ANCAMAN SIBER DALAM PERSFEKTIF PERTAHANAN NEGARA

(STUDI KASUS SISTEM PERTAHANAN SEMESTA)

SIBER THREATS IN STATE DEFENSE PERSFECTIVES

(TOTAL DEFENSE SYSTEM CASE STUDY)

Ratno Dwi Putra [1], Supartono[2], Deni D.A.R.[3]

Prodi SPD Fakultas Strategi Pertahanan Universitas Pertahanan

(ratno.spdunhan@gmail.com)

Abstrak -- Kehidupan manusia senantiasa mengalami perubahan dan peningkatan akibat kemajuan peradaban yang terjadi akibat munculnya penemuan-penemuan oleh para ilmuwan. Internet merupakan salah satu penemuan terbesar dalam sejarah peradaban manusia yang memberikan banyak kemudahan sekaligus tantangan. Hal tersebut harus disikapi secara bijaksana sehingga perubahan yang ada dapat membawa kemajuan bangsa. Namun apabila tidak dapat disikapi dengan baik akan membawa dampak negatif khususnya bagi pertahanan negara. Tesis ini mencoba mengetahui dan menganalisis bagaimana persfektif para pemangku kepentingan khususnya di lingkungan TNI terkait pertahanan siber dihadapkan dengan pengembangan pertahanan negara yang menganut sistem pertahanan semesta. Metode yang digunakan dalam tulisan ini adalah metode penelitian kualitatif. Pengumpulan dan pengolahan data dengan melalui wawancara dengan para informan yang kemudian dilakukan analisis dengan menggunakan metode SWOT. Hasil penelitian ini nantinya diharapkan dapat dijadikan pertimbangan dalam membangun dan mengembangkan pertahanan siber khususnya di lingkungan TNI dalam menghadapi ancaman siber yang menimbulkan gangguan dan kerusakan pada infrastruktur kritis TNI yang dalam eskalasi besar dapat mengganggu pelaksanaan tugas pokok TNI dalam menegakkan kedaulatan negara, mempertahankan keutuhan wilayah Negara Kesatuan Republik Indonesia dan melindungi segenap bangsa dan seluruh tumpah darah Indonesia dari ancaman dan gangguan terhadap keutuhan bangsa dan negara.

Kata Kunci: ancaman, siber, dan pertahanan negara

Abstract *-- Human life has always undergone changes and improvements due to the progress of civilization that occurred due to the emergence of discoveries by scientists. The internet is one of the greatest discoveries in the history of human civilization which provides many conveniences and challenges. This must be addressed wisely so that changes can bring the nation's progress. However, if it cannot be addressed properly it will have a negative impact, especially for the national defense. This thesis tries to find out and analyze how the perspectives of stakeholders, especially within the TNI, regarding cyber defense are faced with the development of national defense that adheres to the universal defense system.*

[1] Penulis adalah alumni pada Program Studi SPD Cohort 5 Tahun 2018 Universitas Pertahanan

[2] Dr. Ir. Supartono, M.M adalah dosen pada Universitas Pertahanan

[3] Deni D.A.R, S.Sos., M.Si(Han) adalah dosen pada Universitas Pertahanan

The method used in this paper is a qualitative research method. Data collection and processing through interviews with informants who then analyzed using the SWOT method. The results of this study are expected to be taken into consideration in building and developing cyber defense, especially in the TNI environment in the face of cyber threats that cause disruption and damage to critical infrastructure of the TNI, which in large escalation can interfere with the implementation of the TNI's main task in upholding state sovereignty, maintaining the territorial integrity of the State The unity of the Republic of Indonesia and protect all nations and all of Indonesia from the threat and disturbance of the integrity of the nation and state.
Keywords: threat, cyber, and national defence

Pendahuluan

Peradaban manusia senantiasa mengalami perubahan dari waktu ke waktu dan dari masa ke masa. Peningkatan dari peradaban manusia merupakan anugerah dari Tuhan Yang Maha Esa, melalui akal dan pikiran yang dimilikinya tersebut digunakan untuk menjadikan kehidupan manusia jauh lebih baik dari hari ke hari. Serangkaian penemuan oleh para ilmuwan termuka di dunia membawa kemajuan dalam peradaban manusia tersebut. Internet merupakan salah satu penemuan terbesar dalam sejarah peradaban manusia yang memberikan banyak kemudahan sekaligus tantangan. Sejarah internet berawal pada tahun 1969, dimana sebuah lembaga riset pemerintah Amerika Serikat, *National Science Foundation (NSF)* membantu pengembangan jaringan *Advanced Research Project Agency Network (ARPANET)*. Pada Oktober 1972, ARPANET diperkenalkan kepada masyarakat secara umum dan mendapat dukungan serta berkembang pesat di seluruh wilayah negara tersebut. Banyak Universitas yang ingin bergabung dalam jaringan tersebut sehingga ARPANET dibagi menjadi 2 (dua) jaringan, yaitu MILNET dan ARPANET. MILNET di khususkan penggunaan untuk kalangan sedangkan ARPANET digunakan untuk pengguna non militer, seperti sekolah-sekolah dan Universitas. Gabungan MILNET dan ARPANET ini pada akhirnya dikenal dengan sebutan DARPA Internet yang kemudian lebih dikenal sebagai Internet.[4] Dalam perkembangannya, Internet membawa perubahan terhadap kehidupan manusia, perkembangan ilmu pengetahuan dan teknologi yang terjadi dewasa ini khususnya pada era globalisasi merupakan suatu hal yang tidak bisa dihindari oleh bangsa-bangsa dan negara-negara di

[4] https://ilmupengetahuan.org/sejarah-perkembangan-internet/, di akses pada tanggal 13 Mei 2018

seluruh penjuru dunia ini. Kondisi ini disadari betul oleh negara maju seperti Amerika Serikat yang menjadikan internet menjadi sebuah matra atau dimensi baru yang harus dijelajahi, dikuasai dan dipertahankan setelah darat, laut, udara dan ruang angkasa.

