAL

Abstrak. Perkembangan teknologi digital telah membawa dampak signifikan terhadap berbagai aspek kehidupan, termasuk sistem pertahanan dan keamanan nasional. Di era digital, ancaman siber menjadi tantangan strategis yang tidak hanya bersifat teknis, tetapi juga berdampak langsung pada stabilitas politik, ekonomi, dan sosial suatu negara. Indonesia sebagai negara berkembang menghadapi peningkatan jumlah insiden siber yang menargetkan infrastruktur vital seperti data pemerintahan, sektor perbankan, dan layanan publik. Salah satu contohnya adalah serangan ransomware pada Pusat Data Nasional Sementara (PDSN) yang mengguncang kepercayaan publik terhadap sistem digital negara. Kelemahan infrastruktur, kurangnya sumber daya manusia yang kompeten, serta minimnya regulasi dan koordinasi antar lembaga menjadi hambatan utama dalam membangun ketahanan nasional yang tangguh di ruang siber. Penelitian ini bertujuan untuk mengidentifikasi jenis ancaman siber yang paling signifikan, menganalisis tantangan keamanan siber di Indonesia, serta merumuskan strategi dan solusi konkret yang dapat diterapkan untuk memperkuat sistem pertahanan digital. Memperkuat tata kelola, pengembangan sumber daya manusia, dan peningkatan kolaborasi dengan multi-ektis adalah kunci kunci untuk mengatasi pertumbuhan ancaman cyber.

Kata Kunci: Keamanan Siber, Ketahanan Nasional, Ancaman Digital.

LATAR BELAKANG

Pengembangan teknologi digital telah membawa perubahan besar dalam banyak aspek kehidupan, termasuk pertahanan dan keamanan nasional. Perkembangan dalam dunia teknologi dan siber telah membawa bawa kemajuan yang bermanfaat dari berbagai macam sisi didalamnya(Alfi et al., 2023). Di era digital saat ini, ancaman dunia maya tidak hanya masalah teknis, tetapi juga masalah strategis yang dapat menempatkan keberadaan negara dan kedaulatan dalam risiko. Serangan cyber dapat memiliki efek yang lebih luas dan lebih menghancurkan daripada ancaman fisik, mulai dari kebocoran data kritis hingga kelumpuhan infrastruktur kritis negara dalam hitungan detik. Kondisi ini membutuhkan kemauan nasional yang adaptif dan ketahanan terhadap dinamika mengancam di dunia maya.

Ancaman siber yang kian berkembang merupakan dampak dari globalisasi, di mana aktivitas masyarakat mulai beralih dari metode konvensional ke sistem berbasis

teknologi informasi dan komunikasi yang saling terkoneksi (Darumaya et al., 2023). Ketahanan nasional di era digital tidak hanya mencakup aspek pertahanan militer, tetapi juga aspek ekonomi, sosial, budaya, dan terutama keamanan siber. Infrastruktur kritis seperti jaringan listrik, sektor perbankan, layanan publik, dan sistem negara adalah target utama serangan siber yang dapat memengaruhi stabilitas dan kesejahteraan masyarakat. Baik aktor negara bagian maupun non-negara memiliki opsi untuk meluncurkan serangan siber dengan berbagai motif, mulai dari pencurian data hingga jamming sistem kritis di negara ini. Dalam perkembangan zaman yang selalu berkembang, keamanan nasional pada negara semakin rentan mengalami serangan cybercrime yang semakin pesat dan mengganggu. (Hasan et al., 2023).

