PEMBENTUKAN TNI ANGKATAN SIBER DALAM PERSPEKTIF TEORI GEOMETRIPOLITISASI (MAZHAB INDONESIA) DAN SEKURITISASI (MAZHAB KOPENHAGEN) TERHADAP RUANG SIBER DI INDONESIA UNTUK MENGHADAPI PERANG SIBER GLOBAL

Adi Rio Arianto[1*], Gesti Anggraini[2]
[1]Departemen Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Pembangunan Nasional Veteran Jakarta
[2]Alumni Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Satya Negara Indonesia
Email: arianto.adirio@gmail.com[1], gestianggra92@gmail.com[2]

*Korespondensi: arianto.adirio@gmail.com

(Submission 23-01-2026, Revissions 27-02-2026, Accepted 27-02-2026)

Abstract

Law Number 3 of 2025 concerning Amendments to Law Number 34 of 2004 on the Indonesian National Armed Forces (TNI Law) focuses on adjusting the duties, functions, and structure of the TNI in response to the dynamics of modern defense threats (cyber and hybrid). This article examines the urgency of establishing a cyber army, namely the Indonesian National Armed Forces Cyber Force, from the perspective of the theory of Geometripolitization and the securitization of cyberspace. This study employs a qualitative approach using a literature review method and conducts a comparative analysis of the theory of Geometripolitics/Geometripolitization through the lens of the Indonesian School of World Relations, specifically "Manunggalisme," and the Securitization approach of the Copenhagen School. The findings indicate that the transformation of global cyber warfare in the 21st century has created a new battlefield in cyberspace; Indonesia's cyber securitization is carried out by framing the complexity of Global Cyber Warfare as a national threat; Indonesia's cyber geometripolitization is conducted by linking balance, power, and security to realize the role of a Cyber Army, which has the potential to become the TNI Cyber Force; and Indonesia must respond to 21st century Global Cyber Warfare by advocating for the establishment of the TNI Cyber Force under the legal framework of Law No. 3 of 2025 concerning Amendments to Law Number 34 of 2004 on the Indonesian National Armed Forces.

***Keywords*:** *Indonesian National Cyber Forces; Geometripolitization, Securitization; Cyber Defence; Global Cyber Warfare.*

Abstrak

Undang-Undang Nomor 3 Tahun 2025 tentang Perubahan Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (UU TNI) berfokus pada penyesuaian tugas, fungsi, dan struktur TNI menghadapi dinamika ancaman pertahanan modern (siber dan hibrida). Artikel ini mengkaji urgensi pembentukan tentara siber, yaitu TNI Angkatan Siber dalam perspektif teori Geometripolitisasi dan sekuritisasi ruang siber. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi pustaka dan melakukan analisis komparatif teori Geometripolitika/Geometripolitisasi pendekatan Mazhab Indonesia (*Indonesian School of World Relations*) "Manunggalisme" dan Sekuritisasi pendekatan Mazhab Kopenhagen (*Copenhagen School*). Hasil kajian menunjukkan bahwa transformasi perang siber global Abad 21 menciptakan medan tempur baru di ruang siber; Sekuritisasi siber Indonesia dilakukan dengan cara membingkai kompleksitas Perang Siber Global sebagai salah satu ancaman nasional; Geometripolitisasi siber Indonesia dilakukan dengan cara menghubungkan keseimbangan, kekuatan, dan keamanan untuk meraih peran Tentara Siber yang berpotensi menjadi TNI Angkatan Siber; dan Indonesia harus merespon Perang Siber Global abad ke-21 dengan cara mewacanakan pembentukan TNI Angkatan Siber di bawah payung hukum UU No. 3 Tahun 2025 tentang Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia.

Kata Kunci: TNI Angkatan Siber; Geometripolitisasi; Sekuritisasi; Pertahanan Siber; Perang Siber Global.

PENDAHULUAN

Pembentukan Tentara Siber Indonesia menjadi wacana yang menguat pada periode awal pemerintahan Prabowo Subianto. Setelah Undang-Undang No. 3 Tahun 2025 tentang Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (UU TNI) disahkan pada bulan Maret 2025, pembentukan TNI Angkatan Siber yang semula berada di tataran akademik, mulai beralih pada tataran kebijakan pemerintah Indonesia. Perubahan UU TNI ini sendiri berfokus pada penyesuaian tugas, fungsi, dan struktur TNI menghadapi dinamika ancaman pertahanan modern, memperkuat peran TNI dalam pertahanan negara, serta mengatur penempatan prajurit dan batas usia pensiun.

Tulisan ini ditujukan untuk mendalami fungsi dan struktur TNI dalam menghadapi dinamika ancaman pertahanan modern, yang di dalamnya termasuk ancaman siber, ancaman hibrida, hingga ancaman geometri. Dalam artikel berjudul "*Building Indonesia National Cyber Defense and Security to Face the Global Cyber Threats Through Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII)" pada *Jurnal Pertahanan dan Bela Negara* tahun 2019, penulis telah mendiskusikan gagasan pembentukan TNI Angkatan Siber setelah pemerintah membentuk Badan Siber dan Sandi Negara (BSSN) tahun 2017, yang sekaligus mengambil alih dan memperkuat fungsi-fungsi terhadap keamanan siber yang telah dijalankan oleh *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII).

Dalam artikel tersebut, penulis merekomendasikan pembentukan Pasukan Siber atau Tentara Siber dalam bentuk TNI Angkatan Siber sebagai pelengkap dari Angkatan Darat, Angkatan Laut, dan Angkatan Udara untuk memperkuat BSSN mencegah ancaman di ruang siber global. Alasan pentingnya, jika dilihat dari variasi aktor, motif, dan targetnya, ancaman ruang siber di Indonesia sangat kompleks. Karena itu, Angkatan Siber diharapkan dapat menjadi bagian dari formasi struktural di tubuh TNI dengan mengembangkan strategi nasional dalam membangun keamanan siber di Indonesia ke depan. Selain itu, Angkatan Siber diperlukan untuk menyelesaikan dan mendukung perkembangan teknologi informasi yang tidak hanya di ranah militer (Geometrik Militer), tetapi juga menjangkau ranah sipil (Geometrik Sipil) dalam membangun keamanan siber nasional untuk mencegah potensi dan ancaman perang siber global.

Penulis menilai bahwa ruang siber Indonesia menghadapi kompleksitas berkenaan dengan fungsionalisme ruang siber, baik untuk membangun kekuatan (*geometripolitisasi*) maupun untuk menghindari ancaman (*sekuritisasi*). Dalam studi Geometripolitika, fungsionalisme ruang siber berada dalam dua domain: *Pertama*, fungsionalisme ruang siber untuk tujuan strategis atau politik tingkat tinggi (Geometrik Militer) berupa formulasi dan aktivasi kekuasaan ruang siber yang berkaitan dengan menghadapi Perang Siber Global (PSG) atau Perang Mayantara Global (PMG), Perang Geometri Antarbangsa (PGA), dan kompleksitas terbentuknya Negara Mayantara (Kedaulatan Mayantara) atau pemerintahan di ruang siber. *Kedua*, fungsionalisme ruang siber untuk tujuan non-strategis atau politik tingkat normal (Geometrik Sipil) berupa perlindungan aktivitas sipil di dunia maya (ruang siber).

Pada tahun 2007, melalui Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet yang kemudian direvisi dengan Peraturan Menteri Komunikasi dan Informatika No. 16/PER/M.KOMINFO/10/ 2010, dan diperbaharui lagi dengan Peraturan Menteri Komunikasi dan Informatika No. 29 /PER/M.KOMINFO/12/ 2010 dibentuklah *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII). ID-SIRTII merupakan tim yang ditugaskan Menteri Komunikasi dan Informatika (Kominfo) untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. Tugas dan fungsi dari ID-SIRTII diantaranya melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan gangguan pada jaringan, berkoordinasi dengan pihak-pihak terkiat di dalam maupun luar negeri dalam menjalankan tugas pengamanan jaringan telekomunikasi berbasis protokol internet, mengoperasikan, memelihara dan

mengembangkan sistem database sistem ID-SIRTII, menyusun katalog-katalog dan silabus yang berkaitan dengan proses pengamanan pemanfaatan jaringan, memberikan layanan informasi atas ancaman dan gangguan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet, menjadi *contact point* dengan lembaga terkait tentang keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet serta menyusun program kerja dalam rangka melaksanakan pekerjaan keamanan jaringan telekomunikasi yang berbasis protokol internet (Kementerian Komunikasi dan Informatika RI, 2010).

Dalam konteks dua domain studi Geometripolitisasi, maka implementasi kebijakan ID-SIRTII/CC harus terintegrasi dengan peran strategis institusi-institusi siber nasional untuk mencegah kejahatan di ruang siber. Sementara untuk menghadapi Ancaman Siber Global, implementasi kebijakan ID-SIRTII/CC harus terintegrasi dengan institusi-institusi siber regional dan global; dan ke depannya – berangkat dari "fungsionalisme ruang siber" dan untuk menciptakan suatu strukturalisme Pertahanan dan Keamanan di ruang siber nasional Indonesia (Hankam Mayantara)—sudah saatnya Indonesia membentuk TNI Angkatan Siber/Mayantara (TNI AS/M) di dalam struktur Kementerian Pertahanan RI sebagai pelengkap dari TNI Angkatan Darat (TNI AD), TNI Agkatan Laut (TNI AL), dan TNI Angkatan Udara (TNI AU). Dalam menjalankan fungsinya, TNI AS/M ini dapat melibatkan BSSN sebagai pengganti ID-SIRTII/CC.