Beberapa negara dewasa ini sudah membentuk Badan atau Organisasi yang khusus menangani permasalahan siber dalam sistem pertahanan negaranya. Amerika Serikat memiliki *United States Cyber Command* (*US CYBERCOM*) di bawah *United States Strategic Command* (*US STRATCOM*). Pakta Pertahanan Negara-Negara di Atlantik Utara atau *NATO* membentuk *NATO Cooperative Cyber Defense Centre of Excellence* (NATO CCD COE) sebagai badan keamanan siber dalam rangka meningkatkan kemampuan pertahanan siber NATO. Negara-negara lain di Kawasan Benua Asia dan Australia juga melihat permasalahan siber merupakan permasalahan serius dan memungkinkan mempengaruhi pertahanan negara. Australia melalui Direktorat Pertahanan Sinyal Departemen Pertahanan Australia membentuk sebuah Badan yang dinamakan *Cyber Security Operations Centre* (CSOC) yang bertanggung jawab untuk mendeteksi dan menangkal ancaman kejahatan cyber terhadap kepentingan dan pemerintah Australia. Negara China turut membentuk pasukan dunia maya. Pasukan tersebut diberi nama "*Blue Army*", pasukan ini bertugas melindungi pertahanan negara China dari serangan siber. Pasukan tersebut memiliki *homebase* di kawasan militer Guangzhou, sebelah selatan China. Inggris juga membangun pertahanan cyber. Sistem yang disebut *Cyber Security Operations Centre* (CSOC) itu berada di *Government Communications Headquarters* (GCHQ) Inggris, di Cheltenham, sekitar 160 kilometer arah barat laut London.[5]

Presiden Republik Indonesia, Joko Widodo pada tanggal 19 Mei 2017 telah menandatangani Peraturan Presiden (Perpres) Nomor 53 tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) yang kemudian dilakukan revisi melalui Perpres Nomor 133 Tahun 2017. BSSN merupakan lembaga pemerintah non kementerian yang berkedudukan di bawah dan bertangung

[5] Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia Letkol Chb Ir. Bagus Artiadi Soewardi, M.Si. Maret 2013.

jawab langsung kepada Presiden. BSSN bukan merupakan lembaga baru yang dibentuk, namun merupakan penguatan dari lembaga yang telah ada sebelumya, yaitu Lembaga Sandi Negara (Lemsaneg) dan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika.

Perkembangan perang siber *(cyber warfare)* merupakan suatu bentuk ancaman yang sangat rentan bagi pertahanan negara. Hal tersebut dibuktikan dengan berbagai kejadiaan peretasan situs yang dimiliki oleh pemerintah, salah satu contoh terkini yaitu situs Komisi Pemilihan Umum (KPU) dengan alamat website infopemilu.kpu.go.id yang menyajikan informasi hasil *real count* atau hitung riil Pilkada sementara 2018 . Halaman situs KPU diserang secara masif oleh oknum yang tidak bertanggungjawab. . Kejadian serupa juga dialami oleh situs milik pemerintah lainnya yaitu situs yang dimiliki oleh Ditjen Pajak, Kementerian Keuangan dengan alamat pajak.go.id. Situs tersebut diserang peretas atau *hacker* pada tanggal 10 Juni 2018. Situs tersebut diretas oleh pihak yang mengaku sebagai Anonymous Arabe. Kejadian-kejadian serangan siber seperti merubah tampilan halaman (deface) terhadap situs pemerintah maupun swasta begitu sering terjadi, situs milik Tentara Nasional Indonesia (TNI) pun pernah mengalami hal serupa.

Ancaman yang paling besar kemungkinan bisa terjadi bilamana informasi-informasi yang bernilai strategis dan berklasifikasi sangat rahasia jatuh ke tangan pihak yang tidak bertanggungjawab akan berpengaruh terhadap kedaulatan negara dan keutuhan wilayah NKRI. TNI menyadari semakin besarnya tantangan dalam menjaga kedaulatan bangsa dan negara termasuk yang memasuki kedaulatan di dunia maya . Melihat realita, fakta-fakta dan mempertimbangkan segala hakekat ancaman yang bakal dihadapi tersebut, maka dibentuklah organisasi siber di tubuh TNI yaitu Satuan Siber TNI. Pembentukan Satuan Siber TNI sebagai upaya dalam menghadapi ancaman dan serangan siber dalam rangka melindungi infrastruktur informasi kritis TNI yang semakin meningkat dan merupakan medan pertempuran utama di masa mendatang. Panglima TNI Marsekal Hadi Tjahjanto dalam amanatnya pada pelaksanaan apel luar biasa jajaran Mabes TNI pada bulan Desember 2017,

mengeluarkan Perintah Harian Panglima TNI yang salah satu isinya yaitu "Sikapi secara cerdas terhadap perkembangan lingkungan strategis, upaya adu domba, provokasi, penyalahgunaan media sosial dan serangan siber dengan memanfaatkan perkembangan ilmu pengetahuan dan teknologi (Ilpengtek)".

Berdasarkan latar belakang tersebut diatas dapat dijelaskan bahwa dunia maya bagi sebagian negar-negara maju dalam hal ini negara *super power* dan negara-negara *great power* seperti Amerika Serikat, Inggris, Rusia, China, Australia dan negara lainnya, menjadi mandala perang baru yang membuat semua negara berusaha untuk memperkuat pertahanan sibernya dalam rangka menjamin kedaulatan negara tersebut di ranah siber.

Negara Indonesia menganut Sistem Pertahanan Semesta. Pertahanan Negara ditujukan dalam menjamin kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia dan menjamin keselamatan seluruh bangsa dan negara Indonesia, dimana ancaman siber merupakan suatu bentuk ancaman nyata yang dapat menganggu pencapaian tujuan negara sebagaimana tercantum dalam Pembukaan undang-Undang Dasar 1945. Dalam menyiapkan Sistem Pertahanan Semesta perlu dirumuskan secara komprehensif dan disinkronisasi dengan Kementerian/Lembaga Negara yang terkait sehingga perkembangan ancaman yang terjadi dapat diantsipasi dengan baik. Perlunya kesatuan pemikiran, pemahaman dan tindakan dalam membangun Sistem Pertahanan Semesta yang tangguh dalam menghadapi segala bentuk ancaman yang salah satunya ancaman siber yang senantiasa berkembang sesuai dengan perkembangan ilmu pengetahuan dan teknologi. Dari untuk itu peneliti merumuskan masalah yaitu Bagaimanakah bentuk ancaman siber saat ini dan tren perkembangan ancaman siber? Dan Bagaimana bentuk Sistem Pertahanan Semesta yang perlu dibangun dalam menghadapi ancaman siber?