Indonesia sendiri mengekspos berbagai insiden cyber yang mengkhawatirkan. Salah satunya adalah serangan ransomware pada pusat data nasional sementara (PDSN) Central-2024, yang mengarah pada gangguan dengan layanan negara dan kunci data kritis. Kejadian ini menunjukkan bahwa sistem keamanan siber nasional masih menawarkan kebutuhan akan strategi yang lebih komprehensif untuk meningkatkan kesenjangan dan resistensi cyber. Selain memperkuat teknologi dan infrastruktur, tantangan utama lainnya adalah memperkuat kesadaran dunia maya di semua tingkat masyarakat dan meningkatkan kerja sama antara pemerintah, sektor swasta dan masyarakat sipil. Langkah-langkah yang diambil masih ersifat sektoral, bergantung pada kepentingan, kemampuan, dan penangkalan yang belum optimal. Hal ini membuat sistem keamanan siber Indonesia masih sangat rentan terhadap serangan yang bersifat masif(Mudra & Prasidya, 2024).

Oleh karena itu, makalah ini menjelaskan dan memberikan solusi strategis yang dapat diimplementasikan, menjelaskan tantangan utama Indonesia dalam mempertahankan keamanan siber dan ketahanan nasional di era digital. Fokus diskusi akan mencakup peran pedoman, memperkuat tata kelola, mengembangkan sektor SDM, dan kerja sama antar sektor sebagai upaya untuk membangun sistem pertahanan dunia maya adaptif yang resisten terhadap peningkatan ancaman. Adapun kepentingan Indonesia di ruang siber meliputi kedaulatan, ketahanan, dan perlindungan siber. (Salah et al., 2023).

RUMUSAN MASALAH

1. Bagaimana karakteristik dan jenis ancaman siber yang paling signifikan mengancam ketahanan nasional di era digital saat ini?
2. Apa saja kelemahan dan tantangan yang dihadapi Indonesia dalam mengelola keamanan siber untuk menjaga ketahanan nasional?
3. Strategi dan solusi apa yang efektif untuk meningkatkan ketahanan nasional melalui penguatan keamanan siber di Indonesia?

TUJUAN PENELITIAN

1. Menganalisis berbagai jenis dan karakteristik ancaman siber yang berpotensi mengganggu ketahanan nasional di era digital.
2. Mengidentifikasi kelemahan dan tantangan utama yang dihadapi Indonesia dalam pengelolaan keamanan siber nasional.
3. Merumuskan strategi dan solusi yang dapat diterapkan untuk memperkuat ketahanan nasional melalui peningkatan keamanan siber secara komprehensif

KAJIAN TEORITIS

Keamanan cyber adalah upaya sistematis untuk melindungi sistem, jaringan, dan data dari berbagai ancaman digital yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Dalam konteks ketahanan nasional, keamanan siber menjadi aspek fundamental karena serangan siber memiliki potensi untuk melumpuhkan infrastruktur vital negara seperti sektor energi, keuangan, dan pemerintahan. Ketahanan nasional sendiri didefinisikan sebagai kemampuan suatu negara dalam menjaga kedaulatan, keutuhan wilayah, serta kesejahteraan masyarakat dari berbagai ancaman, termasuk ancaman di ranah digital.

Ancaman siber di era digital semakin kompleks dan melibatkan aktor negara maupun non-negara, dengan motif yang beragam mulai dari spionase, sabotase, hingga kejahatan ekonomi. Serangan siber seperti ransomware, Advanced Persistent Threats (APT), dan pencurian data telah menimbulkan dampak yang signifikan terhadap stabilitas dan keamanan nasional. Oleh karena itu, penguatan keamanan siber tidak hanya menjadi

tanggung jawab pemerintah, tetapi juga memerlukan kolaborasi lintas sektor, termasuk sektor swasta dan masyarakat sipil.

Selain aspek teknis dan politik, kemampuan digital dan pelatihan di pemerintah daerah adalah dasar utama untuk membangun perlawanan nasional di era digital. Peningkatan kesadaran dan kemampuan masyarakat dalam menghadapi ancaman siber dapat meminimalkan risiko serta memperkuat pertahanan negara secara menyeluruh. Dengan demikian, landasan teori dalam penelitian ini menekankan pentingnya integrasi antara teknologi, kebijakan, tata kelola, serta pengembangan sumber daya manusia untuk menghadapi tantangan dan merumuskan solusi keamanan siber demi ketahanan nasional yang berkelanjutan.

