MENAWAN: Jurnal Riset Dan Publikasi Ilmu Ekonomi
Vol. 2, No. 3 Mei 2024
e-ISSN: 3025-4728, p-ISSN: 3025-5899, Hal 272-284
DOI: https://doi.org/10.61132/menawan.v2i3.552

Peranan Manajemen Sekuriti Terhadap Keamanan Cyber Bersumber Nilai-Nilai Kebangsaan UUD 1945 Dalam Meningkatkan Efektivitas di Era Digitalisasi Untuk Keamanan Nasional

Destya Fitri Andini
Universitas Bhayangkara Jakarta Raya
Email: destyaandini23@gmail.com

Edy Soesanto
Universitas Bhayangkara Jakarta Raya
Email: edy.soesanto@dsn.ubharajaya.ac.id

Lusiana Prastiwi
Universitas Bhayangkara Jakarta Raya
Email: lusianaprastiwi07@gmail.com

*Korespondensi Penulis : destyaandini23@gmail.com**

Abstract.*In the constantly advancing era of digitalisation, ensuring cyber security has become essential in preserving the integrity, confidentiality, and accessibility of organisational data. The primary focus of this research is to emphasise the importance of cybersecurity awareness in safeguarding systems and information. The 1945 Constitution serves as the primary governing document for the government and legal system. The 1945 Constitution enacts legislation that ensures freedom of expression, a pertinent principle in cyber security. This research aimed to examine the role of security management in enhancing cyber security by applying principles in accordance with the 1945 Constitution. This research identified the factors affecting cyber security awareness and proposed strategies to enhance user awareness through a comprehensive literature review and examined recent findings. Security management is essential for guaranteeing the security of IT systems and infrastructure. Based on a literature review, this study determined the role of security management in assisting organisations in identifying, managing, and addressing security threats effectively. In addition, the hypothesised findings concluded that advancing cyber security in Indonesia is a fundamental aspect of state sovereignty, as stated in the 1945 Constitution and the principle of the Unitary State of the Republic of Indonesia (NKRI). These findings demonstrated the significance of comprehending cyber security for users and organisations and the necessity of international cooperation in the realm of national security in cyber. By gaining a more comprehensive comprehension of the function of security management, it is anticipated that organisations can enhance security protocols and mitigate security vulnerabilities as they confront the challenges of the present digital age.*

Keywords: *Security Management, Cyber, 1945 Constitution, Digitalisation*

Abstrak.Dalam era digitalisasi yang berkembang pesat, keamanan *cyber* menjadi aspek yang krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan data organisasi. Kesadaran keamanan *cyber*, sebagai elemen kunci dalam upaya melindungi sistem dan informasi, menjadi fokus utama dalam penelitian ini. Undang-undang Dasar 1945 merupakan konstitusi dasar yang mengatur sistem pemerintahan dan hukum di Indonesia. Konstitusi UUD 1945 menetapkan hukum yang menjamin kebebasan ekspresi, yang juga relevan dalam keamanan *cyber*. Penelitian ini bertujuan untuk menginvestigasi peranan manajemen sekuriti dalam memperkuat keamanan *cyber* berdasarkan prinsip-prinsip yang bersumber dari Undang-Undang Dasar 1945. Penelitian ini ditulis berdasarkan tinjauan literatur menyeluruh dan menggali temuan-temuan terbaru dalam bidang ini, penelitian ini mengidentifikasi faktor-faktor yang memengaruhi kesadaran keamanan *cyber* dan bagaimana kesadaran tersebut dapat ditingkatkan di kalangan pengguna. Manajemen sekuriti memainkan peran kunci dalam memastikan keamanan sistem dan infrastruktur IT. Dengan memanfaatkan tinjauan literatur, penelitian ini menyajikan analisis tentang bagaimana manajemen sekuriti dapat membantu organisasi mengidentifikasi, mengelola, dan merespons ancaman keamanan secara efektif. Hasil hipotesa juga menyimpulkan bahwa pengembangan keamanan *cyber* di Indonesia merupakan bagian integral dari kedaulatan negara yang ditegaskan oleh Undang-Undang Dasar 1945 (UUD 1945) dan prinsip Negara Kesatuan Republik Indonesia (NKRI). Hal ini memperlihatkan pentingnya pemahaman tentang keamanan *cyber* bagi pengguna dan organisasi serta perlunya kerjasama internasional dalam konteks keamanan nasional di bidang *cyber*. Dengan pemahaman yang lebih baik tentang peran manajemen

Received April 30, 2024; Accepted Mei15, 2024; Published Mei 31, 2024
* Destya Fitri Andini , destyaandini23@gmail.com

sekuriti, diharapkan organisasi dapat meningkatkan tingkat keamanan dan mengurangi risiko keamanan dalam menghadapi tantangan era digitalisasi saat ini.

Kata Kunci: Manajemen Sekuriti, *Cyber*, UUD 1945, Digitalisasi

PENDAHULUAN

Era digitalisasi adalah periode yang sangat signifikan dalam perubahan masyarakat dan ekonomi secara global. Di era ini, akses terhadap informasi menjadi lebih cepat dan mudah melalui perangkat teknologi, menciptakan kebiasaan baru dalam berbagai aspek kehidupan sehari-hari. Perkembangan teknologi memiliki dampak yang luas terhadap kehidupan manusia, baik secara positif maupun negatif, termasuk dalam hal ekonomi, sosial, budaya, dan politik (Susanto, Antira, Kevin, Stanzah, & Majid, 2023). Dengan perkembangan yang telah membuat pemenuhan kebutuhan manusia menjadi lebih mudah dan menyenangkan, teknologi digital dari era industri 4.0 telah mengubah cara hidup secara signifikan. Proses digitalisasi informasi telah menghadirkan kemudahan dalam membangun jaringan yang membentuk sistem yang terintegrasi. Ini memfasilitasi berbagai keperluan seperti pengumpulan data, analisis data, evaluasi perkembangan bisnis, dan peningkatan kinerja, dengan produk mereka sendiri diintegrasikan ke dalam satu jaringan yang terhubung secara keseluruhan (Simorangkir, Legionosuko, & Waluyo, 2023). Pada era digital, kehidupan manusia diwarnai dengan berbagai kemudahan dalam memperoleh informasi dan setiap individu menjadi lebih mudah untuk tampil ke publik. Dampak digitalisasi telah menyebar secara meluas diseluruh dunia, tidak terkecuali Indonesia yang juga terkena dampaknya.