Ancaman secara harfiah dapat diartikan sebagai upaya, pekerjaan, kegiatan, dan tindakan, baik yang datang dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat membahayakan keselamatan bangsa, keamanan, kedaulatan, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan

kepentingan nasional di berbagai aspek, baik ideologi, politik, ekonomi, sosial budaya, maupun pertahanan dan keamanan. Prof. Dr. Mahfud M.D (mantan Menteri Pertahanan RI) mengemukakan bahwa ancaman yang menggunakan pendekatan tidak langsung lebih menonjol dibanding ancaman langsung sehingga menuntut kesadaran bela negara yang tinggi. Bela negara merupakan hak dan sekaligus kewajiban dari setiap warganegara, oleh karena itu partisipasi aktif dari warganegara menjadi tolok ukur keberhasilan pelaksanaan bela negara. Sejalan dengan hal tersebut Prof Dr. Juwono Sudarsono mengemukakan bahwa ancaman di masa depan ditandai dengan pengunaan elemen *precision strike, information warfare, dominating maneuvers* dan *space warfare*. Penggunaan teknologi dalam berperang secara langsung membutuhkan perubahan doktrin perang yang ada saat ini. Kemampuan angkatan perang dari suatu negara akan semakin meningkat hal tersebut sejalan dengan peningkatan kemampuan Alustsista yang ada. Teknologi yang ada saat ini tidak hanya berupa Alutsista yang biasa digunakan dalam perang yang bersifat fisik, namun terdapat juga suatu penggunaan teknologi yang bersifat non fisik yang dapat menimbulkan kerusakan fisik seperti pada penggunaan teknologi pada perang siber. Teori ancaman lainnya yaitu dari Stephen M.Walt bahwa dimana negara-negara dalam menghadapi suatu ancaman dengan menerapkan suatu keseimbangan dimana perilaku aliansi negara ditentukan oleh ancaman yang membahayakan mereka dari negara-negara lain. Walt berpendapat bahwa negara-negara pada umumnya akan menyeimbangkan kekuatan angkatan bersenjatanya dengan bersekutu untuk melawan ancaman dalam bentuk suatu aliansi atau pakta pertahanan. Dengan adanya ancaman yang meningkat, negara-negara yang lemah kekuatan angkatan bersenjatanya akan lebih mungkin untuk ikut bergabung dalam suatu aliansi dalam rangka melindungi keamanan mereka sendiri. Teori Walt mengidentifikasi 4 (empat) kriteria yang digunakan untuk mengevaluasi ancaman negara lain: kekuatan agregat (ukuran, populasi, dan kemampuan ekonomi), kedekatan

geografis, kemampuan ofensif, dan niat ofensif.[6]

Pertahanan negara adalah segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara.[7] Bentuk pertahanan negara bersifat semesta dalam arti melibatkan seluruh rakyat dan segenap sumber daya nasional, sarana dan prasarana nasional, serta seluruh wilayah negara sebagai satu kesatuan pertahanan. Teori kesemestaan dalam konteks pertahanan negara menurut Prof. Dr. Mahfud M.D bermakna totalitas sarana, metoda untuk mencapai tujuan Bersama. Kerakyatan bermakna human security, HAM, hak individu, dan publik untuk menikmati rasa aman dan turut serta mengupayakan keamanan. Pertahanan negara disusun berdasarkan prinsip demokrasi, hak asasi manusia, kesejahteraan umum, lingkungan hidup, ketentuan hukum nasional, hukum internasional dan kebiasaan internasional, serta prinsip hidup berdampingan secara damai dengan memperhatikan kondisi geografis Indonesia sebagai negara kepulauan.

Sistem pertahanan negara yang dianut negara Indonesia yaitu sistem pertahanan yang bersifat semesta yang melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah, dan keselamatan segenap bangsa dari segala ancaman. Sistem pertahanan negara dalam menghadapi ancaman militer menempatkan Tentara Nasional Indonesia sebagai komponen utama dengan didukung oleh komponen cadangan dan komponen pendukung. Dalam menghadapi ancaman nonmiliter, menempatkan lembaga pemerintah di luar bidang pertahanan sebagai unsur utama yang disesuaikan dengan bentuk dan sifat ancaman dengan didukung oleh unsur-unsur lain dari kekuatan bangsa. Sistem pertahanan negara melibatkan seluruh komponen pertahanan negara, yang terdiri atas

[6] Sthepen.M.Walt, International Security Vol-9 No.4 Spring, 1985.

[7] Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara.

komponen utama, komponen cadangan, dan komponen pendukung.

Tatanan segenap unsur kekuatan diselenggarakan secara menyeluruh, terpadu dan terarah dibawah kesatuan komando dengan memadukan strategi pertahanan, sehingga merupakan satu totalitas pertahanan negara. Menghadapi ancaman militer, menempatkan TNI sebagai komponen utama didukung komponen cadangan dan komponen pendukung melalui suatu mobilisasi sesuai ketentuan perundang-undangan. Menghadapi ancaman nonmiliter menempatkan K/L diluar bidang pertahanan sebagai Unsur Utama didukung oleh Unsur Lain Kekuatan Bangsa termasuk Pemda. Sedangkan dalam menghadapi ancaman hibrida berdasarkan Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, dilakukan suatu pendekatan pertahanan negara sebagaimana menghadapi ancaman militer dengan menempatkan TNI sebagai komponen utama dengan didukung instansi/Lembaga negara terkait sesuai dengan fungsi dan bidang tugas masing-masing. Penyelengaraan pertahanan tersebut diatas dapat dilakukan melalui sistem pertahanan militer dan sistem pertahanan nirmiliter yang dilaksanakan secara terpadu dengan mengerahkan kekuatan militer dan kekuatan nirmiliter sesuai kebijakan dan keputusan politik negara.

Keamanan Siber adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna. Organisasi dan aset pengguna dalam *cyber-security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya. *Cyber-security* merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan *cyber*. Tujuan keamanan umum terdiri dari: ketersediaan; Integritas termasuk didalamnya keaslian dan kemungkinan upaya mengurangi terjadinya penolakan serta terakhir kerahasiaan. *Global cyber-security* dibangun

di atas lima bidang kerja antara lain: Kepastian Hukum; teknis dan tindakan prosedural; struktur organisasi; *capacity building* dan Pendidikan Pengguna; dan Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*). [8]

Penelitian ini menggunakan metode kualitatif karena tujuan penelitian ingin melihat kedalaman permasalahan yang diangkat oleh peneliti, dimana dalam penelitian kualitatif dapat menyajikan data secara deskriptif. Pada pelaksanaan wawancara, peneliti menggunakan pedoman wawancara. Penelitian ini menggunakan teknik *purposive sampling* sebagai metode pemilihan informan. Informan yang dipilih harus memenuhi kriteria-kriteria tertentu. Kedalaman permasalahan diperoleh melalui pengumpulan data sekunder terkait dengan penelitian yang akan dilakukan. Selanjutnya pengambilan data primer dilakukan dengan menggunakan *indepth interview* melalui tanya jawab secara tatap muka antara peneliti dengan para informan yang berdinas di Satuan Siber TNI dalam rangka mengetahui sejauhmana ancaman siber yang ada di Indonesia dihadapkan dengan Sistem Pertahanan Semesta khususnya dalam menghadapi ancaman siber yang bakal terjadi. Selanjutnya suatu perspektif dapat diungkap melalui pengkajian dengan menggunakan penelitian kualitatif

