



## **IMPLEMENTASI KONSEP KEAMANAN NASIONAL DALAM UPAYA MENGHADAPI ANCAMAN SIBER DI INDONESIA**

**Christo Febi Cahya Manafe, Sapto Priyanto, Imam Subandi**

Program Studi Kajian Terorisme , Sekolah Kajian Stratejik dan Global,

Universitas Indonesia

### **Abstrak**

Studi ini berargumen jika keamanan nasional adalah salah satu aspek terpenting dalam menjaga kewanaman negara. Tidak hanya keamanan secara militer, Pemerintah juga perlu memperhatikan keamanan dari ruang siber. Oleh karena itu Pemerintah harus mengimplementasikan konsep keamanan nasional baik untuk ruang lingkup militer ataupun ruang siber. Penelitian ini dilakukan menggunakan metode kualitatif dengan pendekatan kepustakaan yang berfokus pada teori keamanan nasional dan ancaman siber. Penelitian ini menemukan hasil bahwa: Pemerintah Indonesia saat ini sudah berusaha untuk menjaga keamanan nasional baik dari sisi militer ataupun siber. Namun dalam implementasinya, saat ini belum ada regulasi khusus yang mengatur mengenai keamanan nasional. Sehingga dapat disimpulkan bahwa Pemerintah saat ini sudah menjalankan beberapa strategi untuk menjaga keamanan nasional baik dari bidang militer ataupun bidang siber, akan tetapi perlu adanya regulasi khusus terkait keamanan nasional untuk semakin memperkuat strategi yang disiapkan.

**Kata Kunci:** Kewanaman, Nasional, Ancaman, Siber, Indonesia.

### **PENDAHULUAN**

Pasca Perang Dunia II, negara menjadi peran utama dalam menciptakan keamanan dan kesejahteraan bagi warga negaranya melalui upaya pemenuhan ekonomi, layanan sosial, kesehatan, pendidikan, hukum, ketertiban, penurunan tingkat pengangguran, dan pengembangan

infrastruktur (Fjader, 2014). Dalam hal ini, negara dengan tekun mempertahankan peran sentralnya dalam kehidupan ekonomi, politik, sosial, dan budaya bagi warga negaranya. Istilah "keamanan" berasal dari bahasa Latin "securus" yang berarti bebas dari bahaya, ketakutan, dan ancaman (Liotta,2002). Keamanan dapat

\*Correspondence Address : [manafe.christo@gmail.com](mailto:manafe.christo@gmail.com)

DOI : 10.31604/jips.v10i4.2023.2063-2073

© 2023UM-Tapsel Press

didefinisikan dalam dua pendekatan yang berbeda. Pendekatan pertama adalah keamanan tradisional, yang mengacu pada keamanan negara yang dapat terganggu oleh kekuatan militer dari negara lain dan harus dilindungi oleh negara tersebut melalui upaya militer. Dalam pendekatan ini, negara berperan sebagai subjek dan objek dalam menciptakan keamanan. Pendekatan kedua adalah keamanan non-tradisional, yang berfokus pada kebutuhan keamanan dari pelaku bukan negara (Al A'raf, 2015). Keamanan non-tradisional melibatkan ancaman seperti terorisme, perdagangan ilegal, perubahan iklim, bencana alam, dan tantangan lain yang dapat mempengaruhi keamanan suatu negara. Dalam hal ini, negara tidak hanya menjadi fokus utama, tetapi juga bekerja sama dengan aktor non-negara untuk mencapai keamanan yang holistik. Pertahanan, atau "defence," dapat dianggap sebagai instrumen utama yang digunakan oleh negara untuk menciptakan keamanan nasional. Meskipun istilah "keamanan nasional" telah berkembang sejak akhir tahun 1940-an untuk mencakup aspek wilayah, kedaulatan, dan perlindungan individu warga negara, pertahanan tetap menjadi elemen sentral dalam mencapai tujuan tersebut.

Faktor pertahanan memiliki peran penting dalam sektor publik karena merupakan kewajiban dan kewenangan negara dalam menciptakan keamanan nasional. Pendanaan untuk keamanan nasional memiliki status yang istimewa karena merupakan prasyarat untuk mencapai stabilitas nasional, kemajuan ekonomi dan sosial, stabilitas politik, kesehatan masyarakat, dan sistem demokrasi yang baik (Holcner, 2018). Meskipun istilah "keamanan nasional" telah berkembang sejak akhir tahun 1940-an dan mencakup aspek wilayah, kedaulatan, dan perlindungan individu warga negara, pertahanan tetap menjadi instrumen utama yang

digunakan oleh negara untuk mencapai tujuan tersebut. Oleh karena itu, pendanaan untuk keamanan nasional memiliki posisi yang khusus dalam alokasi sumber daya negara karena pentingnya dalam menjaga kestabilan dan kesejahteraan negara secara keseluruhan. Ketahanan nasional adalah keadaan yang terus berkembang dan saling terkait dari seluruh aspek kehidupan suatu bangsa dalam menghadapi ancaman, tantangan, gangguan, dan hambatan (ATGH). Konsep ketahanan nasional mencerminkan implementasi dari prinsip-prinsip Pancasila dan UUD 1945. Dalam konteks ini, sila ketiga Pancasila, yaitu persatuan, diinterpretasikan dalam UUD 1945 sebagai negara yang bersatu (Pranowo, 2010).