METODE PENELITIAN

Metode penelitian yang digunakan dalam kajian ini adalah pendekatan kualitatif deskriptif. Pendekatan ini dipilih untuk memperoleh pemahaman yang mendalam mengenai karakteristik serta jenis ancaman siber yang paling signifikan dalam mengancam ketahanan nasional di era digital saat ini. Data penelitian dikumpulkan melalui studi literatur, yaitu dengan menelaah berbagai sumber seperti jurnal ilmiah, laporan insiden siber, dokumen kebijakan nasional, serta publikasi resmi pemerintah dan lembaga keamanan siber. Selain itu, peneliti juga melakukan analisis dokumen terhadap laporan insiden dan regulasi yang berkaitan dengan keamanan siber di Indonesia. Data yang telah terkumpul kemudian dianalisis menggunakan teknik analisis konten untuk mengidentifikasi tema-tema utama terkait pola, karakteristik, dan jenis ancaman siber, serta kelemahan dan tantangan dalam sistem keamanan siber nasional. Proses analisis dilakukan melalui reduksi data agar fokus pada isu-isu utama, kemudian diinterpretasikan untuk merumuskan kesimpulan dan rekomendasi strategis yang dapat diterapkan dalam penguatan ketahanan nasional. Dengan metode ini, penelitian diharapkan mampu memberikan gambaran komprehensif mengenai ancaman siber yang signifikan serta solusi strategis yang relevan untuk konteks Indonesia.

HASIL DAN PEMBAHASAN

Karakteristik Dan Jenis Ancaman Siber Yang Paling Signifikan Mengancam Ketahanan Nasional Di Era Digital Saat Ini

Di era digital saat ini, ancaman terhadap ketahanan nasional tidak hanya datang dari agresi fisik, tetapi juga dari serangan yang tidak kasat mata melalui ruang siber. Ancaman siber memiliki karakteristik yang unik beroperasi secara anonim, bersifat lintas batas, sulit dideteksi, dan dapat dilakukan kapan saja tanpa memerlukan kehadiran fisik pelaku. Hal ini menjadikan serangan siber sebagai bentuk ancaman asimetris yang sangat berbahaya, khususnya ketika menyasar sistem vital negara. Negara-negara dengan masyarakat tertutup, seperti Korea Utara, memberikan tantangan khusus bagi para peneliti karena minimnya informasi resmi yang tersedia dan sering kali harus bergantung pada sumber-sumber dari negara rival yang mungkin memiliki bias. (Denning & Jagadish, 2001)

Jenis ancaman siber yang paling signifikan terhadap ketahanan nasional mencakup cyber espionage, di mana data rahasia milik negara atau institusi strategis dicuri untuk kepentingan politik maupun ekonomi oleh aktor negara lain. Ancaman ini berbahaya karena dapat melemahkan strategi nasional dari dalam tanpa disadari. Selain itu, serangan ransomware semakin marak terjadi, di mana data penting disandera oleh pelaku dan hanya akan dibuka kembali setelah tebusan dibayar seringkali menarget institusi layanan publik seperti rumah sakit, lembaga pemerintahan, dan infrastruktur kritikal. Menurut(Wibowo et al., 2023) ada beberapa tantangan besar yang dapat menjadi sandungan bagi dunia industri di tahun mendatang, yaitu ancaman - ancaman terkini yang dapat menyebabkan kerusakan dan kerugian besar yaitu ransomware. Serangan DDoS (Distributed Denial of Service) juga menjadi salah satu metode yang digunakan untuk melumpuhkan sistem layanan daring pemerintah atau swasta, mengganggu pelayanan publik dan menurunkan kepercayaan masyarakat. Ancaman lainnya adalah disinformasi digital, yaitu penyebaran informasi palsu di media sosial yang dapat memecah belah masyarakat, memicu konflik sosial, serta melemahkan legitimasi pemerintah. Menurut (Ananta et al., 2024) serangan Distributed Denial of Service (DDoS) merupakan salah satu bentuk ancaman kejahatan siber yang signifikan di Indonesia.