Keamanan *cyber* adalah salah satu aspek penting dalam konteks keamanan nasional. Dalam era digitalisasi, infrastruktur digital menjadi vital bagi fungsi negara, dan keamanannya sangat penting untuk mempertahankan stabilitas negara (Rosy, 2020). Pada era digital, data menjadi salah satu aset penting yang harus dijamin keamanan, dan keamanan *cyber* memiliki peran vital dalam mempertahankan data tersebut. Perkembangan zaman melibatkan penggunaan teknologi dalam berbagai aspek kehidupan sehari-hari, mulai dari komunikasi, transaksi *online*, belanja, pendidikan, ekonomi, layanan kesehatan, hingga kebutuhan lainnya, yang sekarang dapat dilakukan dengan mudah melalui internet. Transformasi signifikan terjadi ketika cara-cara konvensional beralih menjadi tergantung pada teknologi dalam segala hal. Dalam beberapa dekade terakhir, kemajuan teknologi informasi dan komunikasi telah memberikan dampak positif terhadap pertumbuhan ekonomi global serta memengaruhi produktivitas, persaingan, dan partisipasi masyarakat dengan lebih aktif (Vimy, Wiranto, Rudiyanto, Widodo, & Suwarno, 2022). Namun, semakin terhubungnya pemerintah,

pengusaha, dan masyarakat dalam dunia digital juga menimbulkan tantangan baru terkait dengan ancaman di dunia maya. Oleh karena itu, diperlukan perhatian lebih dalam pengembangan keamanan *cyber* yang lebih kuat untuk mengatasi tantangan tersebut. Infrastruktur digital memiliki peranan krusial dalam operasional negara, dan menjaga keamanannya sangatlah penting untuk memelihara stabilitas negara.

Undang-Undang Dasar 1945 (UUD 1945) menjadi sumber hukum penting dalam menangani keamanan *cyber* di Indonesia. Dalam konteks keamanan nasional, UUD 1945 memberikan kerangka hukum bagi manajemen keamanan *cyber* di Indonesia. Di era digitalisasi, data telah menjadi aset yang sangat berharga yang harus dilindungi, dan keamanan *cyber* memegang peranan kunci dalam menjaga keamanan data tersebut. Ancaman serangan *cyber* semakin meningkat, dan pelanggaran keamanan siber dapat mengakibatkan kerugian ekonomi, reputasi, serta kerugian bagi individu atau Perusahaan (Ramayanti & Lubis, 2023). Pelanggaran keamanan siber juga dapat berdampak negatif pada negara, yang berpotensi mengganggu stabilitas negara.

Saat ini, integrasi teknologi ke dalam kehidupan sehari-hari telah meningkat secara signifikan, menciptakan ancaman keamanan siber yang semakin canggih dan menimbulkan risiko besar bagi organisasi global. Meskipun ancaman keamanan siber terus meningkat, banyak organisasi masih kurang memberikan perhatian terhadap manajemen keamanan. Manajemen keamanan informasi mencakup serangkaian kebijakan, praktik, dan prosedur yang dirancang untuk melindungi organisasi dari ancaman keamanan, termasuk serangan dunia maya. Tujuannya adalah untuk melindungi informasi sensitif dan informasi penting dari akses tidak sah, modifikasi, atau penghapusan, serta menjaga keamanan sumber daya teknologi informasi dan komunikasi (TIK) yang digunakan dalam organisasi (Fachrudin, Respaty, Adilah, & Sinlae, 2024). Faktor-faktor yang berkontribusi terhadap kurangnya perhatian terhadap manajemen keamanan informasi termasuk kurangnya kesadaran akan risiko keamanan siber dan terbatasnya sumber daya untuk menerapkan strategi keamanan yang efektif. Perubahan pesat dalam teknologi dan lingkungan bisnis juga menghadirkan tantangan terhadap manajemen informasi keamanan dan mengharuskan organisasi untuk terus memperbarui strategi dan teknik mereka untuk menghadapi ancaman keamanan siber yang terus berkembang.

Dalam konteks ini, latar belakang masalah menyoroti pentingnya manajemen keamanan informasi yang efektif untuk melindungi data sensitif dan informasi penting dari serangan dunia maya atau siber, lalu Indonesia mampu membentuk suatu kebijakan atau

strategi yang dapat digunakan dalam menghadapi ancaman yang membahayakan keamanan nasional. Oleh karena itu, rumusan masalah yang akan dibahas meliputi:

1. Bagaimana peran manajemen sekuriti dalam menghadapi keamanan *cyber* di era digitalisasi?
2. Bagaimana UUD 1945 mempengaruhi kerangka kerja manajemen sekuriti dalam konteks keamana *cyber*?
3. Apa tantangan utama yang dihadapi oleh manajemen sekuriti dalam mencapai keamanan *cyber* dalam konteks keamanan nasional?

Tujuan

1. Mengidentifikasi peran manajemen sekuriti dalam menghadapi keamanan *cyber* di era digitalisasi.
2. Menganalisis bagaimana UUD 1945 mempengaruhi kerangka kerja manajemen sekuriti dalam konteks keamanan *cyber*.
3. Mengenal pasti tantangan utama yang dihadapi oleh manajemen sekuriti dalam mencapai keamanan *cyber* dalam konteks keamanan nasional.