Pada masa ini, ancaman yang berpotensi mengancam keamanan nasional tidak lagi hanya berupa ancaman militer konvensional saja. Ancaman dalam bentuk serangan siber juga menjadi salah satu hal penting yang harus di perhatikan. Berdasarkan laporan Fortinet pada Quartal IV 2022 diketahui bahwa, lebih dari satu juta serangan berupa virus dan botnets yang terjadi setiap hari di Indonesia. Selanjutnya berdasarkan data International Monetary Fund (IMF) tahun 2020, total kerugian rata-rata tahunan akibat serangan siber di sektor jasa keuangan secara global mencapai sekitar US\$ 100 miliar (Dwitya, 2023)

Untuk kasus terbaru mengenai serangan siber di Indonesia, adalah pembobolan data nasabah Bank Syariah Indonesia di tahun 2023 ini. Dilansir dari Tempo, PT Bank Syariah Indonesia (Persero) Tbk atau BSI mengalami serangan siber pada awal Mei 2023. Wakil Menteri Badan Usaha Milik Negara atau Wamen BUMN II Kartika Wiriartmodjo mengungkapkan jenis data yang bocor. Lebih lanjut Wmen BUUMN II menjelaskan "Untuk data yang di bobol misalnya data mengenai aplikasi kredit,

data marketing. Jadi itu data-data dari personal computernya pegawai cabang, ada juga data nasabah yang bocor tapi bukan data liabilities, kan yang rahasia itu core banking, data mutasi liabilities, misalnya data mutasi tabungan. Nah, so far itu belum kita lihat.” (Amelia, 2023)

Melihat data ini sudah seharusnya Pemerintah Indonesia sudah mulai Menyusun strategi dengan menerapkan konsep keamanan nasional di dalam dunia siber Indonesia. Jika hal ini tidak ditanggapi dengan serius, maka keamanan nasional Indonesia bisa goyah dan rentan diserang oleh pihak lainnya. Oleh karena itu peneliti tertarik untuk melakukan penelitian mengenai “Implementasi Konsep Keamanan Nasional dalam Upaya Menghadapi Ancaman Siber di Indonesia”. Adapun rumusan masalah yang peneliti angkat adalah bagaimana Implementasi Konsep Keamanan Nasional di Indonesia, serta bagaimana implementasi konsep keamanan tersebut di ruang siber. Adapun untuk menjawab rumusan masalah ini peneliti akan menggunakan teori-teori mengenai keamanan nasional dan ancaman siber.

### **Keamanan Nasional**

Barry Buzan (1991) membagi sektor keamanan ke dalam lima bidang; militer, politik, lingkungan, ekonomi dan sosial. Pendekatan militer merupakan salah satu pendekatan dalam sistem keamanan nasional. Sebagai sebuah konsep, keamanan telah mengalami evolusi pemaknaan yang luas dan berkembang mengikuti perkembangan dinamika perubahan zaman.

Dalam kajian keamanan, pemahaman tentang konsep keamanan setidaknya dapat dilihat dari dua pendekatan yakni pendekatan tradisional dan non – tradisional. Dalam pendekatan tradisional keamanan diartikan sebagai keamanan sebuah

negara yang dapat diancam oleh kekuatan militer negara lain harus dipertahankan melalui kekuatan militer negara itu sendiri.

Seiring dengan berakhirnya perang dingin, diskursus mengenai keamanan pun bergeser tidak lagi hanya terfokus pada negara. Perkembangan isu – isu strategis seperti demokratisasi, penegakan HAM dan fenomena terorisme telah memperluas cara pandang dalam melihat kompleksitas ancaman yang ada dan mempengaruhi perkembangan konsepsi keamanan. Ancaman tidak lagi hanya berupa ancaman militer tetapi juga ancaman nir militer.

Dalam pendekatan non – tradisional, konsepsi keamanan ditekankan kepada kepentingan keamanan pelaku – pelaku bukan negara (*non – state actors*). Konsepsi ini berkembang setelah menurunnya ancaman militer yang menggerogoti kedaulatan negara dimana disisi lain menunjukkan adanya peningkatan ancaman terhadap keamanan manusia pada aspek lain seperti penyakit menular, bencana alam, kerusakan lingkungan dan lainnya.