Kelemahan Dan Tantangan Yang Dihadapi Indonesia Dalam Mengelola Keamanan Siber Untuk Menjaga Ketahanan Nasional

Indonesia menghadapi berbagai kelemahan dan tantangan serius dalam pengelolaan keamanan siber yang berdampak langsung pada ketahanan nasional. Salah satu kelemahan utama adalah keterbatasan infrastruktur dan sistem pertahanan siber nasional yang masih belum merata dan kuat. Banyak institusi pemerintahan belum menerapkan standar keamanan informasi yang memadai, sehingga rentan terhadap serangan siber yang terorganisir maupun acak. Tantangan lain yang signifikan adalah kurangnya sumber daya manusia (SDM) yang ahli di bidang cyber security. Minimnya tenaga profesional dan spesialis keamanan siber membuat respon terhadap insiden menjadi lambat dan kurang efektif. Menurut (Putri & Burhanuddin, 2023). tantangan keamanan siber indonesia dalam industri maritim yaitu Minimnya Sumber Daya Manusia (SDM) yang memiliki pemahaman mengenai keamanan atau ancaman siber menjadi salah satu permasalahan di Indonesia. Berdasarkan data dari NCIS per 28 April 2023, tercatat hanya satu program studi di tingkat Sarjana atau setara yang secara khusus berfokus pada keamanan siber atau keamanan informasi elektronik, yaitu di Universitas Bina Nusantara. Kondisi ini mencerminkan masih rendahnya inisiatif dalam membina dan melatih SDM di bidang keamanan siber. Akibatnya, terjadi kesenjangan dalam ketersediaan tenaga profesional keamanan siber di tingkat nasional. Padahal, kinerja perusahaan sangat krusial untuk dicapai, karena menjadi indikator kemampuan perusahaan dalam mengelola dan mendistribusikan sumber dayanya secara efektif.. (Bhatti & Qureshi, 2007).

Selain itu, rendahnya kesadaran publik dan sektor privat terhadap pentingnya perlindungan data pribadi juga menjadi celah besar bagi pelaku kejahatan siber. Banyak masyarakat yang belum paham akan risiko penggunaan jaringan internet tanpa perlindungan yang memadai. Koordinasi antar lembaga juga menjadi tantangan tersendiri. Indonesia masih menghadapi fragmentasi kebijakan dan tumpang tindih regulasi antar institusi, yang membuat penanganan isu siber menjadi kurang terintegrasi. Di sisi lain, perubahan teknologi yang sangat cepat tidak diiringi dengan pembaruan regulasi dan sistem keamanan yang adaptif, sehingga memperbesar potensi celah keamanan yang bisa dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Menurut(Wicaksono et al., 2024) ketidakefektifan regulasi ini disebabkan oleh ketidak mampuan Undang-Undang a quo untuk menormalkan perkembangan kejahatan siber secara berkelanjutan, terutama dalam hal Tindak pidana siber malware yang

menggunakan kecerdasan buatan (Artificial Intelligence) yang belum diatur secara komprehensif serta terfragmentasinya peraturan perundang-undangan terkait erlindungan dari kejahatan siber.