Dengan melihat kemajuan teknologi siber di seluruh dunia, Indonesia merupakan salah satu aktor paling penting dalam tata lalu lintas informasi siber masa depan. Saat ini Indonesia berada di posisi pertama negara berpotensi menjadi target *hacker*, menggantikan Tiongkok. Dengan hadirnya fungsionalisme ruang siber sebagai arena kompleks hubungan dunia dan keamanan dunia, Indonesia perlu mempersiapkan agenda besar guna mendukung pertahanan dan keamanan siber nasional untuk mencegah ancaman siber global, baik di sektor sipil dan sektor militer. Dengan dibentuknya BSSN, Indonesia telah merespon kompleksitas ruang siber sesuai dengan ketersediaan sumber daya manusia dan pendukung teknologi pertahanan siber. Namun demikian, penulis menilai bahwa ke depan, lembaga ini dapat mendorong terbentuknya suatu TNI Angkatan Siber/Mayantara (TNI AS/M) di bawah struktur Kementerian Pertahanan RI. Dalam pelaksanaan fungsinya, TNI AS/M ini tetap melibatkan peran strategis seperti yang pernah dimiliki oleh ID-SIRTII/CC, yang sejak tahun 2017 peran strategisnya telah diambil alih oleh BSSN.

Artikel ini berusaha menjelaskan pentingnya bagi Indonesia untuk membentuk tentara siber, dalam bentuk TNI Angkatan Siber dalam perspektif teori geometripolitisasi dan sekuritisasi ruang siber. Ada empat argumen yang hendak dikaji terkait urgensi pembentukan tentara siber tersebut, yaitu: transformasi Perang Siber Global Abad 21, sekuritisasi siber Indonesia terhadap kompleksitas Perang Siber Global, Geometripolitisasi Siber Indonesia terhadap pembentukan TNI Angkatan Siber, dan perlunya Indonesia merespon Perang Siber Global Abad Ke-21.

KAJIAN TEORI

Geometripolitisasi adalah pemikiran teoritik yang dipelopori oleh Mazhab Indonesia (*Indonesian School of World Relations*) dengan konsep inti "Manunggalisme". Adapun sekuritisasi, adalah pemikiran yang dipelopori oleh Mazhab Kopenhagen (*Copenhagen School*). Teori Geometripolitika dalam pembahasan ini digunakan untuk menjelaskan dilema tata kelola informasi di ruang siber dan teknologi aksesnya. Dilema tersebut berkaitan dengan transformasi ancaman abad ke-21 yang disebabkan oleh pemanfaatan ruang siber sebagai ruang yang berisi ancaman (*sekuritisasi* ruang siber), tetapi di sisi lain pemanfaatan ruang siber juga dapat menciptakan suatu keseimbangan, kekuatan, dan keamanan (*geometripolitisasi* ruang siber) sebagai respon sekaligus mencegah manusia dari dampak berbagai bentuk ancaman siber.

Dalam dunia informasi, secara makro terdapat hubungan yang sangat strategis antara "keseimbangan", "kekuatan", dan "keamanan" terhadap wilayah yang kemudian disebut dengan "matra" atau "medan" yang berkaitan dengan informasi. Proses pembentukan kekuasaan di ruang siber ini kemudian disebut dengan istilah "geometrik" (Arianto, 2017). Dalam teori Geometripolitik, pembentukan kekuasan telah melampaui tahap kekuasaan metapolitik, politik, geopolitik, dan astropolitik. Dulu, kekuasaan dibentuk melalui metapolitik dan juga politik. Seiring dengan waktu, kekuasaan juga dapat dibentuk melalui geopolitik dan Astropolitik. Dan kini berujung pada

Geometripolitik yang menggabungkan seluruhnya sehingga membentuk "Keamanan Dunia Basis Kelima" (*Fifth Base World Security*).

Geopolitik berusaha mengembangkan kekuasaan material dengan mengoptimalkan fungsi ruang "geografi" secara fisik untuk memperluas kekuasaan. Sementara astropolitik berusaha mengembangkan kekuasaan di ruang angkasa. Namun, dengan berkembangnya ruang lingkup keamanan, ancaman pun ikut berkembang sejalan dengan kemajuan teknologi. Dari sini lahir teori Geometripolitika sebagai tahap yang memetakan secara rinci hubungan antara keseimbangan, kekuatan, dan keamanan di berbagai sektor.

Teori Geometripolitika mendefinisikan ruang siber sebagai *matra* maya berbentuk geometris dan tidak terbatas yang berisi sekumpulan *mahadata* elektronik yang tersimpan dan terhubung oleh *netika* atau jaringan komputerik dan sibernetik yang dalam fungsionalismenya (pengguna) membentuk kuasa (dominasi) atas pembuatan, penghilangan, distribusi, kecepatan, percepatan, perlambatan, variasi, dan volume data. Adapun, keamanan siber berusaha untuk menciptakan situasi dimana aktor siber berada dalam kondisi aman, termasuk terdapatnya perlindungan terhadap lingkungan (*matra*), organisasi dan infrastruktur (*netika*), aset (*mahadata*), aktor siber (*pengguna*), dan dominasi atas informasi di dunia maya (*kuasa*) (Arianto dan Anggraini, 2019).

Siber dikatakan bersifat geometris karena keberadaanya tidak dapat diraba oleh fisik, namun efeknya dapat membentuk pandangan tertentu terhadap suatu objek. Dengan istilah lain, siber adalah fatamorgana dari objek yang sesungguhnya. Sedangkan makna ruang siber menurut Cavelty, adalah sebuah arena dimana semua jaringan komunikasi, data, sumber, dan pengguna informasi melebur dalam sebuah dimensi elektronik yang berinteraksi dengan kecepatan, sangat tinggi, beragam, dan dalam volume yang sangat besar (Cavelty, 2013).

Geometripolitika memperluas basis "kekuasaan" menjadi lima basis, yaitu: basis fisik (material), metafisik (metafisikal), psikologik (psikologikal), ideasionik (ideasional), dan geometrik (geometrikal). Dengan demikian, telah terjadi transformasi ancaman akibat bergesernya sifat keamanan yang tadinya hanya berkutat pada dunia material, metafisikal, dan psikologikal, bertambah dengan hadirnya ancaman dari dunia maya yang bersifat ideasionik dan geometrikal. Inilah yang oleh Mazhab Indonesia disebut sebagai "Keamanan Dunia Basis Kelima" atau "*Fifth Base World Security*" (Arianto dan Anggraini, 2023).

Transformasi ancaman ini berkembang seiring dengan berkembangnya ruang lingkup, karakter, dan matra atau medan keamanan yang termuat dalam teori Geometripolitika. Dalam Geometripolitika, siber menjadi satu dari delapan medan kemanan dunia (darat, laut, udara, bawah tanah, siber, ruang hampa, khatulistiwa, dan galaksi) yang mendominasi ancaman abad ke-21. Dalam teori Geometripolitika, lingkungan strategik abad ke-21 menjadi bagian dari Era *Manunggalian*, dimana keamanan informasi menjadi sangat sulit dikendalikan yang berefek pada ancaman perang siber, perang biologi, dan perang nuklir (Arianto, 2016). Inilah yang disebut dengan Perang Geometri Antarbangsa akibat dari sulitnya mendeteksi informasi yang berujung pada "Paradoks informasi."

Paradoks informasi adalah melimpahnya informasi dan sumber informasi di ruang siber yang memicu arus balik informasi, akibatnya informasi tersebut menjadi tidak efektif dan menciptakan serangan balik terhadap informan sehingga berdampak pada kendali taktis atas respon yang dihasilkan oleh ancaman tidak terduga dari ruang siber. Oleh karena itu, siapapun yang tidak cakap menggunakan informasi dengan baik, akan menjadi sumber ancaman. Oleh karena itu, Geometripolitisasi ruang siber menjadi sangat krusial.

Dalam kajian berjudul *Manunggalism: Paradigm, Philosophy, and Theory to View the World Relations (WR) Belong to Indonesian School (Mazhab Indonesia) in Manunggalian Era 21st Century,* penulis merumuskan geometripolitisasi sebagai pendekatan Mazhab Indonesia sebagai berikut:

> *Geometripolitization is a process of making something that initially has no value of balance, power, and security by changing its function or increasing its function into a force to create conditions of securing and controlling something (in world-nations and also world-states) by dispelling threats or force attacks from the intended or targeted party* (Arianto dan Anggraini, 2023).

Dalam konteks ini, Geometripolitisasi adalah proses menjadikan sesuatu yang awalnya tidak memiliki nilai keseimbangan, kekuatan, dan keamanan dengan mengubah fungsinya atau meningkatkan fungsinya menjadi kekuatan untuk menciptakan kondisi pengamanan dan pengendalian sesuatu (di

lingkup bangsa-dunia dan negara-bangsa) dengan menghilangkan ancaman atau serangan paksa dari pihak yang dituju atau ditargetkan. Pada akhirnya, Geometripolitisasi ruang siber menjadi sangat penting untuk membentuk keseimbangan, kekuatan, dan keamanan.