Menurut Christopher S. (2015) bahwa “*national security*” dalam konteks Amerika Serikat (AS) mengandung pengertian: “*the protection of the United States from major threats to our territorial, political, or economic well-being*”. Seperti juga dikonfirmasi oleh Tim National Security Council Amerika Serikat yang dihadirkan oleh Dephan AS, berarti negara (*state*) AS menggunakan istilah “national” untuk pengertian negara federasi (USA), bukan “*state*” yang berarti negara bagian. Bahkan bagi AS “*national security*” adalah keamanan kawasan dunia yang mengancam negara AS, sementara

untuk keamanan dalam negeri mereka mengembangkan “*home land security*”. Konsep keamanan nasional tidak lalu berarti keamanan secara nasional. Keamanan nasional lebih mengandung pengertian keamanan suatu negara sebagai satu kesatuan (*entitas*), bukan totalitas keseluruhan masalah keamanan, yaitu keamanan negara dan keamanan kehidupan dalam suatu negara. Secara umum, keduanya sama – sama berkuat mendebatkan wilayah cakupan keamanan (*referent object of security*).

Dalam pendekatan tradisional, keamanan secara sederhana diartikan sebagai keamanan sebuah negara yang dapat diancam oleh kekuatan militer negara lain dan harus dipertahankan melalui kekuatan militer negara itu sendiri. Dalam pendekatan ini, negara (*state*) menjadi subyek dan obyek dari upaya mengejar kepentingan keamanan. Pandangan kelompok ini menilai bahwa semua fenomena politik dan hubungan internasional adalah fenomena tentang negara. Dalam alam pemikiran tradisional ini negara menjadi inti dalam upaya menjaga keamanan negara.

### **Ancaman Siber**

Ancaman siber adalah setiap kondisi dan situasi serta kemampuan untuk melakukan tindakan, gangguan atau serangan yang dapat merusak atau merugikan yang mengancam kerahasiaan, integritas, dan ketersediaan sistem dan informasi. Jenis ancaman dunia maya dikategorikan berdasarkan target yang terkena dampak langsung. Sumber ancaman siber adalah entitas yang menghendaki atau bermaksud dan benar-benar akan melakukan kegiatan yang melanggar norma dan hukum, peraturan perundang-undangan serta aturan atau kontrol keamanan informasi

dan aset fisik lainnya, dengan tujuan untuk memperoleh materi dan keuntungan immaterial dengan memanfaatkan ruang siber yang ada. (Ratno, 2018).

Menurut Michael D. McDonnell dan Terry L. Sayers, dalam Buku Pedoman Pertahanan Siber Indonesia, jenis ancaman siber dikelompokkan dalam “: a) Ancaman Perangkat Keras (*hardware threat*), yaitu ancaman yang disebabkan oleh pemasangan peralatan tertentu yang berfungsi untuk melakukan kegiatan tertentu dalam suatu sistem, sehingga peralatan tsb merupakan gangguan terhadap sistem Jaringan dan Perangkat Keras lainnya, contoh : Jamming dan Network Intrusion. b) Ancaman Perangkat Lunak (*software threat*), yaitu ancaman yang disebabkan oleh masuknya software tertentu yang berfungsi untuk melakukan kegiatan seperti : Pencurian Informasi (*Information Theft*), Perusakan Informasi / Sistem (*Information / System Destruction*), Manipulasi Informasi (*Information Corruption*) dan lain sebagainya, ke dalam suatu sistem. c) Ancaman Data/Informasi (*data/information threat*), adalah ancaman yang diakibatkan oleh penyebaran data/informasi tertentu yang bertujuan untuk kepentingan tertentu, seperti yang dilakukan dalam information warfare termasuk kegiatan propaganda.” (Pertahanan, 2014)

Sehingga dapat disimpulkan bahwa Ancaman siber mencakup berbagai jenis serangan dan aktivitas yang dilakukan secara daring oleh individu, kelompok, atau negara dengan tujuan merusak, mengganggu, atau mendapatkan akses yang tidak sah ke sistem komputer dan jaringan. Oleh karena itu, penting bagi Pemerintah Indonesia untuk bisa menerapkan konsep keamanan nasional di ruang siber agar masyarakat terlindungi dari ancaman siber tersebut

## **METODE PENELITIAN**

Dalam penulisan tulisan ilmiah ini, penulis menggunakan metode penelitian kualitatif dengan pendekatan tinjauan kepustakaan (literature review). Menurut Creswell (2018), tinjauan kepustakaan adalah pendekatan penelitian yang didasarkan pada non-numeric data yaitu dapat berupa tulisan dan gambar, dan penyaringan terhadap data dilakukan untuk membuat interpretasi dari tinjauan pustaka (literature review). Kajian penelitian ini dilakukan melalui sumber literatur seperti jurnal, buku, tesis, research report, maupun artikel ilmiah dengan sumber yang valid dan realible.

