MENAWAN: Jurnal Riset Dan Publikasi Ilmu Ekonomi
Vol. 2, No. 3 Mei 2024
e-ISSN: 3025-4728, p-ISSN: 3025-5899, Hal 307-324
DOI: https://doi.org/10.61132/menawan.v2i3.552

Implementasi Nilai-Nilai Kebangsaan Bersumber UUD 1945 dan NKRI Guna Membangun Pertahanan Digital yang Kuat: Pentingnya Manajemen Sekuriti dalam Menghadapi Cybercrime

Dhini Dwi Aprilia
Universitas Bhayangkara Jakarta Raya
202210325207@mhs.ubharajaya.ac.id

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

Diah Sekar Arum
Universitas Bhayangkara Jakarta Raya
202210325190@mhs.ubharajaya.ac.id

Alamat: Jl. Harsono RM No.67 Ragunan Pasar Minggu, Jakarta Selatan
Korespondensi penulis: 202210325207@mhs.ubharajaya.ac.id

Abstract

In an era of rapid digital transformation, Indonesia faces major challenges in ensuring security, privacy and compliance are maintained. With increasing cyber threats in the country, BSSN and the Government must be more careful about potential large-scale security breaches and must prioritize building strong defense mechanisms to protect Indonesia's digital assets. Therefore, Cyber Security is the main pillar for the progress and sustainability of Indonesia's digital transformation. Then, legal provisions were issued in the form of Criminal Code Legislation and ITE Law no. 11 of 2008. The research method used in writing this article uses a qualitative method with a literature study approach. This research aims to provide an explanation regarding the compilation of national values originating from the 1945 Indonesian Constitution (UUD 1945) and the Unitary State of the Republic of Indonesia (NKRI) regarding security management. Specifically, this research examines the role of security management in dealing with cybercrime and strengthening digital defenses. It is hoped that the results of this research can be used as a reference for further research in increasing readers' insight and knowledge regarding the theme of this article.

Keywords: *Security Management, Cybercrime, Cyber Security, Digital Defense, 1945 Constitution, Republic of Indonesia*

Abstrak

Di era transformasi digital yang pesat, Indonesia menghadapi tantangan besar dalam memastikan keamanan, privasi, dan ketaatan yang terjaga. Dengan meningkatnya ancaman siber di negara ini, BSSN dan Pemerintah harus lebih berhati-hati terhadap potensi pelanggaran keamanan berskala besar dan harus memprioritaskan dalam membangun mekanisme pertahanan yang kuat untuk melindungi aset digital Indonesia. Oleh karena itu, Cyber Security menjadi pilar utama bagi kemajuan dan keberlanjutan transformasi digital Indonesia. Kemudian, dikeluarkannya ketentuan hukum berupa Peraturan Perundang-undangan KUHP dan UU ITE No. 11 Tahun 2008. Metode penelitian yang diambil dalam penulisan artikel ini menggunakan metode kualitatif dengan pendekatan studi literatur. Penelitian ini bertujuan untuk memberikan penjelasan mengenai kompilasi nilai-nilai kebangsaan yang bersumber dari Konstitusi Indonesia tahun 1945 (UUD 1945) dan Negara Kesatuan Republik Indonesia (NKRI) terhadap manajemen sekuriti. Secara khusus, penelitian ini mengusut bagaimana peran manajemen sekuriti dalam menghadapi kejahatan siber dan memperkuat pertahanan digital. Hasil dari penelitian ini diharapkan dapat digunakan sebagai acuan pada penelitian selanjutnya dalam meningkatkan wawasan serta pengetahuan para pembaca terkait tema artikel ini.

Received April 30, 2024; Accepted Mei 16, 2024; Published Mei 31, 2024
* Suhartini, *202210325151@mhs.ubharajaya.ac.id*

Kata kunci: Manajemen Sekuriti, Cybercrime, Cyber Security, Pertahanan Digital, UUD 1945, NKRI

LATAR BELAKANG

Perkembangan terkini di Indonesia menandakan perubahan besar dalam pertahanan digital. Seiring berkembangnya teknologi informasi dan komunikasi (TIK), tantangan dalam bidang keamanan digital menjadi semakin kompleks. Kemajuan teknologi informasi dan komunikasi membuat negara semakin rentan terhadap berbagai serangan kejahatan siber. Fenomena ini terjadi seiring dengan pesatnya perkembangan internet di masyarakat, pemerintahan, dan bisnis. Indonesia sedang mengalami perubahan pesat dalam infrastruktur teknologinya, sehingga memerlukan sistem pertahanan digital yang kuat untuk melindungi aset, data, dan infrastruktur penting dari ancaman dunia siber.

Seiring dengan meningkatnya kompleksitas ancaman dan serangan digital, penerapan manajemen sekuriti saat menangani kejahatan dunia siber menjadi semakin penting. Salah satu langkah terpenting saat menerapkan manajemen sekuriti adalah pemahaman mendalam tentang ancaman (siber). Manajemen sekuriti berperan penting dalam mengelola dan melindungi informasi pengguna yang tersimpan dalam sistem agar tetap aman dan tidak disalahgunakan (Ningrum et al., 2023). Tujuan utama dari cyber security ini yakni meminimalisir risiko-risiko dan memastikan tiga prinsip utama keamanan CIA triad (Confidentially, Integrity, Availability) tetap terlindungi sebagaimana teknologi dapat diamankan secara efektif.