Teknik Pengumpulan data diperoleh dengan beberapa cara yang mencerminkan metode kualitatif, dengan mengumpulkan beragam jenis data dan memanfaatkan waktu seefektif mungkin dalam mengumpulkan informasi di lokasi penelitian. Adapun teknik pengumpulan data dalam penelitian ini menggunakan wawancara dan dokumentasi (yang didalamnya termasuk pengumpulan materi audio dan visual). Dalam penelitian ini, teknik pengumpulan data yang utama adalah observasi, wawancara, studi dokumentasi

Ancaman siber *(cyber threat)* adalah setiap kondisi dan situasi serta kemampuan yang dinilai dapat melakukan tindakan, gangguan atau serangan yang mampu merusak atau segala sesuatu yang merugikan sehingga mengancam

[8] Edmon Makarim, *Indonesian Legal Framework for Cybersecurity http://www.nisc.go.jp/security-site/campaign/ ajsympo/pdf/lecture2.pdf*

kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan *(availability)* sistem dan informasi. Dalam rangka merumuskan kajian organisasi pertahanan siber diperlukan pemahaman mengenai ancaman dan serangan siber. Ancaman dan serangan siber menjadi acuan dalam penetapan resiko yang mungkin akan timbul untuk menentukan langkah-langkah dalam pengkajian organisasi pertahanan siber di lingkungan TNI dari segi jenis ancaman dan serangan serta dalam skala penanggulangan

Tren Perkembangan Ancaman Siber

Ancaman siber *(cyber threat)* adalah setiap kondisi dan situasi serta kemampuan yang dinilai dapat melakukan tindakan, gangguan atau serangan yang mampu merusak atau segala sesuatu yang merugikan sehingga mengancam kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan *(availability)* sistem dan informasi. Jenis ancaman siber dikelompokkan berdasarkan target yang terdampak langsung. Sumber ancaman siber merupakan entitas yang berkeinginan atau memiliki niat dan benar-benar secara nyata akan melakukan kegiatan yang melanggar norma dan hukum, aturan dan ketentuan serta kaidah atau kontrol keamanan informasi serta aset fisik lainnya, dengan tujuan untuk mendapatkan keuntungan yang bersifat materil dan immaterial dengan memanfaatkan ruang siber yang ada.

Secara umum sumber-sumber yang dapat identifikasi memiliki potensi sebagai sumber ancaman siber meliputi sumber internal dan eksternal, kegiatan intelijen, kekecewaan, investigasi, organisasi ekstremis, *hacktivists,* grup kejahatan terorganisir, persaingan, permusuhan dan konflik serta teknologi. Segala aspek ancaman siber meliputi aspek-aspek ideologi, politik, ekonomi, sosial budaya, pertahanan keamanan, ilmu pengetahuan dan teknologi serta aspek lain yang terkait dalam kehidupan berbangsa dan bernegara termasuk kepentingan pribadi. Ancaman siber dapat dilakukan baik oleh siapa saja baik secara perorangan maupun organisasi

Berbagai bentuk ancaman siber saat ini telah mengancam dan berdampak negatif terhadap kehidupan manusia. Berdasarkan data yang ada para pelaku memiliki motif yang berbeda dalam melaksanakan kegiatannya. Berbagai sasaran baik perorangan maupun organisasi

/institusi tak luput dari ancaman siber yang ada begitu juga beberapa infrastukrur kritis militer menjadi sasaran. Adapun bentuk ancaman siber yang sering terjadi saat ini dapat berupa hal-hal sebagai berikut ; serangan *advanced persistent threats (APT), denial of service (DoS)* dan *Distributed Denial of Service (DDoS)*; serangan *defacement*; serangan *phishing*; serangan *malware;* penyusupan siber; *spam*; dan penyalahgunaan protokol komunikasi.

Dari berbagai ancaman siber yang telah disebutkan diatas penyusupan siber dan penyalahgunaan protocol komunikasi merupakan sesuatu yang bakal menjadi trend ancaman yang perlu diwaspadai dan memerlukan perhatian khusus karena jika tidak dapat di antisipasi secara dini maka dari ancaman yang bersifat potensial menjadi faktual berupa kegiatan atau tindakan yang bertujuan untuk memasuki, menguasai, memodifikasi, mencuri atau merusak, atau menghancurkan atau melumpuhkan sistem atau aset informasi yang kita kenal sebagai serangan siber (*cyber attack)*. Serangan siber yang memiliki intensitas dan skala yang luas akan berdampak langsung terhadap pertahanan negara. Berbagai negara di berbagai belahan dunia juga tidak luput dari ancaman siber. Sebagaimana laporan yang dikeluarkan oleh satu perusahaan keamanan dunia maya Avast menyebutkan bahwa dampak salah satu serangan virus ransomware WannaCry menginfeksi jutaan computer di hamper 99 (sembilan puluh Sembilan) negara. Beberapa ahli mengatakan serangan tersebut kemungkinan dilakukan untuk mengeksploitasi kelemahan sistem Microsoft yang telah diidentifikasi NSA dan diberi nama EternalBlue. Alat peretas milik NSA kemudian dicuri sekelompok *hacker* yang menyebut dirinya sebagai The Shadow Brokers, yang kemudian mencoba menjualnya dalam lelang online.

Bentuk Sistem Pertahanan Semesta yang Perlu Dibangun Dalam Menghadapi Ancaman Siber

Ancaman dan serangan siber yang telah terjadi di beberapa negara termasuk yang pernah terjadi di Indonesia, menjadi acuan dalam penetapan resiko yang mungkin akan timbul dan hal tersebut menjadi pedoman dalam menentukan langkah dalam melakukan pengkajian terhadap peningkatan kemampuan pertahanan siber

negara termasuk didalamnya pertahanan siber di lingkungan TNI. Berdasarkan aturan yang ada menyebutkan Satuan Siber TNI merupakan satuan pelaksana Mabes TNI yang bertugas menyelenggarakan operasi dan kegiatan siber dilingkungan TNI. Dalam pelaksanaan tugasnya Satuan Siber TNI bertindak sebagai perencana operasi dan kegiatan Siber TNI, perencana administrasi dan logistik, pelaksana penangkalan, pemulihan dan perbantuan dukungan terhadap ancaman serangan siber serta diharapkan dapat mendukung tugas dalam melaksanakan operasi militer untuk perang maupun operasi militer selain perang. Pembentukan Satuan SIber TNI dilandasi oleh pemikiran para pemimpin TNI yang memandang bahwa permasalah siber merupakan suatu hal yang penting dan saat ini sudah menjadi bagian dari sistem pertahanan negara. Pengembangan kemampuan siber yang ada dilingkungan TNI tidak dapat dilepaskan dari pengembangan kemampuan siber nasional. Saat ini kondisi Satuan Siber TNI masih belum dapat melaksanakan tugas pokok yang diembannya secara optimal dikarenakan masih adanya beberapa kendala. Kendala-kendala yang ada berasal dari aspek peranti lunak, dan tata kelola, organisasi dan kelembagaan, sumber daya manusia, infrastruktur, serta anggaran.