Dalam Geometripolitika, siber menjadi satu dari delapan medan kemanan dunia (darat, laut, udara, bawah tanah, siber, ruang hampa, katulistiwa, dan galaksi) yang mendominasi ancaman abad ke-21. Selanjutnya, ancaman abad ke-21 dianggap *intangible* (tidak terlihat) seperti ancaman ideologi berupa terorisme dan radikalisme yang berimplikasi pada stabilitas keamanan nasional khususnya di Indonesia (Indrawan dan Efriza, 2017). Ancaman *intangible* beririsan dengan ancaman siber karena sama-sama tidak bisa diraba oleh fisik, namun efeknya bisa dirasakan. Sebagimana yang ditekankan oleh Brascomb bahwa informasi di ruang siber berfungsi layaknya aliran darah bagi tubuh manusia (Brascomb, 1986).

Adapun teori Sekuritisasi yang dirumuskan Barry Buzan berfokusi pada usaha untuk melihat masalah keamanan sebagai hasil konstruksi. Artinya, suatu isu menjadi sebuah masalah keamanan karena adanya *discourse content* yang setidaknya memberikan pengaruh, ditambah lagi terdapat aktor-aktor yang mewacanakannya dengan mengatakan bahwa isu tersebut merupakan ancaman eksistensi bagi suatu entitas. Suatu isu menjadi masalah keamanan karena hasil promosi para aktor karena pengaruh konstruktif diskursif antar aktor dan audiens. Aktor mewacanakan dan audiens menyetujui (Polii, 2017).

Pada dasarnya, sekuritisasi dipahami sebagai proses politik untuk menjadikan suatu masalah atau isu yang semula bukan masalah atau isu menjadi sebuah masalah keamanan dengan cara melihat isu atau masalah tersebut dari sisi *security* sehingga isu atau masalah tersebut dijadikan agenda nasional suatu negara. Konsep sekuritisasi sendiri merupakan konsep baru yang relevan dengan *power of idea*, yang dipahami sebagai kemampuan untuk memproduksi ide dan menghasilkan sebuah discourse untuk mempengaruhi pihak lain (Polii, 2017). Sekuritisasi merupakan proses konstruktif untuk mengkategorikan masalah sebagai hasil dalam perubahan cara mengatasinya. Melalui tanda "keamanan", masalah diubah menjadi ancaman penting yang membutuhkan penanganan darurat yang luar biasa (Polii, 2017).

Berdasar pada pemikir *Copenhagen School*, proses sekuritisasi dapat dipahami melalui beberapa elemen utama yang menjelaskan bagaimana suatu isu diangkat menjadi ancaman keamanan. Elemen-elemen tersebut mencakup *securitizing actor, speech act, existential threat, audience, referent object,* dan *survival* (Buzan, 1998). *Securitizing actor* mengacu pada pihak yang mendorong terjadinya proses sekuritisasi aktor yang menyebarluaskan dan membingkai isu tertentu melalui *speech act*, yaitu sebuah tindakan wacana yang menekankan keberadaan *existential threat* atau ancaman eksistensial. Wacana tersebut disampaikan kepada *audience*, yaitu kelompok atau pihak yang perlu diyakinkan bahwa ancaman tersebut nyata dan mendesak. Ketika *audience* menerima narasi ancaman tersebut, maka perhatian terhadap *referent object* yaitu pihak atau nilai yang dianggap terancam meningkat secara signifikan. Melalui konstruksi urgensi dan ancaman terhadap *survival referent object* inilah tindakan-tindakan luar biasa atau non-rutin dapat dibenarkan dalam rangka mengatasi ancaman yang dinilai sebagai eksistensial (Listya, 2011).

Pendekatan *speech-act* terhadap keamanan mengharuskan adanya perbedaan di antara tiga jenis unit yang terlibat dalam analisis keamanan. Pertama adalah *referent object*, yaitu hal-hal yang dianggap terancam secara eksistensial dan memiliki klaim yang sah atas kelangsungan hidup. Kedua, *securitizing actors*: aktor yang melakukan tindakan sekuritisasi dengan menyatakan sesuatu—*referent object*—sebagai terancam secara eksistensial, sebagai aktor yang menginterpretasikan ancaman serius terhadap keamanan negara. Ketiga, *functional actors, yaitu* aktor yang mempengaruhi dinamika suatu sektor tanpa menjadi *referent object* maupun aktor yang menyerukan keamanan atas nama *referent object*, aktor ini secara signifikan mempengaruhi keputusan dalam bidang keamanan.

METODE

Penelitian ini menggunakan pendekatan kualitatif. Bogdan dan Taylor mendefinisikan pendekatan kualitatif sebagai "prosedur penelitian yang menghasilkan data deskriptif dalam bentuk kata-kata tertulis atau lisan dari narasumber dan perilaku yang dapat diamati (Bogdan dan Taylor 2004). Sementara itu, metode kualitatif, menurut Cassel dan Simon, adalah metode penelitian ilmu sosial yang

mencoba untuk secara akurat menggambarkan dan menafsirkan makna tertentu yang terjadi dalam konteks sosial (Cassel dan Simon 2004).

Adapaun, analisis komparatif kualitatif adalah teknik analitik yang awalnya berfokus pada sampel kecil, tetapi pengembangan lebih lanjut memungkinkan penerapannya pada konteks yang lebih luas (Ragin, 1987; Ragin, 2000). Analisis komparatif melibatkan pemeriksaan persamaan dan perbedaan unit, proses, atau fenomena di berbagai tempat, periode waktu, atau tingkat analisis. Ini adalah metodologi yang digunakan untuk mengembangkan teori, menguji hipotesis, dan mengidentifikasi pola kausal dengan membandingkan dan membedakan berbagai kasus dan data.

Untuk memahami mengapa Indonesia perlu merespon ancaman perang siber global, metode dalam tulisan ini berusaha menjelaskan secara eksplanatif tentang bagaimana Indonesia melakukan geometripolitisasi dan sekuritisasi ruang siber untuk membentuk tentara siber dalam bentuk TNI Angkatan Siber**.** Tulisan ini menggunakan metode telaah pustaka dengan mengumpulkan dan menganalisis literatur spesifik dengan menghubungkan waktu, konteks, dan peristiwa. Sehingga penulis dapat membuat pemilahan, perbandingan, dan menarik kesimpulan dengan cermat.

Adapun teori yang digunakan dalam analisis tulisan ini adalah Geometripolitisasi yang dipelopori oleh Mazhab Indonesia (*Indonesian School of World Relations*) dalam hal ini "Manunggalisme" dan Sekuritisasi yang dipelopori oleh Mazhab Kopenhagen (*Copenhagen School*). Penjelasan lebih cermat mengenai perbandingan kedua teori ini dapat diringkas dalam Tabel 1 berikut:

Table 1. Geometripolitisasi Pendekatan Mazhab Indonesia (*Indonesian School of World Relations*) vs. Sekuritisasi Pendekatan Mazhab Kopenhagen (*Copenhagen School*)

Kategori	Geometripolitisasi (Mazhab Indonesia)	Sekuritisasi (Mazhab Kopenhagen)
Ide Dasar	Geometripolitisasi adalah proses menjadikan sesuatu yang awalnya tidak memiliki nilai keseimbangan, kekuatan, dan keamanan dengan mengubah fungsinya atau meningkatkan fungsinya menjadi kekuatan untuk menciptakan kondisi pengamanan dan pengendalian sesuatu (di lingkup bangsa-dunia dan negara-bangsa) dengan menghilangkan ancaman atau serangan paksa dari pihak yang dituju atau ditargetkan.	Sekuritisasi adalah suatu proses politik untuk menjadikan suatu masalah atau isu yang semula bukan masalah atau ancaman menjadi sebuah masalah keamanan dengan cara melihat isu atau masalah tersebut dari sisi *security,* sehingga isu atau masalah tersebut dijadikan agenda nasional suatu negara untuk menghalau ancaman tersebut sesuai dengan hasil pembingkaian ancamannya.
Fokus Utama	Menekankan dimensi spasial atas eskalasi kekuasaan dan bagaimana kendali atas entitas-entitas membantu para aktor mencapai tujuan.	Menekankan konstruksi sosial untuk penerimaan publik terhadap ancaman yang dinyatakan, yang kemudian melegitimasi penggunaan kekuasaan luar biasa.
Basis Teoritis	Berangkat dari Teori Geometripolitika, sebuah gagasan teoretis yang dipelopori oleh Mazhab Indonesia (*Indonesian School of World Relations*): Manunggalisme.	Teori utama yang dipelopori oleh Mazhab Kopenhagen yang mendefinisikan ulang keamanan dari Perspektif Konstruktivis.
Sumber Daya	Didasarkan pada kemampuan mengendalikan ruang fisikal, metafisikal, psikologikal, ideasional, dan geometrikal sebagai pembentuk keamanan.	Didasarkan pada kemampuan mengendalikan ancaman sosial yang dikonstruksikan melalui bahasa dan praktik sebagai pembentuk keamanan.
Mekanisme	Menghubungkan keseimbangan, kekuatan, dan keamanan melalui pemanfaatan 8 matra "ruang dunia" (darat, laut, udara, bawah tanah, galaksi, ruang hampa, khatulistiwa, dan siber).	Membingkai sebuah ancaman potensial menjadi ancaman eksistensial terhadap "objek rujukan" (misalnya, negara, lingkungan, masyarakat).
Tujuan Akhir	membentuk keseimbangan, kekuatan, dan keamanan dari berbagai situasi	Membentuk ancaman yang dikontruksikan secara sadar
Dampak	Sumber daya menjadi melimpah untuk menghalau ancaman spesifik: Semua jadi kekuatan untuk melawan satu ancaman.	Sumber daya menjadi terbatas untuk menghalau ancaman tertentu: semua jadi ancaman untuk memperkuat keamanan

PEMBAHASAN

- **Peperangan Siber Abad Ke-21**

Hadirnya internet menyebabkan manusia terintegrasi dengan komunikasi dan informasi. Internet telah menyebabkan satu lompatan besar dalam kehidupan. Internet tidak bebas nilai, oleh karena itu Siber pun tidak bebas nilai saat bersentuhan dengan politik yang berujung pada pembentukan kekuasaan. Teknologi akan menjadi efektif jika kita memberi perhatian pada kegunaan dari teknologi yang disesuaikan dengan nilai-nilai sosial maupun pribadi serta adanya peraturan pemerintah yang melindungi masyarakat dari dampak negatif yang ditimbulkannya.