Di era digital, hampir seluruh aspek kehidupan bergantung pada teknologi, termasuk data dan informasi. Seiring dengan semakin canggihnya teknologi, potensi ancaman di dunia digital pun semakin meningkat. Oleh karena itu, penting untuk membangun pertahanan digital untuk melindungi diri, organisasi, bahkan suatu negara dari berbagai risiko dan bahaya.

Untuk mengatasi ancaman siber, pemerintah Indonesia telah mengeluarkan berbagai undang-undang dan peraturan yang bertujuan untuk melindungi keamanan digital negara dan warganya. Ketentuan hukum tersebut berlandaskan undang-undang yang mencakup Peraturan Perundang-undangan Kitab Undang-undang Hukum Pidana (KUHP), UU Informasi dan Transaksi Elektronik (ITE) No. 11 Tahun 2008, UU No.3 Tahun 2002 tentang Pertahanan Negara, UU PDP hingga Perpres No. 47 tahun 2023.

Seluruh undang-undang tersebut menjamin keamanan dalam melindungi data pribadi warga negara.

Dalam membangun pertahanan digital yang kuat dan tangguh, selain diterapkannya manajemen sekuriti perlu dipadukan dengan implementasi dari nilai-nilai kebangsaan. Sebagai negara yang berlandaskan 4 konsensus dasar negara (Pancasila, UUD 1945, Bhinneka Tunggal Ika, dan NKRI), UUD 1945 dan NKRI memiliki peranan yang sangat penting dalam mengaplikasikan pertahanan digital Indonesia. Nilai-nilai kebangsaan mencakup gotong-royong, persatuan, serta semangat keadilan diharapkan mampu melindungi diri dan negara dari berbagai risiko bahaya di dunia digital agar mampu menikmati manfaat teknologi dengan aman dan nyaman.

Dengan itu, penelitian ini yang berjudul "Implementasi Nilai-Nilai Kebangsaan Bersumber UUD 1945 dan NKRI Guna Membangun Pertahanan Digital Yang Kuat: Pentingnya Manajemen Sekuriti dalam Menghadapi Cybercrime" dilatar belakangi untuk menggali lebih dalam bagaimana nilai-nilai kebangsaan dan manajemen sekuriti dalam membangun pertahanan digital yang kuat di Indonesia untuk menghadapi berbagai tantangan cybercrime**.**

METODE PENELITIAN

Metode penelitian yang diterapkan dalam penulisan artikel ini didasarkan pada pendekatan penelitian kepustakaan. Pendekatan ini melibatkan penyelidikan dan analisis terhadap data yang sudah ada termasuk karya-karya maupun literatur yang relevan. Dengan pendekatan ini, memungkinkan peneliti mengumpulkan, mengevaluasi, dan mensintesis informasi dari berbagai sumber, seperti artikel, buku, tesis, dan sumber lainnya.

Dalam konteks penulisan artikel ini, studi literatur akan mencakup tinjauan mengenai implementasi nilai-nilai kebangsaan bersumber UUD 1945 dan NKRI dalam membangun pertahanan digital yang kuat, dengan fokus pada pentingnya manajemen sekuriti untuk menghadapi ancaman cybercrime.

Tabel 1. Penelitian Terdahulu

No	Author (Tahun)	Judul	Hasil Penelitian Terdahulu	Persamaan dengan artikel ini	Perbedaan dengan artikel ini
1	(Sudarmadi & Runturambi, 2019)	Strategi Badan Siber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber di Indonesia	Hasil penelitian ini yaitu upaya penanganan dan pencegahan terhadap risiko keamanan siber di Indonesia dan strategi yang diterapkan oleh BSSN	Membahas mengenai pentingnya manajemen sekuriti menghadapi ancaman siber	Terdapat perbedaan pada fokus penelitian yaitu taktik yang diterapkan BSSN untuk menangani risiko keamanan siber di Indonesia
2	(Irawati et al., 2021)	Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital	Hasil penelitian ini yaitu membahas perlindungan dan keamanan masyarakat dari berbagai tindak kejahatan siber diikuti dengan peran regulasi dan implementasi hukum	Membahas mengenai pentingnya hukum siber guna melindungi masyarakat dari ancaman siber	Terdapat perbedaan pada fokus penelitian yaitu lebih spesifik dalam membahas urgensi dari hukum siber di Indonesia
3	(Haris, 2021)	Implementasi Nilai-Nilai Kebangsaan yang Bersumber dari Negara Kesatuan Republik Indonesia (NKRI)	Hasil penelitian ini yaitu membahas mengenai pentingnya kemandirian Indonesia dan nilai-nilai kebangsaan guna memperkuat identitas nasional	Membahas mengenai implementasi nilai-nilai kebangsaan yang berasal dari nkri	Terdapat perbedaan pada fokus penelitian yaitu hanya menjelaskan implementasi nilai NKRI
4	(Indah & Sidabutar, 2022)	Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)	Hasil penelitian ini yaitu pemberlakuan BSSN memiliki pengaruh terhadap keamanan data penduduk negara	Membahas mengenai peran keamanan siber terhadap ancaman cybercrime	Terdapat perbedaan pada fokus penelitian yaitu kasus yang diambil berbeda yakni Keamanan Data Penduduk Indonesia dengan menggunakan studi kasus Hacker Bjorka
5	(Mahendra & Pinatih, 2023)	Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia	Hasil penelitian ini yaitu strategi keamanan siber yang belum optimal serta lembaga BSSN yang masih kurang respon terhadap tantangan dunia siber	Membahas mengenai isu keamanan digital dan pertahanan negara, pentingnya manajemen sekuriti terhadap risiko keamanan siber	Terdapat perbedaan pada fokus penelitian yaitu pada strategi konkret terhadap risiko keamanan siber di Indonesia