Pada suatu kegiatan penelitian hal terpenting yang perlu diperhatikan untuk menghasilkan keluaran yang bersifat konstruktif adalah suatu proses analisa dari data-data yang telah didapatkan. Pada penelitian ini akan digunakan Metode SWOT sebagai metode dalam menganalisa data-data yang ada untuk menentukan strategi yang akan digunakan dalam rmembangun pertahanan siber yang tangguh dalam kerangka Sistem Pertahanan Semesta. Analisis SWOT dapat diuraikan kedalam tiga aspek, yaitu input, proses, dan output. Input merupakan data awal yang selanjutnya akan diproses sehingga menghasilkan hasil berupa penyelesaian terhadap penelitian yang dilaksanakan. Sehingga tujuan dari pengujian ini adalah untuk menyiapkan kekuatan secara maksimal, meminimalkan kelemahan, mereduksi ancaman, dan menciptakan peluang.

Bentuk Tren Perkembangan Ancaman Siber

Ancaman siber saat ini sudah terjadi di sejumlah infrastruktur kritis yang dimiliki oleh TNI. Hal tersebut ditunjukkan melalui

beberapa peristiwa diretasnya website yang dimiliki oleh TNI. Hal tersebut menjadi suatu permasalahan tersendiri dimana pimpinan TNI saat ini berupaya untuk meningkatkan efektifitas dan efisiensi di segala bidang tugas dengan menerapkan penggunaan teknologi informasi. Dalam konsep *pertahanan siber*, penggunaan teknologi informasi dimanfaatkan untuk mendukung kepentingan komando dan pengendalian antara pimpinan dengan bawahan atau komandan dengan anggotanya. *Komando dan pengendalian tersebut menjadi suatu hal yang sangat vital apalagi jika hal tersebut dihadapkan dalam suatu kondisi operasi atau pertempuran.* Berbagai satuan atau komponen yang ada di mandala operasi dapat saling terhubung secara langsung atau *real-time,* mulai dari tataran strategis, taktis hingga operasional dalam suatu sistem komando dan pengendalian operasi sehingga para Panglima atau para komandan pasukan dapat mengendalikan satuan-satuan yang ada di medan pertempuran. Ancaman siber dan serangan siber dapat merusak sistem komando dan pengendalian operasi bahkan sampai dengan tingkat melumpuhkan sistem tersebut sehingga berdampak besar bagi operasi yang dilaksanakan.

Ancaman siber sebagaimana yang telah disebutkan diatas menyerang hampir diseluruh aspek kehidupan berbangsa dan bernegara. Berbagai kejadian menunjukkan bahwa ancaman tersebut bersifat nyata dan setiap saat dapat mengancam siapapun khususnya institusi/Lembaga/organisasi bahkan perorangan yang tidak memiliki tingkat *security awareness* yang tinggi dalam mengantisipasi ancaman siber yang senantiasa berkembang dari waktu ke waktu. Adapun factor-faktor yang berpengaruh dalam pembahasan persoalan ini yaitu *Political, Economic, Social, Technological* dan *Legal.* Faktor-faktor ini memiliki suatu relasi atau hubungan antara permasalahan yang diteliti dari berbagai sudut pandang dalam bidang kehidupan yang terjadi di masyarakat. Hal tersebut sangat tepat jika dikaitkan untuk meneliti ancaman siber yang saat ini terjadi dan trend perkembangan ancaman siber di masa depan. Adapun penjelasan sebagai berikut:

1. Kebijakan politik. Kebijakan politik dari pemerintah suatu negara dimana hal tersebut terlihat dari ada atau tidaknya suatu peraturan atau regulasi yang mengatur tata kehidupan yang ada di masyarkat. Terkait dengan penelitian ini, peraturan atau regulasi yang dibutuhkan dalam hal perlindungan dalam penggunaan media internet yang ada. Di Indonesia saat ini telah ada peraturan perundang-undangan yang mengatur penggunaan media internet salah satunya yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang selanjutnya disempurnakan melalui revisi menjadi Undang-Undang Nomor 19 Tahun 2016. Peraturan perundang-undangan tersebut memuat sejumlah aturan termasuk didalamnya sanksi-sanksi pidana bagi pelanggar hukum UU ITE tersebut.
2. Ekonomi. Bidang ekonomi merupakan salah satu bidang dalam kehidupan masyarakat yang mengalami dampak dari serangan siber. Serangan siber yang terajdi di Indonesia mengakibatkan potensi kerugian ekonomi sebesar USD 34,2 (tiga puluh empat koma dua) miliar atau Rp 481 (empat ratus delapan puluh satu) triliun atau sekitar 3,7 (tiga koma tujuh) persen dari total pendapatan domestik bruto (PDB). Hak tersebut merupakan hasil studi yang dilakukan Frost dan Sullivan.
3. *Sosial.* Ancaman siber juga berpengaruh terhadap kehidupan sosial masyarakat. Menurut sebuah penelitian dari Digital GFK Asia yang dilakukan pada tahun 2016 sebagaimana yang dirilis oleh *Social Media Week*, perempuan Indonesia setidaknya menghabiskan waktu selama 5,6 jam per hari saat mengutak-utik layar *smartphone* mereka. Adapun pria Indonesia, setidaknya menghabiskan waktu selama 5,4 jam sehari dan membuka sekitar 47 (empat puluh tujuh) aplikasi atau alamat *website*. Secara rata-rata orang Indonesia menghabiskan waktu dengan *smartphone*-nya selama 5,5 jam sehari dan membuka 46 (empat puluh enam) aplikasi dan alamat *website*.
4. Teknologi. Kemajuan dan perkembangan teknologi komunikasi dan informasi membawa dampak bagi kehidupan masyrakat. Semenjak tahun 2005 semenjak ditemukannya sistem operasi Android maka era gadget dan

smartphone dimulai. Hal tersebut membuat internet semakin mudah untuk di akses. Saat ini selain sistem operasi Android juga dikenal sistem operasi IOS yang dibuat oleh perusahaan Apple. Kedua sistem operasi tersebut kini merajai kancah percaturan teknologi smartphone dunia. Berdasarkan data statistik yang dirilis oleh GSMA Intelligence, kelompok penelitian grup perdagangan layanan seluler GSMA, jumlah pengguna perangkat mobile di seluruh dunia telah berkembang menjadi kurang lebih 5 (lima) miliar, dengan 1 (satu) miliar pengguna terakhir ditambahkan hanya dalam empat tahun terakhir dimana hal itu berarti bahwa 5 (lima) miliar dari 7,5 (tujuh koma lima) miliar penduduk dunia sekarang menggunakan perangkat mobile mulai dari smartphone, tablet hingga ponsel.