METODE PENULISAN

Berbagai jenis penelitian dan penulisan yang dilakukan dan metode yang digunakan dalam penyusunan paper ini akan dibahas dalam bagian ini. Penulisan paper ini dilakukan dengan menggunakan metode deskriptif kualitatif, yaitu menggunakan studi pustaka atau *literature review*, dengan menggunakan berbagai jurnal dan web yang relevan dengan penulisan yang ditulis. Penulisan dengan metode deskriptif berupaya untuk memberikan pemecahan masalah yang sedang terjadi saat ini berdasarkan data-data, dengan menyajikan, menganalisis serta menginterpretasikannya (Mayola, Megasari, Dwiyanti, & Lutfiati, 2021). Karena penulis percaya bahwa teknik penulisan paper deskriptif kualitatif penting dalam konteks masalah yang sedang dibahas, konteks masalah yang sedang dibahas dapat dengan mudah dipahami, dan penjelasan diberikan tentang hasil menggunakan metode kualitatif atau pengambilan sudut pandang fenomenologis. Selain itu juga, penulisan dengan metode deskriptif kualitatif memiliki tujuan untuk memahami suatu kejadian yang disajikan secara deskripsi melalui kalimat dan bahasa, pada suatu konteks khusus yang alamiah (Mayola, Megasari, Dwiyanti, & Lutfiati, 2021).

(Semiawan, 2010) dalam buku yang berjudul "Metode Penelitian Kualitatif" Creswell menjelaskan bahwa pendekatan kualitatif dalam penelitian maupun penulisan karya ilmiah adalah untuk menjelaskan berbagai masalah sosial atau manusia dengan membangun

gambaran yang sangat kompleks yang disajikan melalui deskripsi tertulis dari peneliti tentang metode dan data yang mereka kumpulkan. Dengan kata lain, pendekatan kualitatif adalah yang mengambil sudut pandang kualitatif. Untuk memberikan tingkat penjelasan yang lebih dalam, ini menyarankan bahwa tujuan pendekatan kualitatif bukanlah untuk menggeneralisasi tentang populasi besar, tetapi untuk memperoleh informasi tambahan tentang entitas atau peristiwa tertentu.

Hasil penulisan yang menggunakan pendekatan kualitatif memberikan gambaran yang akurat tentang struktur, dinamika, dan posisi umum organisasi yang kuat.

Tabel 1. Hasil Penelitian yang Relevan Terdahulu

No	Penulis, Tahun dan Judul	Hasil Riset Terdahulu	Persamaan dengan artikel ini	Perbedaan dengan artikel ini
1	(Ardiyanti, 2016) (*CYBER-SECURITY* DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA)	Artikel tersebut membahas tentang pentingnya kerjasama dalam membangun pertahanan *cyber*, ancaman hacker yang lebih menakutkan dari teroris, tantangan keamanan *cyber* di Indonesia, penerapan *cyber security*, pengguna internet di Indonesia, serta langkah-langkah yang diambil oleh TNI dalam menghadapi ancaman *cyber*. Selain itu, hasil riset dari jurnal tersebut juga menyoroti kebijakan keamanan *cyber* yang telah dijalankan di Indonesia, prospek pengembangan keamanan *cyber* di negara tersebut, dan tantangan baru yang muncul dari perkembangan tersebut. Selain itu, artikel juga membahas tentang manajemen teknologi informasi dan pengorganisasian terkait dengan penggunaan sistem teknologi informasi.	Kedua artikel sama-sama membahas topik keamanan *cyber*, meskipun dengan fokus yang berbeda.	Artikel Sebelumnya berfokus pada tantangan dalam pengembangan keamanan *cyber* di Indonesia, sementara di artikel ini berfokus pada peran manajemen keamanan dalam meningkatkan efektivitas keamanan *cyber* berdasarkan nilai-nilai kebangsaan yang tercantum dalam UUD 1945 di era digitalisasi.
2	(Budi, Wira, & Infantono, 2021) (Strategi Penguatan *Cyber Security* Guna Mewujudkan Keamanan Nasional di Era Society 5.0)	Hasil riset dari jurnal tersebut membahas strategi penguatan keamanan *cyber* untuk mencapai keamanan nasional di era *Society* 5.0. Dalam konteks Indonesia, peningkatan serangan siber selama pandemi COVID-19 telah mempercepat tren keamanan *cyber*, seperti serangan phishing dan ransomware. Untuk mencapai keamanan nasional, diperlukan langkah-langkah seperti membangun kapasitas, membentuk undang-undang khusus tentang tindak pidana *cyber*, meningkatkan sumber daya manusia, dan meningkatkan kerjasama stakeholder domestik dan internasional di bidang keamanan *cyber*.	Kedua artikel memiliki fokus pada keamanan nasional dan mengakui pentingnya keamanan *cyber* dalam konteks tersebut.	Artikel sebelumnya menempatkan keamanan cyber dalam konteks Era *Society* 5.0 yang menekankan penggunaan teknologi untuk kesejahteraan manusia, sementara artikel ini lebih menyoroti nilai-nilai kebangsaan dan era digitalisasi dalam konteks keamanan nasional.
3	(Fachrudin, Respaty, Adilah, & Sinlae, 2024) (Peranan Penting Manajemen Sekuriti di Era Digitalisasi)	Penelitian ini menunjukkan bahwa manajemen sekuriti memiliki peranan penting dalam melindungi informasi dan teknologi yang digunakan oleh perusahaan atau organisasi dari ancaman keamanan di era digitalisasi, baik dari ancaman dunia maya maupun risiko keamanan yang mungkin terjadi. Dengan menerapkan manajemen keamanan terintegrasi, perusahaan atau organisasi dapat meminimalkan risiko keamanan dan melindungi informasi dan teknologinya yang sangat penting.	Kedua artikel mengatakan bahwa manajemen sekuriti merupakan seperangkat kebijakan, praktik, dan prosedur yang dirancang untuk melindungi organisasi dari ancaman keamanan, termasuk ancaman dunia maya.	Artikel sebelumnya membahas dengan spesifik tentang bagaimana manajemen sekuriti dapat membantu organisasi mengidentifikasi, mengelola, dan merespons ancaman keamanan secara efektif, sementara di artikel ini melindungi informasi sensitif dan data penting yang digunakan oleh perusahaan atau melindungi organisasi dari berbagai ancaman keamanan di era digital.
4	(Fauzi, et al., 2023) (Keamanan *Cyber* dan Peretasan Etis: Pentingnya Melindungi Data Pengguna)	Penelitian ini membahas pentingnya keamanan siber dan penggunaan teknik peretasan etis untuk melindungi data pengguna. *Cyber risk* adalah risiko operasional yang terjadi di dunia maya, dan *cyber security* memastikan perlindungan terhadap aset dan informasi organisasi. Berbagai standar keamanan siber juga	Meskipun fokusnya berbeda, kedua artikel memiliki relevansi dengan keamanan *cyber*. Artikel pertama membahas perlindungan data pengguna dari ancaman siber, sedangkan artikel kedua menyoroti peran manajemen	Artikel sebelumnya bertujuan untuk meningkatkan pemahaman tentang pentingnya keamanan *cyber* bagi pengguna dan organisasi, sementara artikel ini mungkin bertujuan untuk membahas kontribusi manajemen keamanan *cyber* terhadap keamanan nasional.