6	(Syafi'i et al., 2023)	Kajian Ilmu Pertahanan dalam Strategi Pertahanan Negara Guna Menghadapi Ancaman Teknologi Digital di Indonesia	Hasil penelitian ini yaitu membahas tentang taktik Indonesia dalam mengatasi tantangan yang ditimbulkan oleh ancaman digital terhadap pertahanan dan keamanan nasional	Membahas mengenai pentingnya nilai kebangsaan dalam konteks pertahanan	Terdapat perbedaan pada fokus penelitian yaitu menjelaskan strategi pertahanan negara secara umum dan menghadapi ancaman cybercrime
7	(Soesanto, Masyruroh, et al., 2023)	Peranan Manajemen Sekuriti Dalam Mengamankan Dan Memecahkan Masalah PT SK Keris Indonesia	Hasil penelitian ini menunjukkan bahwa Unit Sekuriti di PT SK Keris belum memaksimalkan kerjasama dan koordinasi dengan seluruh entitas keamanan termasuk polisi setempat	Membahas mengenai pentingnya manajemen sekuriti dalam melindungi aset dan mencegah cybercrime	Terdapat perbedaan pada fokus penelitian yaitu peran manajemen sekuriti dalam memastikan keamanan dan menangani isu-isu di PT. SK Keris Indonesia secara efektif
8	(Yunita et al., 2023)	Penerapan Nilai Nilai Bela Negara Dalam Menghadapi Tantangan Era Digital	Hasil penelitian ini menekankan pada pentingnya memahami nilai-nilai patriotisme di kalangan anak muda dalam menghadapi era digital	Membahas mengenai implementasi nilai kebangsaan dalam menghadapi tantangan digital	Terdapat perbedaan pada fokus penelitian yaitu lebih menjelaskan pada penerapan nilai bela negara di era digital
9	(Soesanto, Saputra, et al., 2023)	Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File dan Pengamanan Cyber pada Yayasan Siber Publisher	Hasil penelitian ini yaitu membangun pemahaman mengenai manajemen sekuriti dan memberikan wawasan dalam mengamankan informasi dan sistem di lingkungan yayasan	Membahas mengenai pentingnya manajemen sekuriti dalam menghadapi ancaman siber	Terdapat perbedaan pada objek atau fokus penelitian yaitu dalam menganalisis objek-objek penting, keamanan data, dan keamanan siber di Yayasan Siber Publisher
10	(Kehista et al., 2023)	Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review)	Hasil penelitian ini yaitu bahaya, potensi kerugian, dan taktik keamanan memiliki pengaruh terhadap perlindungan informasi sensitif pelanggan dalam perdagangan elektronik	Membahas mengenai ancaman terhadap keamanan cyber security	Terdapat perbedaan pada fokus penelitian yaitu perlindungan informasi sensitif pelanggan dalam perdagangan elektronik dan variabel

					penelitian yang digunakan
11	(Sufi et al., 2023)	Analisis Ancaman Cybercrime dan Peran Sistem Biometrik: Systematic Literature Review	Hasil penelitian ini yaitu mengidentifikasi ancaman cybercrime yang ada serta peran sistem biometrik dalam menghadapi ancaman cybercrime	Membahas mengenai isu keamanan digital dan ancaman cybercrime	Terdapat perbedaan pada fokus penelitian yaitu menggali peran sistem biometrik sebagai solusi dalam menghadapi ancaman cybercrime
12	(Soesanto, Utami, et al., 2023)	Keamanan Data Pribadi Dalam Sistem Pembayaran Via OVO Terhadap Ancaman dan Pengetahuan (Cybercrime)	Hasil penelitian ini yaitu pembayaran via OVO dapat memungkinkan mengancam kebocoran data hingga terjadinya ancaman dari cybercrime	Membahas mengenai keamanan data pribadi terhadap ancaman cybercrime	Terdapat perbedaan pada fokus penelitian yaitu menekankan pada keamanan data pribadi dalam sistem pembayaran
13	(Gojali, 2023)	Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective	Hasil penelitian ini yaitu membahas populasi kejahatan siber di perusahaan Indonesia dari perspektif legislasi korporasi	Membahas mengenai pentingnya nilai-nilai kebangsaan hingga pada penerepannya dalam menghadapi tantangan ancaman cybercrime	Terdapat perbedaan pada fokus penelitian yaitu menekankan pada kejahatan siber yang ada di perusahaan
14	(Fachrudin et al., 2024)	Peranan Penting Manajemen Sekuriti di Era Digitalisasi	Hasil penelitian ini yaitu membahas peran kritis manajemen sekuriti dalam menghadapi tantangan era digital	Membahas mengenai pentingnya manajemen sekuriti dalam menghadapi ancaman digital	Terdapat perbedaan pada fokus penelitian yaitu menjelaskan pentingnya manajemen sekuriti dalam konteks digitalisasi
15	(Saputra et al., 2024)	Penerapan Manajemen Security terhadap Cybercrime di Kominfo	Hasil penelitian ini yaitu kebijakan perlindungan siber, pengawasan dan identifikasi kejahatan siber, pengelolaan akses masuk, edukasi dan instruksi keamanan, serta skema tanggap darurat keamanan perlu	Membahas mengenai isu pertahanan dan keamanan	Terdapat perbedaan pada fokus atau objek penelitian yaitu lebih spesifik menjelaskan manajemen sekuriti dalam menghadapi cybercrime di Kominfo

			disempurnakan memiliki pengaruh terhadap penerapan manajemen keamanan yang efektif di Kominfo		