Revolusi Industri 4.0 yang ditandai oleh beberapa indikator antara lain *Internet of Things, Big Data, Artificial Inteligent* dan lain sebagainya, memberikan kerawanan khususnya terhadap ancaman siber yang ada. Salah satu ancamannya yaitu spionase siber. Pada beberapa tahun terakhir negara-negara di berbagai belahan dunia terbuka wawasannya, dimana salah seorang mantan agen CIA (Edward Snowden) membocorkan beberapa rahasia yang sedang dilakukan oleh negara Amerika Serikat. *National Security Agency (NSA)* ternyata telah lama memulai aksi spionase siber keseluruh penjuru dunia melalui teknologi *Privacy in Mobile Information and Communicatian Systems (PRISMS)*. Teknologi tersebut mengumpulkan informasi yang dibutuhkan melalui *Facebook, Google* dan *Yahoo*. Hal tersebut dilakukan dengan motif melindungi negara Amerika Serikat dari ancaman teroris. Negara-negara lain yang memiliki kemampuan untuk melakukan spionase siber melalui produksi gadget maupun perangkat elektronik lainnya seperti drone, CCTV, Laptop dan lain sebagainya. Termasuk didalamnya yaitu melalui pemanfaatan operating system yang tertanam di sebuah computer sangat memungkinkan untuk melaksanakan spionase siber terhadap manusia yang ada di seluruh penjuru dunia.

Dari analisa yang telah dijelaskan diatas, maka didapat suatu hasil bahwa ancaman siber yang terjadi berakibat kepada seluruh aspek kehidupan berbangsa dan bernegara. Ancaman siber merupakan

suatu ancaman nyata yang merupakan dampak dari perkembangan teknologi komunikasi dan informasi. Keberadaan IT dewasa ini selain memberikan kemudahan juga sekaligus mengandung kerentanan apabila tidak disikapi secara bijak. Adapun trend ancaman siber kedepan sangat bergantung kepada kemajuan teknologi komunikasi dan informasi yang ada. Ancaman tersebut dapat berdimensi ideologi, politik,ekonomi, sosial budaya dan Hankam

Bentuk Sistem Pertahanan Semesta yang perlu dibangun dalam menghadapi ancaman siber

Keterpaduan antara teknologi telekomunikasi, internet, dan penyiaran, telah mendorong munculnya infrastruktur ekonomi baru yang disebut dengan Jaringan Broadband. Sisi lain yang amat perlu dipahami adalah bahwa saat jaringan broadband domestik tersambung dengan jaringan broadband global, seluruh aset nasional dapat menjadi terhubung ke jaringan global. Saat ini semakin banyak infrastruktur kritikal yang dimiliki oleh TNI bergantung pada teknologi komunikasi dan informasi sehingga menimbulkan kerawanan terhadap ancaman dan serangan siber. Kondisi sarana dan prasarana yang dimiliki Mabes TNI pada saat ini masih terbatas hanya pada penggunaan dan pemeliharaan TIK maupun sistem Kodal yang tersebar pada fungsi Infolahta, Pusdalops dan Satkomlek serta belum ada koherensi antar satu dengan yang lainnya.

Belum tersedianya peranti lunak sebagai pedoman dalam pelaksanaan kegiatan dan operasi siber dapat diatasi dengan memanfaatkan payung hukum dalam penyelengaraan Hanneg berupa Undang-undang Nomor 3 Tahun 2002 tentang Hanneg dan Undang-undang Nomor 34 Tahun 2004 tentang TNI serta Doktrin TNI sebagai landasan dalam pelaksanaan tugas sekaligus pedoman dalam penyelengaraan pertahanan siber. Dengan demikian, maka strategi pertama dalam mengembangkan bentuk Sistem Pertahanan Semesta dalam menghadapi ancaman siber adalah "Mewujudkan pedoman pelaksanaan kegiatan & operasi siber berupa landasan hukum, peraturan dan prosedur kerja melalui penyusunan aturan/regulasi dan tata kelola bidang siber dilingkungan TNI.

Peningkatan kualitas SDM sangat diperlukan dalam setiap organisasi. Terkait dengan penngkatan kemampuan SDM personel satuan siber TNI dapat dilakukan secara formal melalui pendidikan dan latihan yang diselenggarakan oleh Lembaga Pendidikan di lingkup TNI/Kemhan maupun melalui kursus secara swadaya satuan. Dengan demikian, maka strategi kedua dalam mengembangkan bentuk Sistem Pertahanan Semesta dalam menghadapi ancaman siber adalah "Mewujudkan SDM siber TNI yang profesional berdedikasi & memiliki etos kerja yang baik melalui pemenuhan personel baik dari segi kuantitas maupun kualitas, dgn cara rekrutmen, *assesment*, pembinaan karir & Diklat.

Organisasi Siber TNI saat ini memang dirasakan perlu adanya penguatan secara organisasi melalui validasi organisasi. Hal tersebut merupakan suatu hal yang dapat dilakukan untuk menjawab tugas yang diberikan oleh pimpinan TNI. Kemampuan siber di tingkat Mabes Angkatan pun akan menjadi prioritas melalui pembentukkan satuan siber di tingkat Mabes Angkatan. Kemampuan siber di tingkat TNI yang kuat dan tangguh akan berpengaruh langsung terhadap kemampuan pertahanan siber nasional. Dengan demikian, maka strategi ketiga dalam mengembangkan bentuk Sistem Pertahanan Semesta dalam menghadapi ancaman siber adalah "Mewujudkan organisasi siber yang proporsional, efektif & efisien mulai di tingkat Mabes TNI sampai dengan tingkat Mabes Angkatan, melalui penyusunan kajian validasi organisasi siber di tingkat Mabes TNI maupun penyusunan kajian pembentukan organisasi siber di tingkat Mabes Angkatan.