Strategi Dan Solusi Yang Efektif Untuk Meningkatkan Ketahanan Nasional Melalui Penguatan Keamanan Siber Di Indonesia

Dalam rangka memperkuat ketahanan nasional di era digital, Indonesia harus menyusun strategi dan solusi yang bersifat menyeluruh, proaktif, dan adaptif terhadap perkembangan teknologi. Pertama, pemerintah perlu mengembangkan infrastruktur keamanan siber yang kuat dan merata, termasuk peningkatan kapasitas pertahanan digital pada instansi-instansi strategis, seperti kementerian, lembaga intelijen, dan institusi pelayanan publik. Beberapa sektor yang termasuk dalam kategori tersebut meliputi sektor hukum, energi dan sumber daya mineral (ESDM), transportasi, keuangan dan perbankan, kesehatan, teknologi informasi dan komunikasi, pertanian, pertahanan serta industri strategis, layanan darurat, serta pengelolaan sumber daya air (Cloramidine & Badaruddin, 2023)

Kedua, pengembangan SDM di bidang keamanan siber harus menjadi prioritas nasional. Ini dapat dilakukan melalui pelatihan intensif, pendidikan tinggi berbasis teknologi informasi, dan sertifikasi profesional di bidang cyber security. Kolaborasi antara perguruan tinggi, industri, dan pemerintah sangat diperlukan untuk mencetak generasi pakar keamanan siber yang mampu menghadapi ancaman global. Menurut (Putri & Burhanuddin, 2024) Solusi dalam peningkatan cybersecurity maritim di Indonesia yaitu Peningkatan pelatihan dan pemahaman sumber daya manusia (SDM) di sektor maritim Indonesia menjadi langkah penting dalam mengurangi risiko ancaman siber. Dalam hal ini, penyelenggaraan program pelatihan khusus di bidang keamanan siber sangat diperlukan, dengan fokus pada aspek-aspek yang sesuai dengan lingkungan kerja maritim. Materi pelatihan bisa mencakup simulasi serangan siber guna memberikan pengalaman nyata bagi SDM dalam menghadapi berbagai kemungkinan skenario serangan. Melalui pendekatan edukatif yang berkesinambungan, masyarakat Indonesia dapat terus memperluas pengetahuan mereka mengenai potensi ancaman siber.

Ketiga, reformasi kebijakan dan regulasi siber secara nasional sangat penting dilakukan agar lebih responsif terhadap dinamika ancaman digital. Perlu dibentuk satu

otoritas nasional yang memiliki kewenangan penuh dalam koordinasi pengamanan siber, baik di sektor publik maupun swasta. Selain itu, perlu adanya penegakan hukum yang tegas terhadap pelaku kejahatan siber, serta mekanisme mitigasi dan respon insiden yang cepat dan terukur. Menurut (Wicaksono et al., 2024) pentingnya regulasi keamanan siber di Indonesia serta perlunya penguatan kebijakan untuk melindungi kedaulatan negara di dunia maya. Terakhir, peningkatan kesadaran publik melalui edukasi dan literasi digital juga sangat penting. Masyarakat sebagai pengguna utama ruang siber harus dibekali dengan pemahaman yang baik mengenai etika digital, pentingnya perlindungan data pribadi, serta cara menghadapi hoaks dan informasi palsu.

Dengan strategi yang tepat dan kolaborasi lintas sektor, Indonesia dapat memperkuat ketahanan nasional dari ancaman siber dan menjadikan keamanan digital sebagai bagian integral dari pembangunan nasional yang berkelanjutan.

KESIMPULAN DAN SARAN

Di tengah perkembangan teknologi digital yang pesat, ancaman siber telah menjadi tantangan nyata bagi ketahanan nasional Indonesia. Jenis ancaman siber yang paling signifikan mengancam yaitu cyber espionage, ransomware dan Serangan DDoS (Distributed Denial of Service). Oleh sebab itu, Indonesia masih menghadapi berbagai kelemahan dalam sistem keamanan siber, antara lain terbatasnya infrastruktur teknologi yang tangguh, kurangnya sumber daya manusia yang kompeten di bidang cyber security, rendahnya kesadaran publik terhadap ancaman digital, serta minimnya koordinasi antar lembaga dalam penanganan insiden siber. Hal ini menempatkan Indonesia dalam posisi yang rentan jika tidak segera dilakukan pembenahan secara sistematis.