HASIL DAN PEMBAHASAN

Dalam membangun digital yang kuat tidak hanya dibutuhkan infrastruktur dan teknologi yang canggih, tetapi juga dengan implementasi nilai-nilai kebangsaan bersumber UUD 1945 dan NKRI yang kuat. Dengan menggabungkan keduanya, bangsa Indonesia dapat membangun masa depan digital yang gemilang. Berikut terdapat beberapa poin yang terkandung dari kedua nilai tersebut yaitu gotong royong, persatuan dan kesatuan, semangat keadilan, dan kedaulatan rakyat (demokrasi). Dalam konteks nilai-nilai kebangsaan, gotong royong ini menekankan pada kolaborasi antara pemerintah, lembaga swasta serta seluruh masyarakat sipil dalam melindungi infrastruktur digital negara dan membangun pertahanan digital Indonesia yang tangguh. Hal itu dapat dilakukan dengan meningkatkan pengetahuan, pemahaman serta kesadaran masyarakat terhadap teknologi, dan juga bahu membahu dalam melaporkan insiden terhadap ancaman siber dan meresponnya secara cepat. Kemudian, dalam konteks nilai kebangsaan persatuan dan kesatuan menerapkan prinsip-prinsip yang mengedepankan kerjasama serta solidaritas dalam satu lingkup kelompok yaitu sektor publik dan swasta agar siap menghadapi tantangan bersama dan memperkuat fondasi negara.

Selanjutnya, pada konteks nilai kebangsaan semangat keadilan merupakan semangat yang mendorong individu hingga masyarakat agar selalu bertindak secara adil dan setara tanpa adanya kejomplangan pada strata kehidupan. Hal ini dapat dari penekanan pada akses yang adil terhadap teknologi pertahanan digital dan distribusi sumber daya yang merata untuk seluruh lapisan masyarakat serta memastikan bahwa seluruh masyarakat memiliki kesempatan yang sama untuk melindungi diri dari ancaman siber. Dan yang terakhir yaitu kedaulatan rakyat dalam konteks nilai kebangsaan melibatkan masyarakat dalam pengambilan keputusan terkait kebijakan dan regulasi siber. Hal itu dapat dilihat pada suara masyarakat harus dipertimbangkan dan pemerintah harus transparan dan bertanggung jawab atas pengelolaan kebijakan dan regulasi. Jadi

dengan demokrasi yang kuat, maka dapat dipastikan bahwa kebijakan siber dapat mendukung keamanan dan privasi.

Dapat disimpulkan bahwa prinsip-prinsip kebangsaan adalah dasar yang penting untuk menciptakan infrastruktur pertahanan digital yang tangguh dan efisien. Oleh karena itu, nilai kebangsaan bersumber UUD 1945 dan NKRI merupakan pilar utama dalam membangun pertahanan digital yang sesuai dengan identitas nasional, melindungi seluruh masyarakat sipil, serta meningkatkan memperkuat ketahanan nasional. Selain itu, dengan mengintegrasikan nilai-nilai dalam konteks pertahanan digital dapat dipastikan bahwa teknologi dapat diterapkan secara yang etis dan bertanggung jawab, sesuai dengan prinsip-prinsip kebangsaan.

Di era transformasi digital ini, kejahatan cyber menjadi salah satu risiko ancaman yang semakin nyata dan kompleks. Serangan cybercrime ini dapat mengakibatkan banyak kerugian termasuk dalam hal finansial, pencurian informasi data pribadi serta terganggunya infrastruktur pertahanan. Oleh sebab itu, diperlukannya peran penting manajemen sekuriti dalam membangun pertahanan digital yang kuat dan tangguh. Manajemen sekuriti berperan secara aktif dalam melibatkan proses mengidentifikasi, mengevaluasi, dan mengurangi risiko terkait infomasi serta mengintegrasikan strategi yang tepat seperti pembuatan kebijakan dan prosedur keamanan, penerapan teknologi keamanan menggunakan firewall, enskripsi dan antivirus, hingga pada meningkatkan kesadaran terhadap risiko guna melindungi aset digital dari serangan cybercrime yang semakin merajalela. Tingkat keberhasilan manajemen sekuriti diperkuat oleh dengan adanya regulasi dari pemerintah yang mendukung seluruh upaya dalam melindungi data dan sistem informasi. Berikut terdapat beberapa peraturan yang dikeluarkan oleh pemerintah Indonesia:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE): Undang-undang ini menetapkan ketentuan hukum yang berkaitan dengan teknologi informasi dan transaksi elektronik, termasuk cybercrime. Tetapi, UU ITE No 11 Tahun 2008 ini diubah menjadi Undang-Undang Nomor 19 Tahun 2016. Dimana UU No 19 Tahun 2016 ini merinci regulasi yang berkaitan dengan teknologi informasi dan transaksi elektronik, termasuk aspek-aspek seperti tindak pidana, penggeledahan dan penyegelan, serta perlindungan pribadi. Dengan adanya perubahan yang dilakukan, diharapkan Undang-Undang Nomor 19 Tahun 2016 dapat

berperan dalam memastikan keadilan, ketertiban umum, dan kepastian hukum bagi warga negara dalam dunia digital.