## **HASIL DAN PEMBAHASAN**

### **Implementasi Konsep Keamanan Nasional di Indonesia**

Keamanan nasional, atau "*national security*," dapat diartikan sebagai konsep di mana pemerintahan, bersama dengan parlemen, bertanggung jawab untuk melindungi negara dan warga negaranya dari berbagai krisis "nasional" dengan menggunakan berbagai jenis kekuatan, termasuk kekuatan politik, diplomasi, kekuatan ekonomi, kemampuan militer, dan lain sebagainya. Definisi yang sangat berguna untuk keamanan nasional adalah kemampuan suatu bangsa untuk melindungi nilai-nilai internalnya dari ancaman yang berasal dari pihak luar (Berkowitz, 1965). Konsep ini berkembang dengan lebih pesat di Amerika Serikat setelah Perang Dunia II. Pada awalnya, fokus keamanan nasional terutama pada kemampuan militer, namun kemudian berkembang untuk mencakup berbagai aspek non-militer juga.

*The National Security Act of 1947*, bersama dengan amendemen-amendemenya, bersama-sama dengan Doktrin Truman dan Rencana Marshall (Marshall Plan), menjadi komponen utama dalam strategi pemerintahan AS

pada masa Perang Dingin. Yang menarik dalam undang-undang ini adalah tidak adanya batasan atau definisi yang spesifik mengenai keamanan nasional. Baru-baru ini, keamanan nasional telah diinterpretasikan oleh negara sebagai konstruksi yang melibatkan konsep "kepentingan" politik dan ekonomi. Pada masa pemerintahan Obama, konsep ini dipromosikan di seluruh dunia (National Security Strategy, 2010).

Yang lebih mengkhawatirkan, konsep ini kemudian secara terang-terangan diakui sebagai prioritas dalam keamanan nasional AS untuk melindungi kepentingan sekutu-sekutunya (US DoD, 2013). Hal ini memungkinkan AS untuk memberikan justifikasi dalam pembatasan hak asasi individu jika, misalnya, nilai-nilai konstitusional dari sekutu-sekutunya terancam. Interpretasi yang luas terkait hal ini menimbulkan masalah yang terkait dengan hukum hak asasi manusia internasional (UK Gov, 2010). Inggris dan negara-negara Eropa dalam hukumnya juga tidak memberikan definisi spesifik mengenai terminologi "keamanan nasional."

AS dan Inggris memiliki badan yang bertanggung jawab dalam menghadapi ancaman terhadap keamanan nasional. Di Inggris, badan yang memiliki tanggung jawab ini disebut MI5 *National Security Service*. Badan ini berperan sebagai lembaga intelijen yang bertugas melawan berbagai ancaman terhadap keamanan nasional, termasuk terorisme, spionase, dan ancaman *cyber*. Pemerintah Inggris mendefinisikan ancaman terhadap keamanan nasional sebagai ancaman yang dapat berasal dari sektor industri atau tindakan kekerasan yang terkait dengan kegiatan terorisme. MI5 hanya melakukan penyelidikan jika kasus tersebut secara khusus melibatkan upaya untuk menggulingkan atau merusak demokrasi parlementer Inggris. Dengan demikian, hanya kasus-kasus yang

memiliki niat seperti itu yang menjadi fokus penyelidikan oleh badan ini (Mi5, 2012).

Ancaman yang hanya membahayakan keamanan publik saja tidak menjadi prioritas, tetapi harus mencapai tingkat ancaman terhadap keamanan nasional. Untuk itu, MI5 bekerja melalui kerjasama dan kemitraan dengan berbagai pihak terkait. Selain melakukan tindakan pencegahan dan penyelidikan, badan seperti MI5 di Inggris dan NSA di AS juga memiliki peran dalam memberikan saran dan mengidentifikasi ancaman yang akan muncul masa depan terkait dengan keamanan nasional. National Security Agency (NSA) di AS memiliki peran utama dalam isu kriptologi dan intelijen sinyal yang dikenal sebagai SIGINT (*Signal Intelligence*). Badan ini juga bertanggung jawab dalam memastikan keamanan produk dan layanan informasi serta memfasilitasi operasi jaringan komputer untuk pengambilan keputusan yang bermanfaat bagi negara dan sekutunya dalam berbagai situasi.