Dengan demikian, strategi penguatan keamanan siber harus dilakukan melalui pendekatan yang luas. Hal ini meliputi pembangunan infrastruktur siber nasional yang kuat, peningkatan kompetensi SDM melalui pendidikan dan pelatihan berkelanjutan, pembaruan regulasi yang adaptif terhadap dinamika ancaman digital, serta kolaborasi erat antara pemerintah, sektor swasta, dan masyarakat sipil. Edukasi publik juga menjadi elemen penting dalam menciptakan budaya digital yang aman dan sadar risiko. Dengan pelaksanaan strategi yang tepat, Indonesia dapat memperkuat ketahanan nasional di era digital dan membangun sistem pertahanan siber yang responsif, adaptif, serta tahan terhadap berbagai bentuk ancaman yang terus berkembang. Keamanan siber bukan hanya

tanggung jawab satu sektor, melainkan merupakan upaya kolektif dalam menjaga kedaulatan dan keberlangsungan negara di era digital yang penuh ketidakpastian.

DAFTAR REFERENSI

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2), 5. https://doi.org/10.7454/jkskn.v6i2.10082

Ananta, K. D., Ambodo, T., & Tohawi, A. (2024). *Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia*. *9*(2).

Bhatti, K. K., & Qureshi, T. M. (2007). Impact of Employee Participation on Job Satisfaction, Employee Commitment and Employee Productivity. *International Review of Business …*, *3*(2), 54–68. http://www.bizresearchpapers.com/Bhatti.pdf

Cloramidine, F., & Badaruddin, M. (2023). Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (GCI). *Populis : Jurnal Sosial Dan Humaniora*, *8*(1), 57–73. https://doi.org/10.47313/pjsh.v8i1.1957

Darumaya, B. A., Maarif, S., Toruan, T., & Swastanto, Y. (2023). Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan. *Jurnal Keamanan Nasional*, *IX*(2), 299–324.

Denning, D. E., & Jagadish, H. V. (2001). Information Warfare and Security. *SIGMOD Record*, *30*(4), 69–70. https://doi.org/10.1145/604264.604276

Hasan, Z., Apriano, I. D., Simatupang, Y. S., & Muntari, A. (2023). Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online. *Jurnal Multidisiplin Dehasen (MUDE)*, *2*(3), 375–380. https://doi.org/10.37676/mude.v2i3.4153

Mudra, C., & Prasidya, F. G. (2024). *Jurnal Kajian Stratejik Ketahanan Nasional Cybersecurity dan Tata Kelola Intelijen Cybersecurity dan Tata Kelola Intelijen*. *7*(1). https://doi.org/10.7454/jkskn.v7i1.10086

Putri, S. A., & Burhanuddin, A. (2024). Maritime Cybersecurity: Tantangan Dan Strategi Keamanan Maritim Indonesia. *MANDUB: Jurnal Politik, Sosial, Hukum, Dan Humaniora*, *2*(1), 378–386.

Salah, S. S., Gelar, M., Hukum, S., Studi, P., Hukum, I., Hukum, F., & Bosowa, U. (2023). *Program studi ilmu hukum fakultas hukum universitas bosowa makassar 2023*. 1–106.

Wibowo, K., Hidayat, U., & Yasin, V. (2023). Kajian Cyber Security Dalam Rangka Koperasi Menghadapi Revolusi Industri 4.0. *Journal of Information System, Applied, Management, Accounting and Research*, *7*(3), 634–645. https://doi.org/10.52362/jisamar.v7i3.1132

Wicaksono, A. T., Yasin, I. F., & Ampel, U. I. N. S. (2024). *Sectoral Cyber Protection Reformulasi Hukum Pidana Melalui Omnibus Law Sebagai Solusi Perlindungan Siber Yang Bersifat Sektoral Negara Indonesia , sebagai negara penganut sistem hukum civil law , memiliki dari kejahatan siber . 2 Dengan pendekatan yang ko*. 237–261.