		dibahas dalam studi ini. Standar keamanan informasi seperti ISO/IEC 27032 dan ISO/IEC TR 27103 penting untuk melindungi privasi dan menghadapi serangan *cyber*. Studi sebelumnya menunjukkan kompleksitas ancaman siber di Indonesia dan pentingnya pendidikan keamanan siber bagi masyarakat. Organisasi perlu berinvestasi dalam kebijakan dan praktik keamanan siber yang etis untuk melindungi infrastruktur teknologi mereka.	keamanan *cyber* dalam meningkatkan keamanan nasional di era digitalisasi.	
5	(Kementerian Pertahanan, 2016) (PEDOMAN PERTAHANAN SIBER)	Panduan ini mungkin memuat hasil riset terkait dengan ancaman-ancaman *cyber* yang ada, baik yang bersifat umum maupun yang spesifik terhadap entitas yang menggunakan panduan tersebut. Lalu berisi strategi pertahanan *cyber* yang dihasilkan dari penelitian dan analisis terhadap kebutuhan keamanan siber entitas yang bersangkutan. Mungkin juga terdapat kebijakan keamanan *cyber* yang direkomendasikan berdasarkan hasil riset, yang mencakup aturan, prosedur, dan praktik terbaik yang harus diadopsi untuk melindungi sistem dan data dari serangan *cyber*.	Kedua artikel kemungkinan membahas tantangan dan peluang yang muncul dalam era digitalisasi, meskipun dari perspektif yang berbeda.	Artikel Sebelumnya berisi panduan praktis, strategi, dan langkah-langkah konkret untuk memperkuat pertahanan siber, sementara artikel ini mungkin lebih bersifat teoritis dan analitis, membahas peran manajemen keamanan *cyber* dari perspektif nilai-nilai kebangsaan.
6	(Mayola, Megasari, Dwiyanti, & Lutfiati, 2021) (STRATEGI PEMASARAN MARKETING MIX PRODUK BULU MATA PALSU ELLASHES.PRO)	Hasil riset ini menunjukkan bahwa Ellashes.pro merupakan sebuah merek produk bulu mata palsu yang sukses menjual produknya di pasaran, dan strategi pemasaran yang diterapkan oleh mereka membuat produk yang dijual diminati oleh banyak konsumen.	Kedua artikel ini sama-sama menggunakan metode penulisan dengan analisis data deskriptif melalui tahapan reduksi data, penyajian data, dan penarikan kesimpulan.	Artikel sebelumnya membahas terkait strategi pemasaran yang digunakan toko tersebut, sementara di artikel ini tidak membahas terkait hal itu.
7	(Napitupulu, 2017) (Kajian Peran *Cyber Law* Dalam Memperkuat Keamanan Sistem Informasi Nasional)	Hasil riset dari jurnal tersebut menyoroti pentingnya teori informasi, keamanan sistem informasi berbasis internet, *Cyber Law*, dan kebijakan keamanan sistem informasi dalam memperkuat keamanan sistem informasi nasional dan global. Artikel tersebut menekankan perlunya data yang lengkap, terkini, handal, dan terolah dengan baik untuk mendukung pengambilan keputusan manajerial. Selain itu, *Cyber Law* dianggap penting untuk melindungi masyarakat dari ancaman *cyber crime*, mengatur aktivitas *online*, dan memberikan sanksi pada aktivitas merugikan. Kerjasama global juga diperlukan dalam menyikapi kejahatan TI, serta pendekatan teknis, bisnis, dan sosial dalam mengatasi kejahatan *cyber*.	Keduanya mengakui pentingnya keamanan *cyber* dalam konteks keamanan nasional, meskipun dari sudut pandang yang berbeda.	Artikel sebelumnya membahas berbagai aspek perundang-undangan *cyber*, seperti perlindungan data, privasi, tindakan hukum terhadap pelanggaran keamanan siber, dan sebagainya, sementara artikel ini menyoroti peran manajemen keamanan *cyber* dari perspektif nilai-nilai kebangsaan dan efektivitas dalam konteks keamanan nasional.
8	(Putra, et al., 2023) (Pentingnya Manajemen *Security* di Era Digitalisasi)	Jurnal tersebut membahas tentang pentingnya manajemen keamanan informasi menggunakan standar ISO 27001 dalam melindungi informasi dan teknologi dari serangan *cyber*. Penelitian menunjukkan bahwa manajemen keamanan yang efektif dapat membantu meningkatkan efisiensi operasional, membangun kepercayaan pelanggan, serta melindungi perusahaan atau organisasi dari risiko keamanan yang mungkin terjadi. Organisasi kecil dan menengah juga rentan terhadap serangan *cyber*, sehingga perlu memperhatikan manajemen keamanan, investasi dalam teknologi keamanan, dan pendidikan untuk meningkatkan kesadaran keamanan.	Keduanya memiliki relevansi dengan era digitalisasi dan mengakui pentingnya manajemen keamanan dalam menghadapi tantangan keamanan yang berkaitan dengan perkembangan teknologi.	Artikel sebelumnya membahas strategi dan praktik terkait dengan manajemen keamanan secara umum, termasuk manajemen risiko, kebijakan keamanan, dan pengelolaan insiden keamanan, sedangkan artikel ini menyoroti manajemen keamanan *cyber* dan kontribusinya terhadap keamanan nasional.
9	(Rahmawati, 2019) (Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0)	Penelitian ini menyoroti peningkatan serangan *malware* dan peretasan yang ditargetkan terhadap infrastruktur kritis, organisasi pemerintah, bisnis, dan individu di Indonesia. Hal ini mungkin termasuk analisis tentang jenis-jenis malware yang umumnya	Kedua artikel mengakui pentingnya keamanan *cyber* di era digitalisasi dan menyoroti implikasi serta tantangan yang muncul	Artikel sebelumnya membahas berbagai jenis ancaman dan tantangan keamanan siber yang dihadapi oleh Indonesia, seperti serangan *malware*, peretasan, kebocoran data, dan lain-lain,