2. Peraturan Presiden (PERPRES) Nomor 47 Tahun 2023:

   Peraturan Presiden ini menetapkan kerangka kerja untuk strategi keamanan siber nasional, penanganan situasi darurat siber, dan menjaga kedaulatan negara. Diharapkan, dengan peraturan ini dapat dijadikan panduan oleh lembaga pemerintah dan para pemangku kepentingan dalam mengembangkan kekuatan dan kemampuan pertahanan siber, yang bertujuan untuk memastikan stabilitas keamanan siber dan mengatasi berbagai rintangan dalam era digital.

3. Undang-Undang Nomor 3 Tahun 2022 tentang Pertahanan Negara:

   Undang-undang ini mengatur tentang aspek-aspek pertahanan negara yang mencakup hakikat, penyelenggaraan, serta pengawasan dan pembiayaan. Dengan diberlakukannya UU ini, diharapkan Indonesia memiliki kerangka hukum yang dapat mengatur pertahanan negara dan memastikan seluruh warga negara dapat berpartisipasi secara aktif dalam upaya bela negara.

4. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP):

   Undang-undang ini mengatur tentang perlindungan data pribadi warga negara Indonesia yang mencakup asas-asas perlindungan data pribadi hingga pada kewajiban pengendali dan prosesor data pribadi. Dengan pemberlakuan UU ini, diharapkan bahwa hak privasi warga negara Indonesia terkait data pribadi dapat lebih terjamin dan aman dari ancaman serangan siber.

Selain itu, pemerintah Indonesia juga telah mendirikan sebuah lembaga khusus yang bertugas melaksanakan keamanan siber nasional secara efektif dan efisien. Lembaga ini dikenal dengan sebutan Badan Siber dan Sandi Nasional (BSSN). BSSN didirikan dengan tujuan untuk meningkatkan koordinasi dan efektivitas kewenangan, serta memperjelas pembagian tugas, dan fungsi yang terkait diantara berbagai institusi seperti Kementerian Komunikasi dan Informatika (Kominfo), Badan Intelijen Negara (BIN), Kementerian Luar Negeri, Kementerian Pertahanan, TNI, Polri, dan institusi lainnya. Pembentukan BSSN didasarkan pada Peraturan Presiden (Perpres) Nomor 53 Tahun 2017 dengan tujuan agar BSSN memiliki peran strategis dalam menjaga keamanan dan ketahanan negara dari ancaman siber.

Mengingat berbagai permasalahan dan tantangan terkait keamanan siber dan persandian yang semakin kompleks dan meresahkan, maka pembentukan Badan Siber dan Sandi Negara (BSSN) sangat diperlukan sebagai langkah strategis untuk menghadapi dinamika dunia digital yang terus berkembang. Pembentukan lembaga ini menjadi sebuah upaya yang penting dan esensial, karena BSSN diharapkan dapat menjadi garda terdepan dalam mengatasi persoalan-persoalan yang muncul dalam ranah siber, baik pada masa kini maupun di masa yang akan datang. Dengan keberadaannya, diharapkan akan tercipta upaya konkret dalam menghadapi berbagai ancaman siber yang semakin canggih dan kompleks. Intervensi pemerintah dalam hal ini sangatlah penting untuk memastikan bahwa tata kelola keamanan siber menjadi fokus utama, dengan langkah-langkah konkret dalam meningkatkan penerapan standar keamanan yang lebih ketat dan efektif. Prioritas pemerintah dalam hal ini adalah memastikan bahwa keamanan siber tidak hanya menjadi sebuah kebutuhan, tetapi juga menjadi pilar yang memperkuat ketahanan, keamanan, dan kedaulatan nasional. Dengan demikian, BSSN diharapkan dapat menjadi sebuah wadah yang efektif dalam menjembatani kepentingan antara sektor publik dan swasta dalam upaya menjaga keamanan dunia digital yang semakin terinterkoneksi.

Seperti yang telah dijelaskan sebelumnya, bahwa manajemen sekuriti memiliki peran yang sangat krusial dalam menciptakan pertahanan digital yang tangguh. Sama seperti halnya dengan sebuah benteng, manajemen sekuriti menjadi dasar yang kuat dalam menjaga keamanan data dan aset digital dari serangan siber. Beberapa peran krusial dari manajemen sekuriti dicantumkan sebagai berikut:

1. Mencegah ancaman siber: Dalam konteks ini, manajemen sekuriti melakukan beberapa pencegahan terhadap ancaman siber dengan mengimplementasikan langkah-langkah keamanan seperti autentikasi, enkripsi, dan kontrol akses. Dimana hal-hal tersebut dapat mengurangi risiko kebocoran dan pencurian data, hingga pada kerusakan sistem.
2. Mengurangi dampak kerugian: Dalam konteks ini, manajemen sekuriti menerapkan peran dalam mengurangi dampak kerugian dari ancaman siber dengan cara mendeteksi dan juga menanggapi insiden dengan cepat dan akurat. Sehingga hal tersebut dapat mencegah kerusakan yang lebih parah dan mempercepat proses pemulihan pada sistem.