Konsep keamanan nasional yang digunakan oleh negara-negara demokratis seperti AS dan Inggris terlihat tidak memiliki definisi yang jelas dan rinci dalam undang-undang yang mengaturnya. Alasan "fleksibilitas" seringkali dikemukakan sebagai alasan mengapa keamanan nasional tidak didefinisikan secara tegas, sehingga dapat beradaptasi dengan perubahan situasi. Meskipun alasan ini dapat diterima dari sudut pandang politik realis, hal ini menimbulkan pemikiran kritis jika dilihat dari perspektif hukum dan keadilan. Keamanan nasional dapat menjadi konsep yang digunakan oleh pemerintahan untuk mempertahankan posisi atau status quo mereka. Selama ini, keamanan nasional seringkali dihubungkan dengan bentuk-bentuk militer. Namun, pendekatan ini telah dikritik oleh McNamara karena masalahnya telah lama kita "tersesat" di

dalam hutan semantik dan mengidentifikasi keamanan sebagai fenomena militer secara eksklusif, terutama terkait dengan perang dan alat-alat militer (McNamara, 1968). Keamanan nasional dapat didefinisikan sebagai kondisi protektif yang diupayakan oleh warga negara dalam rangka melindungi berbagai komponen politik dari ancaman baik dari dalam maupun luar (Cohen, 1972).

Ketika menghadapi berbagai ancaman, seringkali negara cenderung mengandalkan strategi militer sebagai solusi, yang dapat menyebabkan ketidakpekaan terhadap keamanan dalam konteks yang lebih luas. Hal ini sering terjadi dalam pertempuran asimetris seperti melawan terorisme atau ancaman yang tidak terkait dengan militer.

Negara-negara yang memiliki pengalaman panjang dalam menghadapi ancaman militer, seperti Amerika Serikat pada masa Perang Dingin, cenderung mengadopsi pendekatan militer dalam menghadapi ancaman tersebut. Namun, pemikir-pemikir dalam bidang ini mengamati fenomena ini dan mencetuskan istilah-istilah yang terkait dengan keamanan nasional yang memiliki dimensi nilai-nilai kontekstual, termasuk hak asasi manusia. Salah satu istilah tersebut adalah "keamanan manusia" yang diusulkan oleh Barry Buzan. S

Subsistem Keamanan Publik bertujuan untuk melindungi masyarakat dari ancaman dan segala hal yang dapat membahayakan kepentingan dan kebutuhan publik. Subsistem Keamanan Warga Negara bertujuan untuk memberikan perlindungan keamanan kepada warga negara Indonesia di mana pun mereka berada, termasuk perlindungan terhadap hak-hak mereka untuk bebas dari rasa takut (kebebasan dari rasa takut) dan kebebasan untuk mencapai keinginan mereka (kebebasan dari keinginan), seperti keamanan

ekonomi, pangan, kesehatan, lingkungan, pribadi, komunitas, dan politik. Dalam menjalankan fungsi-fungsi tersebut, negara melaksanakan subfungsi-subfungsi dalam kerangka Keamanan Nasional yang dilakukan oleh aktor-aktor negara.

Keamanan nasional sebagai fungsi pemerintahan diemban oleh aktor negara yang memiliki otoritas politik dan aktor negara yang memiliki otoritas operasional. Otoritas politik merupakan representasi dari kedaulatan rakyat atau warga negara. Dalam konteks keamanan, aktor negara yang memiliki otoritas politik menetapkan kebijakan politik dalam bidang keamanan berdasarkan aspirasi yang berasal dari rakyat itu sendiri. Implementasi kebijakan politik dilakukan oleh aktor negara yang memiliki otoritas operasional. Seluruhnya juga mendapat pengawasan dari rakyat, baik melalui pengawasan sosial maupun lewat lembaga parlemen. Pengawasan yang dilakukan oleh warga negara, baik melalui parlemen maupun pengawasan sosial, bertujuan untuk memastikan bahwa negara benar-benar melaksanakan kewajibannya dalam memberikan perlindungan keamanan kepada negara, masyarakat, dan warga negara.

Pengawasan menjadi semakin penting ketika negara menggunakan kekuatan paksa dalam menjalankan fungsi keamanannya, karena penggunaan kekuatan paksa rentan terhadap penyalahgunaan kekuasaan yang justru dapat mengancam keamanan rakyat itu sendiri. Oleh karena itu, penggunaan kekuatan paksa harus didasarkan pada legitimasi politik yang kuat, transparan, dan akuntabel, serta dilaksanakan dengan penuh pertimbangan. Hal ini bukan hanya untuk melindungi rakyat, tetapi juga untuk melindungi para pelaksana otoritas operasional. Dalam konteks ini, penerahan kekuatan paksa tidak ditentukan semata-mata oleh pelaksana

otoritas operasional itu sendiri, tetapi ditentukan oleh pemegang otoritas politik. Namun demikian, diperlukan pengaturan yang jelas mengenai batasan kewenangan otoritas operasional dalam melaksanakan tindakan tersebut. Selain itu, sistem keamanan nasional harus mencakup pengaturan tentang pelaksanaan fungsi keamanan nasional dalam keadaan darurat dan perang. Dalam keadaan darurat atau perang, demi alasan keamanan nasional, pembatasan terhadap hak-hak warga negara dimungkinkan, sedangkan negara memiliki kewenangan yang lebih luas.