		ditemukan dan taktik yang digunakan oleh peretas. Lalu kekurangan dalam keamanan infrastruktur digital di Indonesia, termasuk pada tingkat perusahaan, pemerintah, dan individu. Ini mungkin mencakup evaluasi terhadap kelemahan yang ada dalam sistem dan jaringan, serta rekomendasi untuk memperbaiki kerentanan tersebut.	seiring dengan perkembangan teknologi informasi.	sedangkan artikel ini lebih fokus pada kontribusi manajemen keamanan *cyber* terhadap keamanan nasional dengan memperhatikan nilai-nilai kebangsaan.
10	(Ramayanti & Lubis, 2023) (Peran Hukum dalam Mengatasi Serangan *Cyber* yang Mengancam Keamanan Nasional)	Hasil riset ini menunjukkan bahwa hukum memiliki peran yang cukup besar dalam mengatasi serangan *cyber* yang mengancam keamanan nasional, dan peran hukum dalam mengatur dan mengatur ulang sistem keamanan, serta mengatur kebijakan, praktik, dan prosedur yang bertujuan untuk melindungi keamanan nasional.	Kedua artikel ini sama-sama membahas bahwa manajemen sekuriti memiliki peran yang cukup besar dalam melindungi keamanan nasional bersumber dari nilai-nilai kebangsaan UUD 1945.	Artikel sebelumnya memiliki tujuan untuk mengetahui peran hukum dalam mengatasi serangan *cyber* yang mengancam keamanan nasional, sementara artikel ini emiliki tujuan untuk mengetahui peranan manajemen sekuriti dalam melindungi keamanan nasional bersumber dari nilai-nilai kebangsaan UUD 1945.
11	(Rosy, 2020) (Kerjasama internasional Indonesia: memperkuat keamanan nasional di bidang keamanan siber)	Isi riset tersebut mengulas tentang kerjasama internasional Indonesia dalam memperkuat keamanan nasional di bidang keamanan siber. Riset ini menunjukkan bahwa Indonesia mengupayakan peningkatan keamanan siber dengan cara bekerjasama dengan negara lain, baik melalui kerjasama bilateral maupun regional.	Kedua artikel ini sama-sama membahas mengenai keamanan di bidang *cyber*.	Pada artikel ini tidak membahas kerjasama internasional dalam konteks keamanan nasional dalam bidang *cyber*.
12	(Semiawan, 2010) (Metode Penelitian Kulitatif)	Mencakup tentang metode penelitian kualitatif, yang merupakan cara untuk meneliti suatu masalah dengan lebih mendalam. Dalam buku ini, terdapat pengertian, tujuan, ciri, dan jenis-jenis metode penelitian kualitatif, seperti etnografi, studi kasus, studi dokumen, pengamatan atau observasi alami, dan fenomenologi.	Kedua artikel ini menggunakan metode yang sama yaitu menggunakan jenis penulisan studi literatur dalam penulisan nya.	Pada artikel sebelumnya menggambarkan tentang metode penelitian kualitatif, yang digunakan untuk menjelaskan dan menganalisis fenomena individu atau kelompok, sedangkan pada artikel ini menggambarkan tentang peran manajemen sekuriti dalam melindungi keamanan nasional bersumber dari nilai-nilai kebangsaan UUD 1945.
13	(Simorangkir, Legionosuko, & Waluyo, 2023) (*CYBER SECURITY* DALAM STUDI KEAMANAN NASIONAL: POLITIK, HUKUM DAN STRATEGI)	Riset ini menunjukkan bahwa *cyber security* merupakan aspek penting dalam studi keamanan nasional, yang membutuhkan peranan politik, hukum, dan strategi yang tepat untuk mengatur dan mengatur ulang sistem keamanan siber nasional. Peranan manajemen risiko dan kepatuhan, serta tenaga profesional yang berpengalaman dalam dunia keamanan dan siber, juga sangat penting dalam membangun sistem keamanan siber nasional yang efektif.	Keduanya menyoroti pentingnya manajemen sekuriti dalam menghadapi tantangan keamanan *cyber*.	Artikel sebelumnya lebih menyoroti aspek-aspek politik, hukum, dan strategi yang terkait dengan keamanan *cyber* dalam konteks nasional secara umum. Sedangkan artikel ini lebih terfokus pada peran manajemen sekuriti dan bagaimana prinsip-prinsip yang bersumber dari UUD 1945 dapat digunakan untuk meningkatkan keamanan *cyber* dalam konteks keamanan nasional.
14	(Susanto, Antira, Kevin, Stanzah, & Majid, 2023) (Manajemen Keamanan *Cyber* di Era Digital)	Riset ini menunjukkan bahwa manajemen keamanan *cyber* di era digital memiliki peranan penting dalam melindungi perangkat lunak, perangkat keras, dan data dari ancaman keamanan. Perkembangan teknologi memerlukan perubahan yang signifikan dalam strategi keamanan siber, dan peranan politik, hukum, dan strategi dalam membangun sistem keamanan siber nasional juga sangat penting.	Persamaan dari kedua artikel tersebut adalah keduanya membahas topik keamanan *cyber* dalam konteks era digital dan bagaimana manajemen sekuriti berperan dalam meningkatkan keamanan dalam ranah tersebut.	Pada artikel sebelumnya, memberikan gambaran umum tentang pentingnya, peran, tantangan, dan solusi manajemen sekuriti. Sementara pada artikel ini, memberikan perspektif yang lebih spesifik tentang peran nilai-nilai kebangsaan UUD 1945 dalam memperkuat manajemen sekuriti.
15	(Vimy, Wiranto, Rudiyanto, Widodo, & Suwarno, 2022) (ANCAMAN SERANGAN SIBER PADA KEAMANAN NASIONAL INDONESIA)	Mengulas tentang ancaman serangan siber yang mengancam keamanan nasional di Indonesia. Ancaman ini disebabkan oleh perubahan lingkungan yang dihadapi oleh seluruh negara pada sistem internasional, yang membuat isu keamanan menjadi semakin kompleks.	Kedua artikel menekankan pentingnya meningkatkan kesadaran dan edukasi tentang keamanan *cyber* serta saling melengkapi dalam memberikan pemahaman tentang ancaman serangan siber pada keamanan nasional Indonesia.	Pada artikel sebelumnya Tidak membahas secara detail tentang nilai-nilai kebangsaan UUD 1945. Sedangkan pada artikel ini Berfokus pada peran nilai-nilai kebangsaan UUD 1945 dalam memperkuat manajemen sekuriti untuk menangkal serangan *cyber*.