3. Membangun kepercayaan: Dalam konteks ini, keberadaan manajemen sekuriti yang efektif dapat meningkatkan kepercayaan dan loyalti dari customer, mitra bisnis hingga para investor yang nantinya akan berkontribusi pada peningkatan reputasi dan persaingan antar organisasi di tengah era digital yang penuh akan tantangan.
4. Kepatuhan terhadap regulasi: Dalam konteks ini, manajemen sekuriti membantu organisasi dalam memenuhi standar regulasi keamanan data dan privasi yang berlaku, sehingga dapat terhindar dari potensi terkena sanksi.
5. Meningkatkan efisiensi operasional: Dalam konteks ini dengan mengotomatisasi proses-proses keamanan, manajemen sekuriti dapat meningkatkan efisiensi operasional organisasi dan mengurangi risiko gangguan operasi akibat serangan siber.

Sebagai elemen vital dalam upaya memperkuat pertahanan digital, manajemen sekuriti memungkinkan organisasi untuk melindungi aset digitalnya, membangun kepercayaan hingga meningkatkan efisiensi serta daya saing dalam lingkungan digital. Selain itu, untuk mencapai keamanan data juga perlu diterapkannya 3 prinsip utama keamanan informasi yakni CIA Triad (Confidentiality, Integrity, Availability). Kerahasiaan (Confidentiality); Pada konteks ini, menyatakan bahwa sebuah informasi tidak dapat diakses oleh semua orang melainkan hanya dapat diakses oleh orang yang berwenang. Integritas (Integrity): Pada konteks ini, dapat dikatakan bahwa sebuah informasi yang dimiliki harus akurat dan lengkap tidak dapat diubah maupun dimanipulasi oleh orang yang tidak berkewenangan. Ketersediaan (Availability); Pada konteks ini, bahwa informasi dan sumber daya yang terkait harus selalu tersedia dan mudah diakses oleh orang yang memiliki kewenangan saat diperlukan. Secara garis besar, manajemen sekuriti yang efektif dapat diselaraskan dengan 3 prinsip CIA Triad. Dengan mengimplementasikan keduanya, suatu organisasi dapat terus meningkatkan ketahanan digitalnya akan ancaman siber yang semakin berkembang.

UUD 1945 dan NKRI menjadi landasan hukum bagi regulasi serta upaya yang dilakukan pemerintah dalam menanggulangi kejahatan siber. Implementasi nilai-nilai kebangsaan yang bersumber dari Undang-Undang Dasar 1945 (UUD 1945) dan semangat Negara Kesatuan Republik Indonesia (NKRI) menjadi landasan penting dalam membangun pertahanan digital yang kuat. Pasal-pasal dalam UUD 1945, seperti pada Pasal 27 ayat (3) yang menegaskan hak dan kewajiban setiap warga negara berhak untuk

berpartisipasi dalam upaya pertahanan negara, menjadi landasan bagi keterlibatan seluruh lapisan masyarakat dalam menjaga keamanan siber. Begitu pula dengan semangat NKRI yang terwujud dalam Pancasila dan semboyan Bhinneka Tunggal Ika menjadi prinsip dalam membangun kolaborasi lintas sektor dalam memerangi ancaman siber.

Implementasi nilai-nilai kebangsaan ini juga tercermin dalam Undang-Undang Nomor 5 Tahun 2017 tentang Pemajuan Kebudayaan, yang memberlakukan pada pentingnya mempertahankan, mengembangkan, dan mengamalkan nilai-nilai kebudayaan yang menjadi bagian dari keberagaman bangsa. Dalam konteks pertahanan digital, manajemen sekuriti memainkan peran penting dalam menghadapi cybercrime. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan Pasal 30 yang mengatur tentang pelanggaran terhadap sistem dan/atau data elektronik merupakan instrumen hukum yang memperkuat upaya penegakan hukum terhadap pelaku kejahatan di dunia siber. Dengan mengintegrasikan nilai-nilai kebangsaan yang bersumber dari UUD 1945 dan semangat NKRI, serta memanfaatkan kerangka hukum yang telah ada, penguatan manajemen sekuriti dapat menjadi landasan kuat dalam membangun pertahanan digital yang efektif dan menghadapi tantangan cybercrime dengan lebih baik.

Hipotesa				**Hasil Analisa**
Variabel X		**Variabel Y**		
X1	Strategi Nasional dan Manajemen Sekuriti untuk Melawan Ancaman Siber di Indonesia	Y1	Undang-Undang Dasar 1945	Berkaitan dengan berbagai regulasi yang dikeluarkan seperti: UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah menjadi UU Nomor 19 Tahun 2016, Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber. Selain itu, juga berkaitan dengan Hak Asasi Manusia seperti: Hak atas Perlindungan Diri Pribadi, Keluarga, Kehormatan, Martabat dan sebagainya.
		Y2	Negara Kesatuan Republik Indonesia	Berkaitan dengan mempertimbangkan nilai-nilai fundamental seperti: Kedaulatan, Kemandirian, Keamanan, Kebersamaan, serta Adaptif dalam membangun kehidupan berbangsa dan bernegara.