Oleh karena itu, status keadaan darurat dan perang ditetapkan oleh otoritas politik melalui mekanisme yang demokratis berdasarkan undang-undang. Dalam perspektif pemerintahan, keamanan nasional memiliki sifat multiaspek dan multifungsi serta diemban oleh berbagai institusi pemerintahan yang memerlukan mekanisme koordinasi dan sinkronisasi yang efektif. Oleh karena itu, berdasarkan kepentingan nasional dan dengan mempertimbangkan dinamika lingkungan strategis, tantangan yang dihadapi, serta kemampuan sumber daya nasional, Presiden menetapkan kebijakan keamanan nasional yang komprehensif dan mencakup semua fungsi keamanan nasional. Kebijakan keamanan nasional tidak hanya penting untuk pelaksanaan tugas lembaga pemerintahan, tetapi juga penting untuk pengawasan yang dilakukan oleh rakyat. Oleh karena itu, diperlukan sebuah Undang-Undang Keamanan Nasional yang dapat mencakup semua aspek dalam menghadapi perkembangan ancaman bagi Indonesia di masa depan, sehingga setiap komponen bangsa Indonesia memahami tugas, fungsi, dan peran masing-masing dengan jelas.

### **Implementasi Konsep Keamanan Nasional di Ruang Siber**

Dalam rangka menjaga keamanan negara di dunia maya, Presiden Republik Indonesia, Joko Widodo pada 19 Mei 2017 telah menandatangani Peraturan Presiden (Perpres) Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) yang kemudian direvisi melalui Perpres Nomor 133 Tahun 2017. BSSN adalah lembaga pemerintah non kementerian yang berkedudukan di bawah dan bertanggung jawab langsung kepada Presiden. BSSN bukanlah lembaga baru, melainkan penguatan lembaga yang sudah ada, yakni Lembaga Sandi Negara (Lemsaneg) dan Direktorat Pengamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika. (Ratno, 2018)

Melalui Badan Siber dan Sandi Negara, Pemerintah telah menyusun strategi keamanan siber untuk Indonesia. Untuk menciptakan lingkungan siber yang strategis dan terselenggaranya sistem elektronik yang aman, andal, dan terpercaya; memajukan dan menumbuhkan ekonomi digital dengan meningkatkan daya saing dan inovasi dunia maya; serta membangun kesadaran dan kepekaan terhadap keamanan dan ketahanan nasional di dunia maya, pemerintah melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) dan peraturan perubahannya Peraturan Presiden Nomor 133 Tahun 2017 membentuk BSSN yang bertugas menyelenggarakan siber keamanan secara efektif dan efisien dengan mendayagunakan, mengembangkan dan memantapkan seluruh elemen yang terkait dengan keamanan siber nasional (BSSN, 2021)

BSSN mengembangkan Strategi Keamanan Siber Indonesia sebagai acuan bagi seluruh pemangku kepentingan keamanan siber nasional dalam menyusun dan mengembangkan kebijakan keamanan siber di instansi masing-masing. Strategi keamanan siber

nasional dikembangkan sejalan dengan nilai-nilai dasar kehidupan bangsa, yaitu: Kedaulatan, Kemandirian, Keamanan, Kebersamaan, dan Adaptif. Visi Strategi Keamanan Siber Indonesia adalah :

“MEMBANGUN DAN MENJAGA KEAMANAN SIBER NASIONAL DENGAN MENSINERGIKAN BERBAGAI PEMANGKU KEPENTINGAN UNTUK IKUT SERTA MEWUJUDKAN KEAMANAN NASIONAL DAN MENINGKATKAN PERTUMBUHAN EKONOMI NASIONAL”

Sasaran strategis Strategi Keamanan Siber Indonesia adalah tercapainya ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber dan keamanan siber dalam ekonomi digital. Strategi Keamanan Informasi Indonesia diharapkan menjadi salah satu tumpuan kepercayaan dunia terhadap Indonesia di berbagai forum keamanan siber internasional. Strategi Keamanan Siber Indonesia merupakan kontribusi Indonesia dalam mendorong perdamaian dunia (BSSN, 2021).