Geometripolitika menemukan hubungan strategis antara keseimbangan, kekuatan, dan keamanan terhadap wilayah, informasi, dan proses pembentukan kekuasaan melampaui Metapolitik, Politik, Geopolitik, dan Astropolitik (Salam, Arianto, dan Hikmawan, 2017; Arianto, 2017). Sedangkan istilah telematika dikenal sebagai "*the new hybrid of technology*" yang muncul karena perkembangan teknologi digital yang membuat perkembangan teknologi telekomunikasi dan informatika semakin terpadu atau yang biasa disebut dengan konvergensi. Konvergensi antara teknologi telekomunikasi, media dan informatika tersebut akhirnya mendorong penyelenggaraan sistem elektronik berbasis teknologi digital yang kemudian dikenal dengan istilah "*the net*." Konvergensi itu sendiri merupakan gejala yang mengemuka dalam industri jasa Teknologi Informasi Komunikasi (TIK) yang muncul sejalan dengan pesatnya kemajuan teknologi elektronika pada akhir abad 20.

Dampak konvergensi secara sosial telah dirasakan positif maupun negatifnya (BPPT, 2007). Salah satu dampak negatif yang muncul dalam ruang siber adalah terjadinya kejahatan siber. Maraknya kejahatan siber memerlukan perhatian dalam mengembangkan Keamanan Siber bagi sebuah negara. Perkembangan selanjutnya, para praktisi menyebut media dalam telematika tersebut dengan istilah multimedia. Sementara seiring dengan pemakaian jaringan sistem komputer yang mengunakan infrastruktur sistem telekomunikasi, masyarakat penggunanya kemudian seolah-olah mendapati dunia baru yang dinamakan ruang siber (Sanusi, 2005). Ruang siber adalah tempat maya dimana komunikasi terjadi. Istilah ruang siber, menurut novelis sains-fiksi William Gibson dalam bukunya "*Neuromancer*" adalah ruang integrasi antar komputer dengan manusia (Vivian, 2008).

Di sinilah Mazhab Indonesia sebagai suatu pendekatan menilai ruang siber sebagai suatu medan peperangan, oleh karenanya krusial untuk ditelaah. Dalam pendekatannya, Mazhab Indonesia merumuskan adanya dua domain untuk memahami penggunaan siber, yaitu pemanfaatan siber untuk tujuan sipil (Geometrik Sipil) dan militer (Geometrik Militer). Pemanfaatan siber untuk tujuan Geometrik Sipil adalah pemanfaatan siber yang tujuan utamanya difungsikan untuk memperluas (*wide*), mempercepat (*speed)*, dan mengefektifkan (*effective*) terhadap sutau penyebaran informasi di sector atau isu-isu sipil (non-militer). Sedangkan pemanfaatan siber untuk tujuan Geometrik Militer adalah pemanfaatan siber untuk tujuan perang di dunia maya yang dikendalikan oleh pasukan siber. Inilah yang disebut dengan perang siber atau "*cyber* war".

Jika menilik ke konflik dalam bentuk "perang siber" tingkat tinggi (*high politic in using of siber*), sudah banyak contoh yang membuktikan betapa posisi siber sangatlah strategis. Alvin & Heidi Toffler dalam *"War and Anti War"* menyebutkan bahwa abad ke-21 adalah abad perang gelombang ke-3 *(the third wave war)*, yaitu perang dengan penggunaan teknologi perang tingkat tinggi yang terintegrasi dengan komputer. Pernahkah kita membayangkan bagaimana jika secara tiba-tiba negara kita lumpuh padahal tidak ada invasi pengerahan tentara secara fisik baik dari negara luar maupun teroris? Atau ketika sistem perbankan lumpuh, bursa efek macet, listrik padam, air bersih terhambat, dan seterusnya. Serangan terhadap sistem perbankan nasional, kelistrikan dan distribusi air yang terintegrasi secara online, bisa melumpuhkan suatu negara. Inilah yang dinamakan sebagai serangan siber *(cyber attack)*.

Serangan siber terhadap suatu sistem yang terintegrasi secara *computerized* ini kian marak beberapa tahun belakangan ini. Sebelum Rusia melancarkan serangan fisik dengan operasi militer ke Ukraina, misalnya, mereka menyerang terlebih dahulu keamanan sistem siber Ukraina melalui para *hacker.* Serangan siber juga terjadi di Korea Selatan. Koneksi internet Korea Selatan diputus selama 20 hari disebabkan adanya serangan dari *hackers* sehingga mengacaukan roda perekonomian, bursa saham, hingga distribusi energi dan pangan. Serangan siber seperti ini telah mengakibatkan suatu kondisi yang cukup merugikan kehidupan manusia. Kita tentu masih ingat bagaimana daya rusak akibat dari serangan virus *worm Stuxnet* yang melumpuhkan pembangkit nuklir Bushehr, Iran tahun 2010.

Beberapa ahli komputer mengatakan canggihnya virus tersebut hanya bisa dilakukan oleh negara (*state actor*).

Serangan siber juga pernah melanda negeri Paman Sam, tepatnya terhadap Pusat Komando AS tahun 2008. Sebuah USB flash drive asing disisipkan ke salah satu laptop di sebuah markas militer AS di Timur Tengah. Flash disk yang mengandung konten berbahaya tersebut dikembangkan oleh intelijen asing yang kemudian menyebar melalui sistem komputer Departemen Pertahanan AS sehingga menyebabkan pencurian data ke server asing. Serangan siber ini juga terjadi di Georgia pada tahun 2008 yang berawal dari konflik Rusia dan Georgia di Ossetia Selatan. Setelah Georgia menyerang Ossetia Selatan, serangan cyber melumpuhkan situs-situs pemerintah Georgia serta situs-situs media lokal lainnya. Serangan ini serupa dengan serangan ke Estonia pada 2007 yang menghadapi gelombang serangan siber yang melanda segenap infrastruktur internet, mulai dari situs pemerintahan, perbankan, hingga situs media lokal. Serangan ini melumpuhkan sistem pemerintahan Estonia.

Serangan-serangan seperti ini bisa berkembang menjadi perang siber (*cyber warfare*), yaitu perang antar-aktor yang menggunakan teknologi persenjataan canggih dan saling menyerang sistem informasi atau siber antar-aktor baik negara, swasta maupun masyarakat. Paul Hirst dalam *War and Power in the 21st Century* (2001) menyebut perang siber sebagai perang informasi. Perang seperti ini dapat diarahkan terhadap sistem informasi yang mengendalikan operasi militer atau sistem yang mengendalikan kegiatan masyarakat. Peretasan ke dalam komputer militer atau sistem yang mengendalikan kawat (transfer) antarbank, pengendalian lalu lintas udara dan stasiun tenaga nuklir memberi kemampuan kepada para prajurit perang informasi untuk mendatangkan kerusakan besar. Perang semacam ini pun cukup dilakukan oleh pasukan dalam jumlah kecil. Lawan yang paling sulit dihadapi oleh negara maju seperti Amerika Serikat ialah masyarakat dengan teknologi rendah yang memiliki sekelompok kecil elit prajurit siber (*cyberwarriors*).

Maraknya perang siber ini sedikit banyak mengamini prediksi James Canton yang dalam *The Extreme Future* (2006) yang menyatakan bahwa pada masa depan, perang yang terjadi lebih kompleks, lebih asimetris, dan tak semata-mata di wilayah ideologi dan militer, tapi juga ekonomi dan budaya. Salah satu ancaman perang itu adalah pencurian siber. Lebih spesifik, James Canton mengungkapkan adanya *cyjack* atau "maling siber" yang mencuri miliaran dolar dan institusi finansial yang mereka jadikan korban, dan mereka tidak tahu bahwa uangnya telah digondol maling. Ia juga menekankan 1 dari 10 tren keamanan masa depan berkaitan dengan serangan *cyber teror* yang telah tiba. Ketika dunia amat mengandalkan jaringan jasa-jasa penting, koneksi perdagangan, keuangan, komunikasi, pangan, transportasi, energi dan kesehatan, saat itulah suatu negara amat mudah diserang.

Sejalan dengan perkembangan teknologi informasi, perang telah mengalami perubahan paradigma dari yang sebelumnya perang hanya dilakukan secara konvensional dengan pengerahan massal para tentara secara fisik, kini perang dilakukan dengan serangan siber yang sarat teknologi (*high-tech*). Dampak nyata terhadap dunia kemiliteran dapat terlihat kira-kira sejak dekade 1990an hingga sekarang. Dalam dunia militer dikenal RMA (*Revolution in Military Affairs*) yang intinya adalah transformasi dunia militer yang sarat teknologi. Andrew P. Krevinevich dalam "*The State of the Art in the Global Defence Industry*" (2007) menyatakan bahwa RMA muncul pada saat penggunaan teknologi baru ke dalam sistem militer yang digabungkan dengan konsep operasional yang inovatif dan adaptasi organisasional yang mengubah secara mendasar karakter dan penyebab terjadinya sebuah konflik. Sehingga perang pun berevolusi, dari sebelumnya hanya dilakukan secara konvensional kini juga dilakukan dengan serangan siber.