PEMBAHASAN

Peran Manajemen Sekuriti Dalam Menghadapi Keamanan *Cyber* di Era Digitalisasi

Konsep dasar manajemen sekuriti adalah mengidentifikasi, menganalisis, dan mengurangi risiko kekerasan *cyber* yang dapat mengakibatkan dampak negatif terhadap organisasi (Fauzi, et al., 2023). Peran manajemen sekuriti dalam menghadapi keamanan *cyber* di era digitalisasi adalah sangat penting karena kekerasan cyber semakin berkembang dan menjadi lebih kompleks. Perkembangan era digital telah mengubah banyak aspek kehidupan manusia, termasuk dalam hal keamanan *cyber*. Seiring dengan kemajuan teknologi informasi dan komunikasi yang pesat, muncul ancaman keamanan *cyber* yang semakin rumit dan maju. Menghadapi keamanan *cyber* di era digitalisasi merupakan masalah yang sangat penting dan menjadi tumpuan utama bagi manajemen sekuriti. Serangan *cyber* dapat memiliki konsekuensi negatif yang beragam, seperti pencurian data, penipuan keuangan, gangguan layanan, dan bahkan kerusakan pada infrastruktur (Putra, et al., 2023). Dampak ini dapat menyebabkan kerugian yang signifikan bagi individu, organisasi, dan bahkan negara. Oleh karena itu, diperlukan langkah-langkah untuk meningkatkan keamanan *cyber* di era digital ini. Salah satu cara kunci untuk mencapai hal ini adalah melalui penerapan manajemen keamanan yang efektif.

Perkembangan era digital membawa berbagai kesempatan dan tantangan yang kompleks. Meskipun digitalisasi membuka pintu akses informasi serta memudahkan berbagai aspek kehidupan, namun sebaliknya, meningkatkan risiko keamanan *cyber*. Ancaman serangan *cyber* dapat terjadi tanpa peringatan kepada siapa pun, kapan pun, dan berpotensi menimbulkan kerugian yang besar. Manajemen sekuriti memegang peran sentral dalam menghadapi tantangan keamanan *cyber* di era digital ini. Ini merupakan proses berkesinambungan yang bertujuan untuk mengelola risiko *cyber* serta melindungi kekayaan informasi yang dimiliki. Berdasarkan penelitian sebelumnya, Fachrudin, Respaty, Adilah, & Sinlae (2024) menyimpulkan bahwa manajemen sekuriti memegang peran vital dalam menjaga integritas informasi serta teknologi yang dimanfaatkan oleh perusahaan atau organisasi dari segala ancaman keamanan yang timbul di era digital. Baik itu dari ancaman *cyber* ataupun risiko keamanan yang mungkin terjadi. Dengan menerapkan pendekatan manajemen keamanan yang terpadu, perusahaan atau organisasi dapat mengurangi risiko keamanan secara signifikan dan menjaga keamanan serta integritas informasi serta teknologi yang menjadi aset utama mereka. Peran-peran penting manajemen sekuriti dalam menghadapi keamanan *cyber* di era digitalisasi sebagai berikut:

1. Melindungi aset informasi

Manajemen sekuriti membantu organisasi untuk melindungi aset informasi mereka dari berbagai ancaman *cyber*, seperti pencurian data, *malware*, dan *ransomware*. Hal ini dapat membantu organisasi untuk menghindari kerugian finansial, reputasi, dan operasional.

2. Mematuhi peraturan

Manajemen sekuriti dapat membantu organisasi untuk mematuhi peraturan tersebut dan menghindari denda dan sanksi.

3. Meningkatkan ketahanan nasional

Upaya untuk memperkuat pertahanan dan kesiapsiagaan sebuah negara terhadap ancaman *cyber* yang bisa membahayakan kepentingan nasional. Hal ini melibatkan penerapan strategi, kebijakan, dan praktik keamanan *cyber* yang efektif untuk melindungi infrastruktur kritis, data sensitif, dan sistem penting lainnya dari serangan *cyber*. Manajemen sekuriti dalam konteks ini bertanggung jawab untuk mengidentifikasi, menganalisis, dan merespons ancaman keamanan *cyber* dengan cara yang meminimalkan risiko serta memperkuat kemampuan negara dalam menghadapi tantangan tersebut. Upaya ini dapat melibatkan kerjasama antara pemerintah, sektor swasta, dan lembaga internasional untuk menciptakan lingkungan *cyber* yang aman dan andal bagi pertumbuhan dan keberlangsungan negara secara keseluruhan.

Peran Konstitusi UUD 1945 dalam Kerangka Kerja Manajemen Sekuriti terhadap Keamanan *Cyber*

Peran Konstitusi UUD 1945 dalam kerangka kerja manajemen sekuriti terhadap keamanan *cyber* adalah penting karena Konstitusi UUD 1945 menetapkan hukum yang menjamin hak asasi manusia, termasuk hak keamanan privasi, hak kebebasan informasi, dan hak kebebasan ekspresi (Ramayanti & Lubis, 2023). Hal ini membuat konstitusi UUD 1945 sangat penting dalam mengatur dan mengatur keamanan *cyber*, karena keamanan *cyber* tidak hanya merupakan masalah teknis, tetapi juga merupakan masalah hukum dan etika. Konstitusi UUD 1945 menegaskan hukum yang menjamin perlindungan hak privasi, yang merupakan unsur krusial dalam keamanan *cyber*. Hak privasi mencakup data pribadi, seperti nama, alamat, dan nomor telepon, yang harus dilindungi dari akses yang tidak sah. Selain itu, Konstitusi UUD 1945 juga menegaskan hukum yang menjamin kebebasan informasi, yang penting dalam konteks keamanan *cyber*. Hak ini mencakup informasi yang diperoleh melalui internet, yang harus dilindungi dari pengumpulan, pengolahan, dan penyebaran yang tidak sah.