X2	Pentingnya Pengembangan Kerangka Hukum dan Strategi Keamanan untuk Melindungi Aset dan Operasional	Y1	Undang-Undang Dasar 1945	Berkaitan dengan Pasal 33 UUD 1945 mengenai bumi, air, dan kekayaan alam yang terkandung di dalamnya dikuasai oleh Negara dan dipergunakan untuk kemakmuran rakyat. Selain itu, UU Nomor 19 Tahun 2016 tentang perubahan atas UU ITE No. 11 Tahun 2008.
		Y2	Negara Kesatuan Republik Indonesia	Berkaitan dengan Nilai Persatuan, Keadilan, Kemerdekaan, Kerakyatan, Ketuhanan yang merupakan aspek penting dalam mendukung stabilitas dan kemajuan Negara.
X3	Pentingnya Implementasi Nilai-Nilai NKRI dan Bela Negara dalam Penggunaan Teknologi	Y1	Undang-Undang Dasar 1945	Berkaitan dengan pasal-pasal yang ada di dalam UUD 1945 yakni Pasal 27 ayat 3 tentang kewajiban warga negara dalam upaya bela negara, Pasal 30 ayat 1 tentang hak dan kewajiban yang dimiliki warga negara dalam upaya pertahanan negara. Selain itu, juga didukung dengan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas UU ITE Nomor 11 Tahun 2008.
		Y2	Negara Kesatuan Republik Indonesia	Berkaitan dengan aspek-aspek seperti: Kemanusiaan, Persatuan Bangsa, dan Ketaatan Hukum yang berperan penting dalam membentuk sikap dan perilaku yang mendukung kedaulatan dan integritas bangsa di era digital.
X4	Perlindungan Data, Keamanan Siber, dan Meningkatkan Kepercayaan Pengguna dalam Konteks E-Commerce dan Pembayaran Digital	Y1	Undang-Undang Dasar 1945	• Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi • Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyedia Jasa Sistem Pembayaran • Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah diubah dengan Undang-

				Undang Nomor 19 Tahun 2016 • Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen Sejalan dengan UUD 1945 yang terletak pada Pasal 28G ayat (1): "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".
		Y2	Negara Kesatuan Republik Indonesia	Mencerminkan nilai kebangsaan NKRI yang berorientasi pada: • Kedaulatan • Keamanan nasional • Kesejahteraan masyarakat Nilai-nilai kebangsaan NKRI mengedepankan kedaulatan data, keamanan siber untuk melindungi infrastruktur digital, dan kesejahteraan masyarakat melalui ekonomi digital yang aman. Kedaulatan ini memberikan perlindungan data pribadi, dan keamanan nasional melindungi e-commerce dan pembayaran digital dari ancaman dunia siber. Pada akhirnya, kesejahteraan sosial dicapai dengan meningkatkan kepercayaan pengguna terhadap ekosistem digital yang aman.
X5	Peranan Sistem Biometrik sebagai Tambahan Keamaan dalam Cybercrime	Y1	Undang-Undang Dasar 1945	• Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 4 Tahun 2021 yang mengatur tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis

				dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik • Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang menggantikan Peraturan Pemerintah Nomor 82 Tahun 2012 Sejalan dengan Pasal 5 ayat (2) pada UUD 1945 yaitu memberi wewenang kepada Presiden untuk mengeluarkan peraturan pemerintah untuk menegakkan hukum dan dapat dilihat dengan melihat asas legalitas peraturan perundang-undangan di Indonesia. Peraturan tersebut dikeluarkan berdasarkan kewenangan yang diberikan oleh UUD 1945 dan merupakan bagian dari sistem hukum nasional yang bertujuan untuk melindungi keamanan informasi dan transaksi elektronik di Indonesia.
		Y2	Negara Kesatuan Republik Indonesia	Peran sistem biometrik sebagai tambahan keamanan terhadap kejahatan siber mencerminkan komitmen Republik Indonesia dalam memperkuat keamanan dan perlindungan data nasional. Hal ini menunjukkan nilai-nilai NKRI dalam melindungi kepentingan dan privasi individu serta menjaga kedaulatan negara dari ancaman kejahatan dunia siber yang semakin canggih.

KESIMPULAN DAN SARAN

Dalam upaya membangun pertahanan digital yang tangguh, dibutuhkannya integrasi antara teknologi digital yang canggih dengan implementasi dari nilai-nilai kebangsaan yang bersumber dari UUD 1945 dan NKRI. Nilai-nilai yang terkandung seperti gotong royong, persatuan dan kesatuan, semangat keadilan hingga pada kedaulatan rakyat menjadikan dasar yang penting dalam membangun hubungan antara lintas sektor serta melibatkan seluruh lapisan masyarakat dalam menghadapi tantangan siber. Selain itu, dibutuhkannya peran krusial dari manajemen sekuriti dalam memerangi ancaman siber seperti melakukan pencegahan, meminimalisir dampak kerugian, membangun kepercayaan, mematuhi peraturan hingga pada menigkatkan efisiensi operasional. Disamping itu, demi tercapainya peran manajemen sekuriti yang efektif diperlukan pula penerapan 3 prinsip keamanan yaitu CIA Triad (Confientiality, Integrity, Availability) yang sangat penting dalam menjaga keamanan informasi dan data. Dari gabungan kedua hal tersebut, juga harus diselaraskan dengan penetapan regulasi yang dikeluarkan oleh Pemerintah Indonesia sebagai langkah konkret dalam memperkuat pertahanan digital dan menanggulangi ancaman cybercrime seperti UU ITE, PERPRES, UU Pertahanan Negara, UU Perlindungan Data Pribadi hingga pada pendirian Badan Siber dan Sandi Nasional (BSSN). Dengan menerapkan nilai-nilai kebangsaan, memanfaatkan kerangka hukum yang telah ada serta penguatan manajemen sekuriti, Pemerintah Indonesia bertanggung jawab untuk menciptakan lingkungan digital yang ramah, aman, berkeadilan serta sesuai dengan identitas nasional jauh dari ancaman cybercrime.