- **Sekuritisasi Siber Indonesia Terhadap Kompleksitas Perang Siber Global**

Indonesia saat ini berada dalam keadaan mendesak keamanan siber atau keamanan dunia maya. Tingkat kejahatan di dunia maya atau kejahatan siber di Indonesia sudah mencapai tahap memprihatinkan. Penanganan keamanan siber membutuhkan pemikiran yang komprehensif karena kejahatannya berbeda dari kejahatan lain. Data Kementerian Komunikasi dan Informatika (Kemkominfo) menyebutkan bahwa pengguna internet di Indonesia hingga saat ini telah mencapai 82 juta orang. Dengan capaian tersebut, Indonesia berada pada peringkat ke-8 di dunia (Kemkominfo, 2025). Indonesia merupakan negara yang lemah keamanan sibernya. Ini terlihat dari maraknya berbagai kejadian, salah satunya adalah peretasan terhadap data kartu debit nasabah sebuah bank karena hacker berusaha menyusup ke sistem pengamanan kartu nasabah bank yang terjadi pertengahan Mei 2014. Ini menjadi catatan betapa buruknya keamanan siber di Indonesia. Satu fakta yang mengejutkan datang dari

perusahaan monitoring internet Akamai yang mengungkap bahwa kejahatan internet di Indonesia meningkat dua kali lipat. Angka ini menempatkan Indonesia di posisi pertama negara berpotensi menjadi target hacker, menggantikan Tiongkok.

Menurut Riant Nugroho (2014) dalam *National Security Policy* mengutip ID-SIRTII, bahwa pada tahun 2012 saja dilaporkan jumlah serangan ke dalam jaringan internet Indonesia mencapai 27 juta serangan atau 74.000 serangan per hari. Serangan terbesar berasal dari dalam negeri (63%), disusul serangan dari China (14%), dan Amerika Serikat (9%). Kasus website rumah sakit yang mendapat serangan virus ransomware bernama wannacry mengakibatkan kekacauan layanan online di rumah sakit tersebut. Menurut berita yang beredar, virus ransomware ini menyerang sekitar 99 negara. Cara kerjanya memblok file sehingga tidak dapat diakses. Korban yang ingin mengakses diharuskan membayar sejumlah uang sebagai tebusan.

Serangan siber juga terjadi pada rumah sakit. Fakta bahwa adanya serangan siber ke rumah sakit ini membuka mata kita tentang realita kemajuan teknologi perang. Ini juga menggambarkan dua hal: Pertama, telah ada sejumlah aktor yang *concern* dengan dunia perang siber ini. Kedua, sistem keamanaan siber institusi rumah sakit tersebut (dan ini mungkin mewakili institusi-institusi lain di Indonesia baik pemerintah maupun swasta) sangat lemah, yang terbukti berhasil diretas dan dijebol pertahanannya. Sebagian pihak memandang serangan siber belum menjadi ancaman yang sangat mengerikan bagi Indonesia karena belum semua urusan pemerintahan dan hajat masyarakat dikelola dengan teknologi siber.

Kembali pada prediksi James Canton bahwa perang masa depan bersifat asimetris, tidak hanya invasi kemiliteran, namun juga ekonomi dan budaya termasuk siber, maka Indonesia juga berpotensi memiliki ancaman yang serius nantinya. Dengan demikian, sekuritisasi ruang siber Indonesia terhadap Perang Siber Global menjadi krusial untuk direspon oleh Indonesia sebagai suatu ancaman fundamental yang perlu dipersiapkan daya penangkalnya. Secara bertahap, urusan pemerintahan dan hajat masyarakat di masa mendatang yang dikelola dengan teknologi siber sebaiknya tidak meninggalkan sistem pengelolaan secara fisiknya. Mulai dari sistem perbankan, bursa efek, pendidikan, transportasi, transaksi bisnis, kelistrikan hingga distribusi energi dan pangan, semuanya telah dan akan masuk ke era dunia siber. Jika tidak diantisipasi sejak dini, serangan siber bisa mematikan roda pemerintahan Indonesia.

Mengingat banyak negara yang "berkepentingan" dengan Indonesia, maka Indonesia harus siap menghadapi perang siber ini. Di sinilah urgensinya Indonesia mempersiapkan pasukan siber beserta penunjang-penunjangnya sejak dini. Berdasarkan kajian penulis, maka hasil dari sekuritiasi ruang siber Indonesia pada saat ini bisa dilihat pada Tabel 2:

Table 2. Sekuritisasi Siber Indonesia Terhadap Kompleksitas Perang Siber Global

Kategori	Sekuritisasi Siber Indonesia Terhadap Kompleksitas Perang Siber Global	Hasil
Ide Dasar	Sekuritisasi ruang siber Indonesia yang semula bukan ancaman menjadi sebuah masalah keamanan yang diisukan secara nasional, sehingga perang di ruang siber dijadikan agenda nasional Indonesia untuk menghalau ancaman perang siber global.	UU No. 3 Tahun 2025 tentang Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (UU TNI) menyebutkan ancaman siber dan hibrida menjadi ancaman nasional.
Fokus Utama	Menekankan konstruksi ruang siber untuk untuk diwacanakan secara publik sebagai ancaman yang kemudian melegitimasi pemerintah untuk membentuk undang-undang.	Institusi yang berwenang dalam menghalau perang siber yaitu TNI.
Basis Teoritis	Teori utama yang dipelopori oleh Mazhab Kopenhagen yang mendefinisikan ulang keamanan dari Perspektif Konstruktivis.	Sekuritisasi ruang siber Indonesia sebagai ancaman nasional
Sumber Daya	Didasarkan pada kemampuan mengendalikan ancaman sosial yang dikonstruksikan melalui bahasa dan praktik sebagai pembentuk keamanan.	Pidato Presiden Prabowo Subianto tentang Tantangan Indonesia menghadapi Perang Asimetris

Mekanisme	Membingkai sebuah ancaman potensial menjadi ancaman eksistensial terhadap "objek rujukan" (misalnya, negara, lingkungan, masyarakat).	Terbentuknya wacana "Indonesia Bisa Bubar" jika tidak bersiap dengan medan tempur siber yang dibentuk oleh pihak Barat.
Tujuan Akhir	Membentuk ancaman yang dikontruksikan secara sadar	Indonesia mulai tersadar untuk mewacanakan kategorisasi ancaman siber secara nasional
Dampak	Sumber daya menjadi terbatas untuk menghalau ancaman tertentu: semua jadi ancaman untuk memperkuat keamanan	Institusi pemerintah maupun non-pemerintah terkait isu siber menjadi sempit ruang geraknya akibat sektoralisasi ancaman siber

- **Geometripolitisasi Siber Indonesia Membentuk Tentara Siber: TNI Angkatan Siber**

Dalam hal pembentukan Pasukan Siber –dalam hal ini TNI Angkatan Siber—Indonesia sebaiknya tidak kalah langkah dari negara-negara seperti Amerika Serikat, Rusia, Cina, Israel, Australia, Inggris, bahkan Iran yang telah mempersiapkan tentara siber yang fokus menjaga pertahanan negaranya sekaligus mungkin melakukan serangan siber ke pihak lain. Amerika Serikat memiliki *United States Cyber Command* (US CYBERCOM) di bawah *United States Strategic Command* (US STRATCOM) yang mulai diaktifkan pada tahun 2009. Israel diketahui mempunyai sebuah unit khusus bernama Unit 8200 yang mempunyai spesialisasi cyber warfare di bawah *Israel Defense Forces* (IDF). Salah satu catatan yang fenomenal dari unit ini adalah keberhasilannya menghentikan operasi radar senjata anti pesawat udara Suriah. Negara Cina juga memiliki tentara siber yang dinamakan *"Blue Army"* yang berbasis di kawasan militer Guangzhou, sebelah selatan China. Inggris juga membangun *Cyber Security Operations Centre* (CSOC) di *Government Communications Headquarters* (GCHQ) di Cheltenham, arah barat laut kota London. Di negeri Kanguru, Departemen Pertahanan Australia membuat sebuah badan bernama *Cyber Security Operations Centre* (CSOC).

Berangkat dari berbagai bentuk pasukan siber di atas, Indonesia perlu mempersiapkan tentara siber serupa guna menghadapi kemungkinan perang siber dengan tentara siber negara-negara tersebut, minimal untuk melindungi pertahanan negara di dunia siber. Pasukan siber ini bisa dimulai dari manajemen teknologi dan informasi. Menurut Ronald Thompson & William Cats Barril (2003), terdapat empat pondasi utama yang mendukung perkembangan manajemen teknologi informasi yaitu: perkembangan perangkat lunak (*software*) seperti sistem dan aplikasi serta perkembangan alat keras (*hardware*) perkembangan sarana dan prasarana teknologi informasi, manajemen isi (*content management*), *telecommunication and networking*, perkembangan internet serta perdagangan online atau melalui internet. Sementara untuk pengorganisasian terkait dengan penggunaan sistem teknologi informasi, setidaknya ada empat hal utama yang harus diperhatikan yaitu: 1) Sistem informasi (*information systems*); 2) Kompetisi organisasi (*organizational competition*); 3) *Information systems* (sistem informasi) dan *organizational decision making* (sistem informasi dan pengambilan keputusan dalam organisasi); dan 4) Ppengorganisasian penggunaan sistem informasi.