Lebih jauh sebelumnya, Pemerintah melalui Kementerian Pertahanan juga sudah membuat buku pedoman pertahanan siber yang didalamnya membahas mengenai bagaimana Prinsip-prinsip Pertahanan Siber yang harus di terapkan di Indonesia. Adapun prinsip ini antara lain: (Pertahanan, 2014)

- a. Memiliki model pengamanan informasi yang terstruktur dan terintegrasi serta mengadopsi berbagai standar dan panduan pengamanan informasi yang ditetapkan oleh institusi yang berwenang.
- b. Faktor kerahasiaan, integritas dan ketersediaan pertahanan siber harus dipastikan sejak tahap perancangan sebagai salah satu prinsip dasar keamanan informasi.



- c. Pertahanan siber mengandung unsur kebijakan, kelembagaan, teknologi dan infrastruktur pendukung serta Sumber Daya Manusia.
- d. Implementasi pertahanan siber harus dilakukan oleh SDM yang memiliki kompetensi, integritas yang tinggi dan terlindungi.
- e. Dilakukan secara efektif dan efisien dalam bentuk keamanan fisik dan keamanan logis secara terintegrasi dengan memanfaatkan semaksimal mungkin teknologi terbuka dan produk Indonesia dalam rangka kemandirian dan kedaulatan.
- f. Penetapan zona pengamanan berdasarkan klasifikasi SDM yang terlibat seperti administrator, pengguna dan tipe lain.
- g. Mengacu kepada prinsip-prinsip tata kelola yang menjamin terwujudnya pengawasan melekat dalam pertahanan siber.
- h. Menjamin bahwa implementasi sistem siber aman dan tahan terhadap serangan siber lawan
- i. Mengembangkan kondisi yang lebih menguntungkan untuk tindakan ofensif.
- j. Menghindari kerugian pada sistem komputer yang tidak diinginkan.”

Berdasarkan uraian diatas, dapat dikatakan bahwa Pemerintah sudah mulai menerapkan konsep keamanan nasional dalam ruang siber. Hal ini dibuktikan dengan didirikannya BSSN serta disusunnya buku pedoman pertahanan siber Indonesia. Dalam hal ini Pemerintah sudah menerapkan

keamanan nasional sesuai dengan teori yang telah dibahas sebelumnya yang mana pemerintahan, bersama dengan parlemen, bertanggung jawab untuk melindungi negara dan warga negaranya dari berbagai krisis nasional dengan menggunakan berbagai jenis kekuatan untuk menghadapi ancaman siber, termasuk kekuatan politik, diplomasi, kekuatan ekonomi, kemampuan militer, dan lain sebagainya.

## **SIMPULAN**

Konsep keamanan nasional yang diperkenalkan oleh AS selama Perang Dingin sangat terkait dengan pendekatan militer sebagai pendekatan tradisional. Namun, setelah berakhirnya Perang Dingin, terjadi perubahan yang signifikan terutama dalam konteks perang melawan terorisme. Konsep keamanan nasional menjadi tidak relevan ketika diterapkan dengan pendekatan yang sama seperti pada masa Perang Dingin. Konsep ini menjadi ambigu dan tidak memiliki definisi yang jelas, terutama dalam kaitannya dengan kepentingan ekonomi, politik, dan perang melawan terorisme. Hal ini membuka peluang untuk penyalahgunaan kekuasaan. Dalam hal hak asasi manusia, perlu memperhatikan Standar Johannesburg dan memberikan “kesempatan bagi individu untuk menguji langkah-langkah yang diambil negara” dalam rangka keamanan nasional yang berdampak pada mereka. Individu harus dapat menguji langkah-langkah tersebut melalui lembaga-lembaga independen yang memiliki wewenang. Bagi Indonesia, sangat penting untuk memiliki payung hukum yang mengatur tentang keamanan nasional.

Hingga saat ini, Indonesia belum memiliki payung hukum dan kerangka regulasi yang khusus mengatur tentang keamanan nasional. Akan tetapi untuk permasalahan keamanan nasional di ruang siber, walau belum ada aturan khusus yang mengatur mengenai

keamanan nasional di ruang siber, Pemerintah melalui BSSN dan Kemhan dengan Pedoman Pertahanan Siber telah berusaha Menyusun strategi untuk menjaga keamanan nasional Indonesia di ruang siber. Kedepannya, diharapkan Indonesia memiliki payung hukum dan kerangka regulasi yang mengatur tentang keamanan nasional baik secara umum ataupun secara khusus di ruang siber agar semua komponen bangsa Indonesia memahami peran, tugas, fungsi, dan tanggung jawab masing-masing dalam menjaga stabilitas nasional. Dengan demikian, ketahanan bangsa Indonesia dalam menghadapi ancaman baik dari dalam maupun luar dapat diminimalisir secara efektif.