Perkembangan teknologi IT yang menjadi basis dalam penguasaan siber mutlak menjadi suatu peluang yang dapat mengatasi kelemahan yang ada. Saat ini beberapa industri bergerak di bidang IT baik BUMN maupun Swasta. Terbatasnya sarana dan prasarana yang ada dapat diatasi melalui perencanaan komprehensif dalam pengadaan materiil yang ada dengan memprioritaskan pemenuhan kebutuhan yang bersumber dari industri strategis dalam negeri. Dengan demikian, maka strategi keempat dalam mengembangkan bentuk Sistem Pertahanan Semesta dalam menghadapi ancaman siber adalah "Mewujudkan infrastruktur siber TNI yang

ideal melalui pembangunan dan pengembangan sarana dan prasarana siber TNI secara bertahap dalam rangka tercapainya ketahanan siber di lingkungan TNI.

Terbatasnya anggaran untuk mendukung pelaksanaan kegiatan dan operasi dapat diatasi dengan memanfaatkan Kerjasama baik berupa MoU maupun Perjanjian Kerjasama dibidang siber. MoU maupun perjanjian kerjasama terus senantiasa dijalani dalam rangka mewujudkan ketahanan siber di lingkup nasional dan TNI. Hal tersebut harus senantiasa dijalin dengan instansi/Lembaga/organisasi yang bergerak di bidang siber baik di dalam maupun luar negeri. Memanfaatkan forum kerjasama kawasan dalam rangka meningkatkan kemampuan organisasi siber yang ada.. Dengan demikian, maka strategi kelima dalam mengembangkan bentuk Sistem Pertahanan Semesta dalam menghadapi ancaman siber adalah "Mewujudkan keamanan dan ketahanan siber di lingkungan TNI melalui pelaksanaan kegiatan dan operasi siber termasuk kerjasama dengan Lembaga/institusi/organisasi terkait baik DN maupun LN.

Kesimpulan

Berdasarkan pokok-pokok hasil penelitian dan analisis pada bab-bab sebelumnya dapat disimpulkan beberapa hal sebagai berikut:

1. Ancaman Siber merupakan ancaman nyata yang saat ini menjadi pokok perhatian dari para stake holder tingkat nasional maupun di tingkat TNI. Berbagai peraturan dan kebijakan telah dikeluarkan dalam rangka mengantisipasi kemungkinan ancaman siber yang bakal terjadi. Salah satu bentuknya yaitu lahirnya Peraturan Presiden yang mendasari terbentuknya BSSN. Di lingkup TNI saat ini sudah terbentuk Satuan Siber TNI berdasarkan Peraturang Panglima TNI dimana satuan tersebut berkedudukan langsung dibawah Panglima TNI. Namun berdasarkan hakikat ancaman siber yang telah dirumuskan pada Permenhan No 82 Tahun 2014 maka terdapat beberapa ancaman siber yang perlu mendapatkan perlakuan khusus antara lain : Penyusupan siber (spionase siber) yang dapat menyerang sistem melalui

identifikasi pengguna yang sah dan parameter koneksi seperti *password*, melalui eksploitasi kerentanan yang ada pada sistem dan Penyalahgunaan Protokol Komunikasi yang tujuan akhirnya memungkinkan untuk melewati *firewall* dan mendirikan sebuah hubungan yang aman antara dua entitas, yaitu *hacker* dan *target*, sehingga dapat mengekploitasi sistem yang ada.

Kedua bentuk ancaman tersebut harus dapat diantisipasi salah satunya melalui penerapan standar keamanan informasi yang ada di setiap institusi TNI. Standarisasi tersebut harus dirumuskan oleh berbagai Lembaga/Instansi yang terkait dan penerapan terhadap standarisasi keamanan informasi tersebut di sahkan melalui Keputusan Presiden maupun keputusan Menteri atau Pimpinan Lembaga/Instansi/Kementrian/Lembaga Pemerintah. Standarisasi juga diperlukan dalam pemenuhan materiil/perangkat yang dibutuhkan dalam menjamin keamanan yang ada. Standarisasi tersebut harus dapat berlaku untuk semua Lembaga/instansi/organisasi yang ada dan juga dapat diintegrasikan khususnya untuk memudahkan memonitoring kerawanan-kerawanan yang mungkin saja terjadi.

2. Sistem Pertahanan Negara yang berdasarkan Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara menegaskan bahwa sistem pertahanan negara disusun berdasarkan hakekat ancaman yang terjadi. Dalam menghadapi ancaman militer maka diperlukan sistem pertahanan militer dimana TNI sebagai komponen utama dengan didukung oleh komponen pendukung dan komponen cadangan. Dalam menghadapi ancaman siber yang ada khususnya yang mengancaman kedaulatan negara dan keutuhan wilayah NKRI serta mengancam keselamatan seluruh bangsa dan negara maka TNI membentuk Satuan Siber TNI *sebagai leading sector* dalam membangun pertahanan siber dalam rangka mendukung sistem pertahanan militer. Hal tersebut tidak serta merta berlangsung dengan mulus sesuai dengan harapan dan keinginan dari pimpinan TNI. Beberapa kendala dan hambatan muncul dalam membangun pertahanan siber yang tangguh. Berbagai

strategi dapat dilakukan dalam rangka mengatasi hal tersebut dengan memanfaatkan peluang dan kekuatan dalam rangka mengatasi kelemahan dan ancaman siber yang datang dari dalam maupun dari luar negeri.

Daftar Pustaka

Buku

Andress, Jason and Steve Winterfield. 2011. Cyber Warfare, Techniques, Tactics and Tools for Security Practitioners. Elsiever, Inc.

Brooker, Paul. 2010. Modern Stateless Warfare. Palgrave Macmilan.

Carr, Jeffrey. 2010. Mapping The Cyber World Inside Cyber Warfare. O'Rieilly Media, Inc.

Carayannis, Elias G, David F.J Campbell and Marios P.E. 2014. *Cyber-Development, Cyber-Democray, and Cyber-Defense, Challenges, Opportunities and Implication for Theory, Policy and Practise.* Springer

Creative Industries Research Institute. (n.d). *S.W.O.T Analysis*. Product Brief Developments Tools: AUT University.

Creswell, John W. 2009. *Research Design, Qualitative, Qualitative, and Mixed Approaches*. Third Edition. Los Angeles: Sage Publication, Inc.

Czosseck, Christian and Kenneth Geers. 2009. The Virtual Battlefield: Perspectives on Cyberwarfare. IOS Press

David Hunger dan Thomas L. Wheelen. 2003. *Manajemen Strategi*, Yogyakarta.

Erbschloe, Michael. 2001. Information Warfare; How to Survive Cyber Attacks. Mc Graw Hill Companies.