Pada dasarnya sistem informasi itu terintegrasi. Karena itu, teknologi informasi dibangun berbasis sistem yang dirancang untuk dapat mendukung kerja, manajemen dan pengambilan keputusan dalam organisasi. Teknologi Informasi Komunikasi (TIK) adalah salah satu komponen paling penting dalam pengembangan sistem informasi. Pengelolaan sumber daya sistem informasi adalah permasalahan selanjutnya terkait dengan tantangan pengembangan TIK. Ada empat kunci utama yang harus diperhatikan agar pengelolaan sumber daya sistem informasi berhasil, yaitu: 1) Pengelolaan sumber daya sistem informasi haruslah ditempatkan sebagai proses manajemen bisnis; 2) Pembangunan sistem informasi; 3) Sumber daya eksternal sistem informasi, dan; 4) Manajemen sumber daya informasi.

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 siber dan organisasi dan aset pengguna. Termasuk di dalam organisasi dan aset pengguna dalam keamanan siber adalah perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya. Untuk memastikan suatu keamanan siber

memiliki pencapaian dan pemeliharaan terhadap keamanan organisasi dan aset pengguna terhadap keamanan siber, maka harus ada lima bidang kerja yang perlu dilakukan oleh suatu institusi yaitu:

1) Kepastian hukum (undang-undang kejahatan siber);
2) Teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak);
3) Struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih);
4) *Capacity building* dan pendidikan pengguna (kampanye publik dan komunikasi terbuka dari ancaman kejahatan siber terbaru); dan
5) Kerjasama internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman Siber).

Di Indonesia, tanggung jawab terhadap keamanan siber melibatkan beberapa lembaga seperti Kepolisian Republik Indonesia, TNI, Kemendagri, Kemenlu, Kementerian Pertahanan, serta Kementerian Informasi dan Komunikasi, dan kini BSSN yang menggantikan peran ID-SIRTII. Semua lembaga ini sebelum dibentuk BSSN, masing-masing saling berkoordinasi membentuk suatu tim siber nasional yang dinamakan ID-SIRTII (*Indonesia Security Incident Response Team on Internet Infrastructure*). ID-SIRTII dibentuk sesuai dengan Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet yang kemudian direvisi dengan Peraturan Menteri Komunikasi dan Informatika No. 16/PER/M.KOMINFO/10/ 2010, dan diperbaharui lagi dengan Peraturan Menteri Komunikasi dan Informatika No. 29 /PER/M.KOMINFO/12/ 2010.

ID-SIRTII merupakan tim yang ditugaskan Menteri Komunikasi dan Informatika (Kominfo) untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. Tugas dan fungsi dari ID-SIRTII diantaranya melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan gangguan pada jaringan, berkoordinasi dengan pihak-pihak terkiat di dalam maupun luar negeri dalam menjalankan tugas pengamanan jaringan telekomunikasi berbasis protokol internet, mengoperasikan, memelihara dan mengembangkan sistem database sistem ID-SIRTII, menyusun katalog-katalog dan silabus yang berkaitan dengan proses pengamanan pemanfaatan jaringan, memberikan layanan informasi atas ancaman dan gangguan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet, menjadi *contact point* dengan lembaga terkait tentang keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet serta menyusun program kerja dalam rangka melaksanakan pekerjaan keamanan jaringan telekomunikasi yang berbasis protokol internet (Kementerian Komunikasi dan Informatika RI, 2010).

Tujuh tahun kemudian pada 2017 lahirlah BSSN. Keberadaan BSSN ini minimal mempelopori fungsi sebagai "pasukan siber" Indonesia meskipun pada praktiknya belum maksimal sesuai dengan harapan sekelas tantara siber: dalam hal ini TNI Angkatan Siber. Kerangka hukum keamanan siber di Indonesia dibangun melalui UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta surat edaran menteri dan peraturan menteri. Adanya UU dan peraturan ini menjadi jaminan kepastian hukum dalam pengembangan keamanan siber. Namun persoalannya, legalitas penanganan kejahatan di dunia siber masih lemah, terutama terkait dengan aturan yang mengatur secara khusus kejahatan siber dan penanganan kejahatan siber. Sementara di sisi lain, bentuk kejahatan dunia siber semakin meningkat dan pola kejadiannya sangat cepat sehingga sulit untuk ditangani oleh aparat penegak hukum.

Secara nasional, menurut Hasyim Gautama (dalam Arianto dan Anggraini, 2019) mengungkapkan bahwa terdapat sejumlah permasalahan terkait dengan pembangunan keamanan siber yang tangguh, di antaranya:

1) Lemahnya pemahaman penyelenggara negara atas security terkait dengan dunia siber yang memerlukan pembatasan pengunaan layanan yang servernya berada di luar negeri dan diperlukan adanya pengunaan *secured system,*
2) Legalitas penanganan penyerangan di dunia Siber,
3) Pola kejadian kejahatan siber sangat cepat sehingga sulit ditangani,
4) Tata kelola kelembagaan keamanan siber nasional,
5) Rendahnya *awareness* atau kesadaran akan adanya ancaman siber attack internasional yang dapat melumpuhkan infrastruktur vital suatu negara, dan

6) Masih lemahnya industri kita dalam memproduksi dan mengembangkan perangkat keras atau hardware terkait dengan teknologi informasi yang merupakan celah yang dapat memperkuat maupun memperlemah pertahanan dalam dunia Siber.

Dengan adanya permasalahan ini, maka perlu diatur sebuah kebijakan yang mengatur tentang berbagai elemen yang terkait dengan keamanan siber. Kebijakan ini termasuk mengatur tentang sistem teknologi informasi komunikasi yang digunakan, yang meliputi pengaturan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait dengan keamanan informasi, serta standar infrastruktur yang wajib dipenuhi yang sesuai dengan standar internasional dalam menghadapi perang siber. Termasuk di dalamnya adalah adanya perimeter defense yang memadai, adanya *network monitoring system*, *system information and event management* yang berfungsi memonitor berbagai kejadian di jaringan terkait dengan insiden keamanan, *network security assement* yang berperan sebagai *control* dan *measurement* keamanan.

Pengaturan dan penataan kelembagan keamanan siber nasional yang kuat dalam rangka membentuk pasukan siber Indonesia merupakan salah satu prasyarat terwujudnya keamanan siber Indonesia yang handal. Penanganan keamanan siber harus terintegrasi secara kuat dan melibatkan berbagai lembaga terkait, yaitu intelijen, penegak hukum (Polri), pertahanan dan keamanan baik itu Kementerian Pertahanan RI maupun TNI serta pemerintah sebagai regulator yang dalam hal ini diwakili oleh Kominfo RI dan BSSN.

Selanjutnya, untuk menyikapi kejahatan siber yang sudah mencapai tahap memprihatinkan, maka salah satu alternatif kebijakannya adalah dengan menempatkan keamanan siber dalam konteks pertahanan, yaitu dengan mendorong Indonesia melakukan Geometripolitisasi terhadap ruang siber melalui pembentukan TNI Angkatan Siber guna menyelesaikan isu-isu terkait Geometrik Militer. Dengan pembentukan TNI Angkatan Siber ini, maka BSSN lebih difokuskan pada persoalan Gemetrik Sipil. Dengan demikian, penempatan ruang siber sebagai pertahanan akan menjadikan Indonesia siap dalam merespon Perang Siber Global. Sebagai konsekuensinya, Indonesia harus serius menciptakan pembangunan infrastruktur penunjang, termasuk di antaranya satelit khusus untuk pertahanan siber yang di dalamnya kerja penanganan pertahanan siber dikendalikan secara penuh oleh Indonesia mengingat sejumlah provider telekomunikasi sebagain besar dikelola oleh asing.

Tantangan lainnya ke depan dalam pengembangan kebijakan pasukan siber adalah sifat dari ancaman siber yang multidimensional, yang membuat penanganannya tidak hanya menjadi tanggungjawab dari TNI dan/atau Polri, Kemhan RI maupun Kemenkominfo RI. Salah satu strategi yang bisa dicermati dalam menghadapi *cyberwar* di antaranya adalah upaya serius pemerintah Amerika Serikat dalam mengembangkan *The National Cyber Security Division* (NCSD). Ini adalah divisi khusus yang bertugas menangani keamanan Siber secara nasional yang didukung oleh sektor swasta dan masyarakat yang memiliki tugas untuk membangun dan memelihara ruang siber nasional yang efektif melalui pembangunan sistem keamanan Siber atau dunia maya yang responsif. Divisi ini membuat dan menerapkan program manajemen risiko untuk ruang siber guna melindungi infrastruktur telekomunikasi dan siber dari situasi kritis yang dikenal dengan the *National Cyber Space Response System*.