Konstitusi UUD 1945 juga menetapkan hukum yang menjamin kebebasan ekspresi, yang juga relevan dalam keamanan *cyber*. Menurut Undang-Undang RI Nomor 3 Tahun 2002 tentang Pertahanan Negara, tujuan pertahanan negara adalah untuk menjaga dan melindungi

kedaulatan negara, integritas wilayah Negara Kesatuan Republik Indonesia (NKRI), dan keselamatan seluruh rakyat dari segala jenis ancaman, baik itu bersifat militer maupun non-militer (Kementerian Pertahanan, 2016). Ancaman non-militer, terutama dalam *cyber*. Hak ini mencakup informasi yang disampaikan kepada publik, yang harus dijaga dari pengumpulan, pengolahan, dan penyebaran yang tidak sah. Selain itu, Konstitusi UUD 1945 juga menjamin kebebasan ekonomi, yang mencakup aktivitas ekonomi seperti transaksi elektronik dan perdagangan, yang harus dilindungi dari ancaman keamanan *cyber*. Dalam manajemen sekuriti, Konstitusi UUD 1945 berperan sebagai landasan hukum yang menegaskan hak asasi manusia dan membantu dalam pengaturan dan pengelolaan keamanan *cyber* (Napitupulu, 2017). Konstitusi ini mendukung manajemen sekuriti dalam mengidentifikasi serta mengelola risiko keamanan *cyber*, membantu dalam pengambilan keputusan yang tepat terkait keamanan *cyber*, dan juga mendukung pengembangan kapabilitas organisasi untuk mengelola keamanan *cyber*. Selain UUD 1945, strategi kemanan *cyber* juga di atur dalam peraturan presiden (PERPRES) No. 47 Tahun 2023 mengatur mengenai Strategi Keamanan *cyber* Nasional dan Manajemen Krisis *cyber*. Strategi Keamanan *cyber* Nasional dan Manajemen Krisis Siber merupakan acuan bagi Instansi Penyelenggara Negara dan Pemangku Kepentingan untuk mewujudkan kekuatan dan kapabilitas siber dalam rangka mencapai stabilitas Keamanan *cyber*. Pendanaan penyelenggaraan Strategi Keamanan *cyber* Nasional dan Manajemen Krisis Siber bersumber dari APBN, APBD, dan sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

Tantangan Manajemen Sekuriti dalam Mewujudkan Keamanan *Cyber* untuk Keamanan Nasional

Indonesia saat ini menghadapi keadaan yang mendesak dalam hal keamanan *cyber* atau keamanan dunia maya. Hal ini disebabkan oleh kenyataan bahwa tingkat kejahatan di dunia maya atau *cyber crime* di Indonesia telah mencapai tingkat yang mengkhawatirkan. Namun, penanganan terhadap kejahatan *cyber* berbeda dengan penanganan kejahatan lainnya, karena memerlukan pendekatan yang komprehensif untuk mengatasi masalah tersebut (Ardiyanti, 2016). Perubahan Revolusi Industri 4.0 dalam teknologi industri dan peningkatan interkoneksi antara dunia bisnis dan kehidupan sehari-hari telah memicu transformasi bisnis dan meningkatkan kualitas hidup bagi karyawan dan pelanggan di berbagai belahan dunia (Rahmawati, 2019). Karena itu, pemerintah, sektor swasta, pelaku bisnis, dan masyarakat digital di Indonesia diharapkan akan menjadi pionir dalam menanggapi tantangan serta ancaman keamanan siber yang mungkin terjadi di masa depan. Kemajuan teknologi informasi telah mengubah pandangan tentang keamanan secara signifikan. Sekarang, interaksi tidak

lagi terbatas pada ruang fisik tetapi juga meluas ke dunia maya. Oleh karena itu, negara perlu menyesuaikan diri dengan perkembangan ini. Keamanan dalam dunia maya harus dianggap sebagai area yang perlu dilindungi oleh negara, sebagaimana negara menjaga keamanan wilayah fisiknya.

Periode digitalisasi telah mengakibatkan transformasi yang signifikan dalam berbagai bidang kehidupan, termasuk dalam hal keamanan. Keamanan *cyber* telah menjadi perhatian utama yang tidak dapat diabaikan, terutama dalam konteks keamanan nasional (Budi, Wira, & Infantono, 2021). Manajemen sekuriti memiliki peran sentral dalam memastikan keamanan *cyber*. Namun, dalam pelaksanaannya, ada beragam tantangan yang harus dihadapi seperti dalam mewujudkan keamanan *cyber* untuk keamanan nasional meliputi penguatan kelembagaan *cyber security*, ketidakadaan dasar hukum yang kuat untuk keamanan *cyber*, dan kurangnya tenaga professional serta kerjasama di dalam negeri maupun dengan dunia internasional. Pemerintah harus mempersiapkan orang-orang yang dibutuhkan di dunia yang semakin digital dan disahkan UU Keamanan Siber secepat mungkin untuk memulai upaya keamanan nasional Indonesia terhadap peningkatan serangan siber di era *society* 5.0. Namun, disamping itu kebijakan terkait pertahanan *cyber* telah mulai dirumuskan dan akan diimplementasikan pada fase selanjutnya. Kebijakan tersebut merupakan tambahan dari kebijakan yang sudah ada, yang umumnya terfokus pada pengembangan dan penggunaan teknologi informasi di lingkungan Kementerian secara keseluruhan. Salah satu dasar kebijakan yang ada adalah Peraturan Menhan Nomor 16/2010 tentang Organisasi dan Tata Kerja Kemhan, yang menjelaskan peran Pusat Data dan Informasi (Pusdatin) Kemhan dan unit-unit Data dan Informasi (Datin) di satuan kerja Kemhan (Kementerian Pertahanan, 2016). Selain itu, kebijakan yang mendukung pertahanan *cybe*r juga telah disusun. Kebijakan ini akan menjadi pedoman untuk persiapan, pengembangan, pelatihan, dan operasionalisasi pertahanan *cyber* di masa mendatang.