#### DAFTAR PUSTAKA

- A'raf, Al. (2015). "Dinamika Keamanan Nasional". *Jurnal Keamanan Nasional*. Vol. 1. No.1.
- Amelia Rahima Sari. (2023) Serangan Siber BSI, Wamen BUMN Ungkap Jenis Data yang Bocor. Jakarta: Tempo. Tersedia pada: <https://bisnis.tempo.co/read/1733822/serangan-siber-bsi-wamen-bumn-ungkap-jenis-data-yang-bocor>
- Anthony, Mely Caballero. (2015). "From Comprehensive Security to Regional Resilience: Coping with Nontraditional Security Challenges". ASEAN@50: Vol. 4-Building ASEAN Community Political Security and Socio-Cultural Reflections.
- B. Buzan, O. Wæver and J. de Wilde. (1991). "Security: A New Framework for Analysis, Boulder: Lynne Rienner, 1991, pp. 23-26."
- B. Saul. (2008). *Defining Terrorism in International Law*, Oxford: Oxford University Press.
- Berkowitz, Morton, and Bock, P.G, eds. (1965). *American National Security*. New York: Free Press,
- BSSN. (2021). PENGANTAR STRATEGI KEAMANAN SIBER INDONESIA. Tersedia pada: <https://bssn.go.id/strategi-keamanan-siber-nasional/>
- Creswell, J. W., & Poth, C. N. (2018). "Qualitative Inquiry and Research Design. Choosing Among Five Approaches (4th Edition ed.). California: Sage. De-radicalization Programs. *Terrorism and Political Violence*, 22(2), 267-291."
- Dwitya Putra. (2023). Hati-hati, Serangan Siber di Indonesia Capai 1,65 Juta. Jakarta: CNBC. Tersedia pada: <https://www.cnbcindonesia.com/tech/20230221220938-37-415809/hati-hati-serangan-siber-di-indonesia-capai-165-juta>
- Emmerson, Ben. (2012). "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Framework principles for securing the human rights of victims of terrorism, United Nations General Assembly
- Eshel, Yohanan and Kimhi, Shaul. (2016). "A New Perspective on National Resilience: Components and Demographic Predictors". *Journal of Community Psychology*. Vol. 44. No. 7.
- Fitrah, Elpeni. (2015). "Gagasan Human Security dan Kebijakan Keamanan Nasional Indonesia". *Jurnal Insignia*. Vol. 2. No. 1. April.
- Fjader, Christian. (2014). "The Nation-State, Nation Security and Resilience in the age of globalisation". *Journal Resilience*. Vol. 2 No.2.
- Friesendorf, Cornelius. (2012). *International Intervention and the Use of Force: Military and Police Roles; Geneva: A Center for Security, Development, and the Rule of Law*
- Kementerian Pertahanan Republik Indonesia. (2014). *Pedoman Pertahanan Siber*. Jakarta: Kementerian Pertahanan Republik Indonesia
- Lasswell, Horold D., and Kaplan, Abraham. (1950). "Power and Security. New Haven: Yale University Press."
- Lazarou, Elena dan Dobрева, Alina. (2019). "Security and Defence". *Journal European Parliamentary Research Service*. Juni.
- Liotta, P. H. (2002). "Boomerang Effect: The Convergence of National and Human Security". *Journal ResearchGate: Security Dialogue*. Vol. 4.
- Makdori, Yopi. (2019). "Lemhannas: Indeks Ketahanan Nasional Indonesia Cukup Tangguh", dalam <https://www.>

liputan6.com/news/read/3948215/lemhannas-indeks-ketahanan-nasionalindonesia-cukup-tangguh,

McNamara, Robert S. (1968). *"The Essence of Security"*. New York: Harper & Row

Ratno Dwi Putra, dkk. (2018). ANCAMAN SIBER DALAM PERSPEKTIF PERTAHANAN NEGARA (STUDI KASUS SISTEM PERTAHANAN SEMESTA). *Jurnal Prodi Perang Asimetris* | Agustus 2018, Volume 4, Nomor 2

United Kingdom government (2010). *"A Strong Britain in an Age of Uncertainty: The National Security Strategy"* (London) [2010] United Kingdom government "A Strong Britain in an Age of Uncertainty: The National Security Strategy" (London)

United States government. (2010). *National Security Strategy* Washington: diunduh di [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/national\\_security\\_strategy.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf)

Victoria, Artur. (2018). "Nation-National Defence and Security-Introduction", dalam <https://zenodo.org/record/1296358#.X6gXyWgzZnK>, DOI:10.5281/zenodo.1296358.