Dalam membangun pasukan/tentara siber di Indonesia, perlu empat pondasi yang harus dipenuhi untuk mendukung perkembangan teknologi informasi, termasuk di dalamnya pengembangan pertahanan siber yaitu: perkembangan perangkat lunak (*software*) seperti sistem dan aplikasi dan perkembangan alat keras (*hardware*), perkembangan sarana dan prasarana teknologi informasi, manajemen isi (*content management*), *telecommunication and networking*, perkembangan internet serta lalu lintas internet yang wajib dilihat dari kerangka pertahanan nasional. Selain memenuhi keempat pondasi utama pengembangan pasukan siber, langkah lainnya yang mutlak dilakukan adalah pengorganisasian terkait dengan penggunaan sistem teknologi informasi dengan memperhatikan empat hal utama yaitu: sistem informasi; kompetisi organisasi; sistem informasi; pengambilan keputusan dalam organisasi; dan, pengorganisasian penggunaan sistem informasi.

Dengan disahkannya UU No. 3 Tahun 2025 tentang Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (UU TNI), maka perubahan UU ini bisa semakin fokus pada penyesuaian tugas, fungsi, dan struktur TNI menghadapi dinamika ancaman pertahanan modern (siber dan hibrida), memperkuat peran TNI dalam pertahanan negara, serta mengatur penempatan prajurit dan batas usia pensiun.

Berdasarkan analisis penulis, Tabel 3 adalah hasil Geometripolitisasi ruang siber Indonesia Membentuk TNI Angkatan Siber.

Table 3. Geometripolitisasi ruang siber Indonesia Membentuk Tentara Siber: TNI Angkatan Siber

Kategori	Geometripolitisasi ruang siber Indonesia Membentuk Tentara Siber: TNI Angkatan Siber	Hasil
Ide Dasar	Geometripolitisasi adalah proses menjadikan sesuatu yang awalnya tidak memiliki nilai keseimbangan, kekuatan, dan keamanan dengan mengubah fungsinya atau meningkatkan fungsinya menjadi kekuatan untuk menciptakan kondisi pengamanan dan pengendalian sesuatu (di lingkup bangsa-dunia dan negara-bangsa) dengan menghilangkan ancaman atau serangan paksa dari pihak yang dituju atau ditargetkan.	UU No. 3 Tahun 2025 tentang Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (UU TNI) menyebutkan ancaman siber dan hibrida menjadi ancaman nasional sehingga ruang siber menjadi salah satu prioritas untuk dibentuk penangkalnya melalui fungsionalisme ruang siber di sipil oleh BSSN dan militer: Tentara Siber.
Fokus Utama	Menekankan dimensi spasial atas eskalasi kekuasaan dan bagaimana kendali atas entitas-entitas membantu para aktor mencapai tujuan.	Indonesia menjadikan ruang siber sebagai ruang pengambilan keputusan yang bisa mempengaruhi pemerintah mengambil sebuah keputusan.
Basis Teoritis	Berangkat dari Teori Geometripolitika, sebuah gagasan teoretis yang dipelopori oleh Mazhab Indonesia (*Indonesian School of World Relations*): Manunggalisme.	Geometripolitisasi ruang siber Indonesia sebagai keseimbangan, kekuatan, dan keamanan nasional membentuk gotong royong di ruang siber.
Sumber Daya	Didasarkan pada kemampuan mengendalikan ruang fisikal, metafisikal, psikologikal, ideasional, dan geometrikal sebagai pembentuk keamanan.	Pidato Presiden Prabowo Subianto tentang Tantangan Indonesia mengendalikan isu Perang Siber dan Perang Hibrida di negara-negara besar.
Mekanisme	Menghubungkan keseimbangan, kekuatan, dan keamanan melalui pemanfaatan 8 matra "ruang dunia" (darat, laut, udara, bawah tanah, galaksi, ruang hampa, khatulistiwa, dan siber).	Terbentuknya wacana "Indonesia Calon Pemimpin Dunia" harus siap dengan berbagai bentuk kerjasama dengan bangsa Timur lainnya.
Tujuan Akhir	Membentuk keseimbangan, kekuatan, dan keamanan dari berbagai situasi	Indonesia mulai kerjasama dengan bangsa pemimpin teknologi seperti: Tiongkok, Rusia, dan Korea Utara.
Dampak	Sumber daya menjadi melimpah untuk menghalau ancaman spesifik: Semua jadi kekuatan untuk melawan satu ancaman.	Pemerintah Indonesia Bersama Masyarakat Jagatmaya (*Netizen)* Bersatu melawan berbagai dampak perang siber global: kombinasi geometrik sipil dan militer.

- **Indonesia Menghadapi Perang Siber Abad Ke-21**

Indonesia sebaiknya mampu mengembangkan model pasukan siber yang handal untuk menciptakan sebuah sistem pertahanan siber yang kuat. Menurut Sukamta (2017), setidaknya ada empat hal yang harus mendapat perhatian dalam model tersebut, yaitu regulasi, teknologi, SDM yang berkualitas, dan institusi. Pemerintah semestinya mengeluarkan kebijakan tentang ketahanan siber. Regulasi berupa undang-undang dan peraturan-peraturan terkait perlu disiapkan. Dengan payung hukum tersebut, akan terdapat alokasi APBN untuk pembangunan dan pengembangan ketahanan siber. Hal ini perlu dipikirkan dan dikerjakan secara serius agar efisien dan tidak terkesan membuang-buang anggaran negara. Teknologi ketahanan siber musti diperbaharui terus-menerus.

Meskipun selama ini masyarakat Indonesia lebih cenderung menggunakan teknologi produk negara lain, perlu direncanakan dalam grand design bahwa ke depannya agar Indonesia mandiri dalam hal menciptakan teknologi dan produk ketahanan siber. Hal ini dapat dilakukan dengan tukar informasi dan teknologi dengan negara lain. Demikian pula dengan SDM, Indonesia sebetulnya memiliki jumlah SDM teknologi informasi yang jumlahnya tidak bisa dibilang sedikit. Namun dengan jumlah itu, kualitas

mereka harus terus ditingkatkan dan dikembangkan, mengingat kecepatan perkembangan teknologi informasi sangatlah cepat. Salah satu solusinya adalah membuka jurusan spesifik tentang ketahanan siber pada kampus-kampus yang membuka teknologi informasi yang sudah ada. SDM-SDM seperti inilah yang nantinya direkrut untuk menjadi Angkatan Siber (setelah AD, AL, AU) atau *cyber army*. Agar pertahanan siber berjalan optimal, perlu diorganisasikan dalam sebuah institusi atau gugus tugas *(task force)*.

Melalui institusi atau gugus tugas ini, para *cyber army* bisa bersatu dan bekerja sama menggunakan keahlian mereka dalam satu misi dan visi untuk memperkuat pertahanan siber Indonesia. Institusi atau gugus tugas ini harus bisa mengoordinasikan institusi-institusi yang selama ini juga memiliki tugas terkait siber, pertahanan dan keamanan, seperti BSSN, Kementerian Pertahanan RI, TNI, Polri, BIN dan Lembaga terkait. Keberadaan BSSN belumlah cukup untuk mengemban pertahanan siber karena kewenangannya yang masih terbatas. Sedangkan, institusi pertahanan siber harus melingkupi sektor publik seperti perbankan, distribusi air bersih, distribusi gas, bahkan instalasi listrik. Apalagi jika mengingat ke depannya semakin banyak urusan negara, pemerintahan dan kepentingan publik yang dilakukan dengan teknologi siber.

Payung hukum terkait ketahanan siber yang ada selama ini, yaitu Undang-undang Nomor 3 Tahun 2002 tentang Pertahanan Negara dan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transkasi Elektronik yang telah direvisi menjadi Undang-undang No. 19 tahun 2016 (UU ITE) perlu diperkuat. Jika skala serangan siber bersifat individu atau mikro, ini lebih sering masuk kategori cyber crime. Aturan dalam UU ITE mencakup serangan siber pada skala mikro atau *cyber crime*. Serangan siber yang bersifat makro yaitu kenegaraan bahkan internasional, masuk ke dalam kategori *cyber war*.

Selanjutnya, Undang-undang No. 3 tahun 2002 tentang Pertahanan Negara bisa diperkuat terutama secara tegas dan jelas agar bisa mengatur pertahanan negara dari serangan siber yang berskala makro dan termasuk kategori *cyber war*. Namun faktanya, Undang-undang Pertahanan Negara tersebut khususnya pada Pasal 6 tidak menyebutkan secara tegas soal ketahahan di bidang siber: *"Pertahanan negara diselenggarakan melalui usaha membangun dan membina kemampuan, daya tangkal negara dan bangsa, serta menanggulangi setiap ancaman."* Pada pasal tersebut disebutkan "setiap ancaman", namun tidak tegas dikatakan siber, meskipun tercakup di dalamnya, karena kini ancaman itu juga berbentuk serangan siber.

Pada tahun 2025, Indonesia seharusnya sudah bisa mempersiapkan diri untuk pembentukan Tentara Siber Indonesia dengan membentuk TNI Angkatan Siber sesuai dengan payung hukum yang sudah disahkan, yaitu UU No. 3 Tahun 2025 tentang Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (UU TNI). Perubahan UU ini berfokus pada penyesuaian tugas, fungsi, dan struktur TNI menghadapi dinamika ancaman pertahanan modern (siber dan hibrida), memperkuat peran TNI dalam pertahanan negara, serta mengatur penempatan prajurit dan batas usia pensiun. Dari sini, Indonesia bisa melebarkan sayap untuk mengembangkan fungsi dan struktur TNI dalam menghadapi dinamika ancaman pertahanan modern seperti ancaman siber, ancaman hibrida, hingga ancaman geometri. Hal ini membuat ruang baru bagi Indonesia, khususnya TNI untuk membentuk TNI Angkatan Siber. Pembentukan TNI Angkatan Siber merupakan langkah terbaik bagi Indonesia untuk merespon Perang Siber Abad ke-21.