Fomo, Richard and Ronald Baklarz. 1999. The Art of Information Warfare. Universal Publisher.

Garvalho, F.D. 2006. *Cyberwar-Netwar, Security in The Information Age.* IOS Press.

Giles, Lionel. 2008. *The Art of War Sun Tzu.* Pax Librorum Publishing House.

Halpin, Edwar, Phillipa Trevorrow, David Webb and Steve Wright. 2006. *Cyberwar, Netwar and The Revolution in Military Affairs*. Palgrave Macmilan.

Hart, Liddel, B.H. 1991. "The Theory of Strategy", dalam *Strategy: The Classic Book on Military Strategy*. London: Meridian Book.

International Group of Experts. 2013. *Tallin Manual on The International Law Applicable to Cyber Warfare.* Cambridge University Press.

Kasali, Rhenaldi. 2018. *Disruption*.PT Gramedia Pusaka Utama.

Knapp, Kenneth J. 2009. *Cyber Security and Global Information Assurance, Threat Analysis and Response Solutions.* IGI Global.

Kott, Alexander. 2008. Battle of Cognition, The Future Information Rich Warfare and The Mind of The Commander, Preager Security International.

Libicki, Marthin C. 2007. Conquest In Cyber Space, National Security and Information Warfare. Cambridge University Press.

Molander, Roger C, Andrew Riddile, Peter A. Wilson, Stephanie Williamson. *Strategic Information Warfare: A New Face of War.*

Moleong, Lexy J. 2014. *Metodologi Penelitian Kualitatif.* Bandung: PT Remaja Rosdakarya.

Nurmantyo, Gatot. 2016. *Memahami Ancaman, Menyadari Jati Diri sebagai Modal Membangun menuju Indoensia Emas*. Jakarta. Puspen TNI.

Poerwadarminta. W.J.S. 2003. *Kamus Umum Bahasa Indonesia*. Jakarta: Balai Pustaka.

Prilleltensky, Isaac and Ora Prilleltensky. 2006. *Promoting Well being, Linking Personal, Organizational and Community Change.* John Wiley & Sons, Inc.

Setiawan Hari Purnomo. 1996. *Manajemen Strategi: Sebuah Konsep Pengantar*, Jakarta: Fakultas Ekonomi Universitas Indonesia.

Skopik, Florian. 2018. *Collaborative Cyber Threat Intelligence, Detecting and Responding to Advanced Cyber Attacks at The National Level.* CRC Press Taylor and Prancis Group, LLC.

Sugiyono. 2014. *Metode Penelitian Kuantitatif, Kualitatif, dan Kombinasi (Mixed. Methods)*. Bandung: Alfabeta.

Tanuwidjaja, William. 2008. Buku "*101 Intisari Seni Perang Sun Tzu*".

Tippe, Syarifudin 2012. *Human Capital Management*, Jakarta: Pt. Elek Media Komputindo

Ulsch, Macdonnel. 2014. *Cyber Threat! How to Manage The Growing Risk of Cyber Attacks.* John Wiley & Sons, Inc.

Velez, Tony Uceda and Marco M. Morana. 2015. *Risk Centric Threat Modeling, Process for Attack Simulation and Threat Analysis.* John Wiley & Sons, Inc.

Waters, Garry. 2008. Australia and Cyberwarfare. Anu E. Press.

Peraturan

Undang - Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Undang - Undang Republik Indonesia Nomor 34 Tahun 2004 tentang TNI.

Peraturan Presiden Nomor 97 Tahun 2015 tentang Kebijakan Umum Pertahanan Negara Tahun 2015-2019.

Doktrin Tri Dharma Eka Karma Tahun 2017

Doktrin TNI AD Kartika Eka Paksi Tahun 2017

Doktrin Operasi Gabungan TNI Tahun 2013

Pedoman Strategis Pertahanan Nirmiliter, Kementerian Pertahanan Republik Indonesia, Jakarta, 2014.

Pedoman Pertahanan Siber, Kementeian Pertahanan Republik Indonesia,Jakarta, 2014.

Kemhan. 2010. *Minimum Essential Force Komponen Utama*. Jakarta: Direktorat Jenderal Strategi Pertahanan, Kementerian Pertahanan.

Jurnal

Chotimah, Chusnul Hidayat. 2015. *Membangun Pertahanan dan Keamanan Nasional dari Ancaman Cyber di Indonesia. Jurnal Diplomasi*.

Edmon Makarim, *Indonesian Legal Framework for Cybersecurity* http://www.nisc.go.jp/security-site/campaign/ajsympo/pdf/lecture2.pdf

Elvia, Marissa. 2018. *Peran Kepolisian dalam Penenaggulangan Tindak Pidana Penyebar Berita Bohong (Hoax)*. Jurnal Universitas Lampung.

Khanisa. 2013. Dilema Kebebasan Dunia Maya: Kajian Dari Sudut Pandang Negara.

Kurnia, Erwin. 2014. Sistem Pertahanan Negara berbasis teknologi informasi dalam mengantisipasi cyberwarfare.

Montratama, Ian dan Yanyan Mochammad pada tahun 2017 dengan judul " Bargaining: Revisi Teori Perimbangan Kekuatan dalam Hubungan Diplomasi

Indonesia, Malaysia, Cina dan Amerika Serikat"

Paresti, Awindtya. 2016. Negara Liliput Dalam Persoalan Digital: Upaya-Upaya Swiss Menghadapi Ancaman Keamanan Siber.

Praditya, Yosua. 2017. *Penggunaan Strategi Operasi Kontra Intelijen dalam rangka Menghadapi Ancaman Siber Nasional*. Jurnal Pertahanan dan Bela Negara.

Usmani, Amarmuazam. 2017. Analisis Penggunaan Media Siber Terhadap Keamanan Nasional : Suatu Studi di Malaysia.

Sthepen.M.W. 1985 *International Security* Vol-9 No.4 Spring.

Internet

https://ilmupengetahuan.org/sejarah-perkembangan-internet/, diakses pada tanggal 13 Mei 2018.

https://www.cnnindonesia.com/pilkadaserentak/nasional/20180703145756 32-311128/situs-kpu-diretas-serangan-hampir-tiap-menit?; diakses pada tanggal 7 Juli 2018

https://finance.detik.com/berita-ekonomi-bisnis/d-4063468/situs-resmi-diretas-ini-penjelasan-ditjen-pajak: diakses pada tanggal 7 Juli 2018

https://news.linuxsec.org/waduh-situs-ppid-tentara-nasional-indonesia-dijahili-hacker/;diakses pada tanggal 7 Juli 2018