DAFTAR PUSTAKA

Fachrudin, R., Respaty, E., Adilah, I. S., & Sinlae, F. (2024). Peranan Penting Manajemen Sekuriti di Era Digitalisasi. *Nusantara Journal of Multidisciplinary Science*, *2*(January). https://www.researchgate.net/publication/377219065_Peranan_Penting_Manajemen_Sekuriti_di_Era_Digitalisasi

Gojali, D. S. (2023). Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective. *International Journal of Cyber Criminology*, *17*(1), 1–11. https://doi.org/10.5281/zenodo.4766600

Haris, D. (2021). Implementasi Nilai-Nilai Kebangsaan yang Bersumber dari Negara Kesatuan Republik Indonesia (NKRI). *Jurnal Sains, Sosial Dan Humaniora (Jssh)*, *1*(2), 33–36. https://doi.org/10.52046/jssh.v1i2.914

Indah, F., & Sidabutar, A. Q. (2022). Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, *1*(1), 2. https://ejournal.kreatifcemerlang.id/index.php/jbpi/article/view/78%0Ahttps://ejournal.kreatifcemerlang.id/index.php/jbpi/article/download/78/8

Irawati, A., Fadholi, H. B., Alamsyah, A. N., Dwipayana, D. P., & Muslih, M. (2021). Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital. *Prosiding Conference On Law and Social Studies*, 1–15. http://prosiding.unipma.ac.id/index.php/COLaS

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*, *4*(5), 625–632. https://doi.org/https://doi.org/10.31933/jimt.v4i5

Mahendra, Y. C., & Pinatih, N. K. D. S. A. (2023). Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia. *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, *6*(4), 1941–1949. https://doi.org/https://doi.org/10.31004/jrpp.v6i4.20659

Ningrum, D. A., Fauzi, A., Syaridwan, A., Putri, I. A., Putri, M. P., & Amelia, S. (2023). Peran Manajemen Sekuriti Terhadap Keputusan Pembelian pada Pengguna Aplikasi Shopee (Studi Pustaka Manajemen Sekuriti). *JURNAL ILMU MANAJEMEN TERAPAN*, *4*(5). https://doi.org/https://doi.org/10.31933/jimt.v4i5.1564

Saputra, F., Soesanto, E., & Cahyaningtyas, K. I. (2024). Penerapan Manajemen Security Terhadap Cyber Crime di Kominfo. *IJM : Indonesian Journal of Multidisiciplinary*, *2*, 146–154.

Soesanto, E., Masyruroh, A. J., Putri, G. A. M., & Maharani, S. P. (2023). Peranan Manajemen Sekuriti Dalam Mengamankan Dan Memecahkan Masalah PT SK Keris Indonesia. *Jurnal Manajemen Riset Inovasi*, *1*(3), 46–57. https://doi.org/10.55606/mri.v1i3.1259

Soesanto, E., Saputra, F., Puspitasari, D., & Putra Danaya, B. (2023). Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File dan Pengamanan Cyber pada Yayasan Siber Publisher. *Jurnal Ilmu Multidisiplin (JIM)*, *2*(1), 23–29. https://doi.org/https://doi.org/10.38035/jim.v2i1 Received:

Soesanto, E., Utami, A. S., Chantica, J. A., Nabila, R. A., & Ricki, T. S. (2023). Keamanan Data Pribadi Dalam Sistem Pembayaran Via OVO Terhadap Ancaman dan Pengelabuan (Cybercrime). *IJM : Indonesian Journal of Multidisciplinary*, *1*, 424–435. https://journal.csspublishing/index.php/ijm%0AKeamanan

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 157–178. http://jurnalpkn.ui.ac.id/index.php/jkskn/article/view/28

Sufi, F. Y. N., Putri, D. K., & Suhartini, D. (2023). Analisis Ancaman Cybercrime dan Peran Sistem Biometrik : Systematic Literature Review. *Prosiding Senapan*, *3*(1), 19–29.

Syafi'i, M. H., Supriyadi, A. A., Prihanto, Y., & Gultom, R. A. G. (2023). Kajian Ilmu Pertahanan dalam Strategi Pertahanan Negara Guna Menghadapi Ancaman Teknologi Digital di Indonesia. *Journal on Education*, *5*(2), 4063–4076. https://doi.org/10.31004/joe.v5i2.1100

Yunita, E., Margiyanti, I. Y., Alawiyah, S., & Triadi, I. (2023). Penerapan Nilai Nilai Bela Negara Dalam Menghadapi Tantangan Era Digital. *Ilmu Hukum Dan Tata Negara*, *1*(4), 40–57. https://doi.org/https://doi.org/10.55606/birokrasi.v1i4.713