KESIMPULAN

Untuk mencegah ataupun menghadapi ancaman perang siber global, Indonesia perlu melakukan geometripolitisasi dan sekuritisasi ruang siber untuk membentuk tentara siber dalam bentuk TNI Angkatan Siber. Pada periode pemerintahan Prabowo Subianto, wacana pembentukan Tentara Siber Indonesia membentuk TNI Angkatan Siber kini mulai beralih dari tataran akademik menjadi tataran kebijakan pemerintah Indonesia setelah pada Maret 2025 disahkannya UU No. 3 Tahun 2025 tentang Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (UU TNI). Perubahan UU ini berfokus pada penyesuaian tugas, fungsi, dan struktur TNI menghadapi dinamika ancaman pertahanan modern (siber dan hibrida), memperkuat peran TNI dalam pertahanan negara, serta mengatur penempatan prajurit dan batas usia pensiun.

Dalam menghadapi ancaman modern seperti ancaman siber, ancaman hibrida, dan ancaman geometri Indonesia dapat menyesuaikan diri terhadap kemajuan pemanfaatan ruang siber (kombinasi geometrik sipil dan militer) guna mendukung pertahanan siber yang menemui tantangan baru akibat

hadirnya paradoks informasi abad ke-21. Dengan menggunakan teori Geometripolitika/Geometripolitisasi pendekatan Mazhab Indonesia (*Indonesian School of World Relations*) "Manunggalisme" dan Sekuritisasi pendekatan Mazhab Kopenhagen (*Copenhagen School*), ruang siber telah menjadi salah satu medan tempur, yaitu bagaimana geometripolitisasi ruang siber membentuk keseimbangan, kekuatan, dan keamanan setelah sekuritisasi atas fenomena perang siber melalui kacamata pertahanan Indonesia.

Studi ini menyimpulkan bahwa: (1) Transformasi Perang Siber Global abad ke-21 menciptakan medan tempur baru di ruang siber; (2) Sekuritisasi siber Indonesia dilakukan dengan cara membingkai kompleksitas Perang Siber Global sebagai salah satu ancaman nasional; (3) Geometripolitisasi siber Indonesia dilakukan dengan cara menghubungkan keseimbangan, kekuatan, dan keamanan untuk meraih peran Tentara Siber yang berpotensi menjadi TNI Angkatan Siber; dan, (4) Indonesia harus merespon Perang Siber Global abad ke-21 dengan cara mewacanakan pembentukan TNI Angkatan Siber di bawah payung hukum UU No. 3 Tahun 2025 tentang Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (UU TNI).

DAFTAR PUSTAKA

Anne W. Brascomb (ed), Toward A Law of Global Communication Network, New York: Lognman, 1986.

Arianto, Adi Rio. 2016. "Keamanan Siber Menuju Perang Geometri Antarbangsa: Geometripolitika dan Arsitektur Keamanan Dunia Era Horizontal (Era Manunggalian) Abad Ke-21." *Asosiasi Ilmu Hubungan Internasional Indonesia,* Vol. 7, No. 1, 2016. Journal link: https://aihii.or.id/prosiding-vennas-vii/

Arianto, Adi Rio. 2017. "Cyber Security: Geometripolitika dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21." *Jurnal Power in Internasional Relatios,* Vol.1, No.2. Journal Link: https://download.garuda.kemdikbud.go.id/article.php?article=1469214&val=17736&title=Cyber%20Security%20Geometri%20Politik%20Dan%20Dimensi%20Pembangunan%20Keamanan%20Dunia%20Era%20Horizontal%20Abad%2021

Arianto, Adi Rio, and Gesti Anggraini. 2019. "Building Indonesia's National Cyber Defense And Security to Face The Global Cyber Threats Through Indonesia Security Incident Response Team On Internet Infrastructure (ID-SIRTII)." *Jurnal Pertahanan dan Bela Negara,* Vol. 9, No. 1, 2019. Journal link: https://jurnal.idu.ac.id/index.php/JPBH/article/view/515/JPBHV9N1EA2

Arianto, Adi Rio, and Gesti Anggraini. 2020. "Manunggalism and the World Order in the Era of Manunggal 21st Century: The Role of Indonesia-China Cultural Cooperation in Building the Future of World Security Architecture by Promoting the Values of Mutual Cooperation "Gotong Royong", Unity, and Harmony." *Center for Southeast Asian Social Studies Universitas Gadjah Mada,* 2020. Journal link: https://pssat.ugm.ac.id/conference-proceeding-symposium-on-social-science-rethinking-the-social-world-in-the-21st-century/

Arianto, Adi Rio, and Gesti Anggraini. 2021. "Manunggalisme dan Disiplin Ilmu Antarbangsa (IA): Menggagas Mazhab Indonesia (MI) Melalui Tradisi Animisme, Dinamisme, dan Waliisme dan Mengarusutamakan "Gotong Royong Sebagai Sistem Dunia" Untuk Membangun Keamanan dan Tatanan Dunia Era Manunggal Abad Ke-21." *Asosiasi Ilmu Hubungan Internasional Indonesia*, Vol. 11, No. 1, 2021. Journal link: http://aihii.or.id/prosiding-vennas-xii/

Arianto, Adi Rio, and Gesti Anggraini. 2023. "Manunggalism: Paradigm, Philosophy, and Theory to View the World Relations (WR) Belong to Indonesian School (Mazhab Indonesia) in Manunggalian Era 21st Century". *UGM Digital Press*, Vol. 9, No. 1 , 2023. Journal link: https://digitalpress.ugm.ac.id/article/433

Arsyad Sanusi, Hukum Teknologi dan Informasi, Bandung: Tim Kemas Buku, 2005

Brascomb, Anne W. 1986, Toward A Law of Global Communication Network, USA: Lognman

Buzan, Barry and Waever, Olle. 1998. Security: A New Framework for Analysis. *www.researchgate.net*.

Buzan, Barry. 1994. New Patterns of Global Security in the Twenty-First Century. *International Affairs (Royal Institute of International Affairs* 1944). Vol. 67, No. 3 (Jul., 1991), pp. 431-451 (21 pages). Published By: Oxford University Press

Elizabeth Longworth, The Possibilities for legal framework for cyber space- Including New Zealand Perspective, Theresa Fuentes et.al (editor), The International Dimesions of Cyberspace Law: Law of Cyberspace Series, Vol.1, Aldershot: Ashgate Publishing Limited, 2000.

Indrawan, Jerry dan Efriza, "Bela Negara Sebagai Metode Pencegahan Ancaman Radikalisme di Indonesia", *Jurnal Pertahanan dan Bela Negara*, Universitas Pertahanan Indonesia, Nomor 3, Volume 7, Desember 2017, hal. 1-2

John Vivian, 2008, Teori Komunikasi Massa, Jakarta: Kencana, hal. 264.

John Vivian, Teori Komunikasi Massa, Jakarta: Kencana, 2008 M.

Kemkominfo: Pengguna Internet di Indonesia Capai 82 Juta, http://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Internet+di+Indonesia+Capai+82+Juta/0/berita_satker#.U9G4o5R_tfs, diakses 1 Oktober 2025 pukul 09.00 WIB.

Nathalie Chaplan, Cyber War: The Challenge to National Security, *Global Security Studies*, Winter 2013, Volume 4, Issue 1, University of North Carolina Wilmington

Pasal 9 Peraturan Menteri Komunikasi dan Informatika No. 29/PER/M.KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Peraturan Kepala Divisi Teknologi Informasi Kepolisian Negara Republik Indonesia No.1 Tahun 2011 tentang Hubungan Tata Cara Kerja Di Lingkungan Divisi Teknologi Informasi Kepolisian Negara Republik Indonesia.

Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet

Peraturan Nomor 24 Tahun 2008 Tentang Penyelenggaraan Sistem Komunikasi Dan Elektronika Pertahanan Negara.

Pusat Teknologi Informasi dan Komunikasi Badan Pengkajian dan Penerapan Teknologi (BPPT), Kajian Konvergensi Teknologi Informasi dan Komunikasi, Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT, 2007

Pusat Teknologi Informasi dan Komunikasi Badan Pengkajian dan Penerapan Teknologi (BPPT), Kajian Konvergensi Teknologi Informasi dan Komunikasi, Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT, 2007, hal.3

Ronald Thompson & William Cats Barril, Information Technology and Management, New York: Mc Graw Hill, 2003.

Salam, Syahrul, dan Adi Rio Arianto, dan Rizky Hikmawan, "Pemikiran Bela Negara dan Hubungan Internasional: Pergeseran Peran Negara dan Implikasinya terhadap Perkembangan Sudut Pandang Studi Ilmu Hubungan Internasional", *Jurnal Pertahanan dan Bela Negara*, Universitas Pertahanan Indonesia, Nomor 3, Volume 7, Desember 2017

Sanusi, M. Arsyad, 2005, Hukum Teknologi dan Informasi, Bandung: Tim Kemas Buku, hal.92-93.

Sukamta, 2017, "*Menghadapi Perang Siber**, disampaikan pada Seminar Nasional, Peran Cyber Intelligence dalam Mendukung Keamanan Nasional, Sekolah Kajian Strategik dan Global, Universitas Indonesia, 19 Mei 2017.

Thompson, Ronald & William Cats Barril, 2003, Information Technology and Management, New York: Mc Graw Hill, hal. 29