Hasil Analisis Hipotesa

Hipotesa		
Variabel X	**Variabel Y**	**Analisa**
X1 → Pengembangan keamanan *cyber* di Indonesia	**Y1 → UUD 1945**	**X1 → Y1** Berhubungan karena menegaskan kedaulatan Indonesia atas segala aspek kehidupan nasional, termasuk dalam domain cyber. Pengembangan keamanan cyber menjadi penting untuk melindungi kedaulatan negara dari ancaman di dunia maya seperti serangan cyber dari negara lain atau entitas asing.
X2 → Pemahaman tentang pentingnya keamanan *cyber* bagi pengguna dan organisasi	**Y1 → UUD 1945**	**X2 → Y1** Berhubungan untuk memberikan dasar hukum serta mendorong perlindungan keamanan cyber sebagai bagian dari tanggung jawab negara dalam melindungi warga dari ancaman.
X3 → Kerjasama internasional dalam konteks keamanan nasional dalam bidang *cyber*.	**Y1 → UUD 1945**	**X3 → Y1** Kerjasama internasional dalam bidang keamanan cyber dapat dilihat sebagai implementasi dari prinsip-prinsip hubungan internasional yang diakui oleh UUD 1945, seperti perdamaian, keadilan, dan kerjasama antarbangsa. Hal ini memperkuat pertahanan negara terhadap ancaman cyber yang melintasi batas-batas negara, sesuai dengan semangat kerjasama global yang dianjurkan oleh konstitusi Indonesia.

X4 → Ancaman dan tantangan keamanan *cyber* yang dihadapi oleh Indonesia	**Y1 → UUD 1945**	**X4 → Y1** Berhubungan dengan keamanan *cyber* yang merupakan bagian integral dari keamanan nasional dan kedaulatan negara. Selain itu, UUD 1945 mengandung semangat untuk mencapai kemandirian nasional dalam berbagai aspek kehidupan, termasuk dalam teknologi. Ancaman dan tantangan keamanan cyber menyoroti pentingnya Indonesia untuk menjadi mandiri dalam bidang keamanan cyber, termasuk pengembangan teknologi keamanan dan kebijakan yang sesuai dengan kebutuhan nasional.

KESIMPULAN

Menyimpulkan bahwa perlindungan keamanan cyber telah menjadi prioritas utama bagi Indonesia dalam menegaskan kedaulatan nasionalnya di era digital saat ini. Perlindungan ini diperlukan untuk melawan ancaman di dunia maya, termasuk serangan cyber dari negara lain atau entitas asing, serta sebagai tanggung jawab negara dalam melindungi warganya. Kerjasama internasional dalam bidang keamanan cyber dianggap sebagai sarana untuk memperkuat pertahanan negara terhadap ancaman lintas batas. Hal ini terintegrasi dengan keamanan nasional dan kemandirian negara dalam teknologi. Namun, tantangan yang dihadapi dalam mencapai keamanan cyber untuk kepentingan nasional meliputi perlunya penguatan kelembagaan keamanan cyber, dasar hukum yang kokoh, peningkatan jumlah tenaga ahli, dan kerjasama baik di dalam negeri maupun internasional. Oleh karena itu, pemerintah perlu mengambil langkah-langkah yang tepat untuk mempersiapkan sumber daya yang diperlukan dan merumuskan kebijakan yang efektif untuk mengatasi tantangan keamanan cyber di masa mendatang.

DAFTAR PUSTAKA

Ardiyanti, H. (2016). CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA. Jurnal DPR RI.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia .

Fachrudin, R., Respaty, E., Adilah, I. S., & Sinlae, F. (2024). Peranan Penting Manajemen Sekuriti di Era Digitalisasi. Nusantara Journal of Multidisciplinary Science, 95.

Fauzi, A., Akbar, R., Rizkha, A., Putri, S. T., Fadhilah, I., Iskandar, N. P., & Agung, G. N. (2023). Keamanan Cyber dan Peretasan Etis: Pentingnya Melindungi Data Pengguna. Jurnal Ilmu Multidisiplin.

Kementerian Pertahanan. (2016). PEDOMAN PERTAHANAN SIBER. kemenhan.

Mayola, C. A., Megasari, D. S., Dwiyanti, S., & Lutfiati, D. (2021). STRATEGI PEMASARAN MARKETING MIX PRODUK BULU MATA PALSU ELLASHES.PRO. e-journal UNESA.

Napitupulu, D. (2017). Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional. Universitas Budi Luhur.

Putra, R. G., Fauzi, A., Prasetyo, E. T., Pratama, S. R., Ramadhan, I. D., Febriyanti, & Nurlela, S. (2023). Pentingnya Manajemen Security di Era Digitalisasi. Jurnal Ilmu Multidisiplin.

Rahmawati, C. (2019). Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0. Seminar Nasional Sains Teknologi dan Inovasi Indonesia.

Ramayanti, H., & Lubis, A. F. (2023). Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam Keamanan Nasional. Jurnal Hukum dan HAM .

Rosy, A. F. (2020). Kerjasama internasional Indonesia: memperkuat keamanan nasional di bidang keamanan siber. Jurnal Ilmu Pemerintahan.

Semiawan, C. (2010). Metode Penelitian Kulitatif. GRASINDO.

Simorangkir, B., Legionosuko, T., & Waluyo, S. D. (2023). CYBER SECURITY DALAM STUDI KEAMANAN NASIONAL: POLITIK, HUKUM DAN STRATEGI. Media Bina Ilmiah.

Susanto, E., Antira, L., Kevin, Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber di Era Digital. Jurnal Bisnis dan Kewirausahaan.

Vimy, T., Wiranto, S., Rudiyanto, Widodo, P., & Suwarno, P. (2022). ANCAMAN SERANGAN SIBER PADA KEAMANAN NASIONAL INDONESIA. Jurnal Kewarganegaraan.