# Perang Kasat Mata: Membangun Kapasitas Operasi Siber TNI dalam Koridor Demokrasi

Cakrawala Strategis | No. 004/2025 - 11 Agustus 2025

**Tim Penulis:**
Christian Guntur Lebang
Feline Cloramidine
Micha Angelia Loing

**Ilustrator:**
Muhammad Ilham
Rudi Yusuf

## Ringkasan Eksekutif

Transformasi lingkungan strategis digital menuntut Tentara Nasional Indonesia (TNI) untuk membangun kemampuan operasi dan peperangan siber sebagai bagian integral dari sistem pertahanannya. Revisi UU TNI 2025 yang menambahkan peran OMSP dalam menghadapi ancaman siber menjadi tonggak penting, namun juga menimbulkan kekhawatiran akan perluasan wewenang militer ke ranah sipil tanpa batasan yang jelas. Tanpa pengaturan hukum dan akuntabilitas yang ketat, pelibatan TNI dalam ruang digital berisiko mencederai prinsip-prinsip supremasi sipil dan memperburuk kualitas demokrasi Indonesia.

Persepsi terhadap ancaman siber mengaburkan batasan dari operasi siber TNI. Hal ini bisa dilihat mulai dari pernyataan pimpinan pemerintahan dan TNI, UU serta dokumen strategis sektor pertahanan, hingga doktrin di tubuh TNI. Ancaman tersebut dimakna secara luas, sehingga cukup besar fokus terhadap operasi informasi dan bagaimana ruang siber digunakan untuk menyerang keutuhan bangsa. Dalam konteks demokrasi Indonesia, keadaan tersebut membuka peluang penggunaan kemampuan siber TNI terhadap masyarakat sipil dan cenderung tidak menjunjung hak asasi manusia (HAM).

Di sisi lain, kematangan kemampuan siber TNI sendiri masih jauh dari cukup. Perdebatan mengenai perlu tidaknya Angkatan Siber menghadirkan diskusi yang lebih luas mengenai tantangan yang dihadapi TNI dalam pengembangan kemampuan sibernya. Kekurangan personil, tertatih-tatihnya perkembangan organisasi, hingga fokus terhadap ancaman informasi dari media sosial menjadi bagian tidak terpisahkan dari dinamika tersebut.

Maka dari itu, diperlukan rencana pengembangan kemampuan siber TNI yang tetap berada dalam koridor demokrasi. Cakrawala Strategis ini melihat bahwa kemampuan peperangan siber TNI memerlukan pembaruan dokumen strategis yang memuat gradasi ancaman, batas pelibatan, dan definisi ulang ancaman hibrida, serta dukungan legislasi keamanan siber dan nasional. Secara kelembagaan, Satsiber perlu ditingkatkan menjadi Kotama Operasi menuju Komando Gabungan, dengan mengkaji ulang fokus pengendalian konten. Dari sisi personel, dibutuhkan jalur karier jelas, promosi perwira tinggi berlatar siber, standarisasi kurikulum pelatihan, serta rekrutmen talenta non-teknis seperti ahli hukum. Terakhir, hubungan sipil-militer harus diperkuat melalui koordinasi operasi siber dengan institusi sipil, mekanisme akuntabilitas oleh DPR, dan keterbukaan dokumen strategi kepada publik.

# Pendahuluan

Tahun 2025 adalah tahun yang akan menjadi titik penting sejarah Indonesia, di mana bangsa ini akan merayakan kemerdekaannya yang ke-80. Keistimewaan tahun ini juga bisa dirasakan di sektor pertahanan, terutama di tubuh Tentara Nasional Indonesia (TNI). Senafas dengan perayaan kemerdekaan, TNI juga akan berumur 80 tahun di tahun ini. 2025 juga menjadi tonggak sejarah bahwa telah seperempat abad berlalu sejak institusi militer tersebut berubah nama dari Angkatan Bersenjata Republik Indonesia (ABRI) di tahun 1999 sebagai bagian dari proses reformasi dan mendorong TNI menjadi tentara yang modern dan profesional. Salah satu bentuk upaya reformasi tersebut adalah melalui regulasi Undang-Undang (UU) TNI yang dikeluarkan pada tahun 2004.

Setelah lebih dari 20 tahun dan dengan segala perkembangan dinamika ancaman, pemerintah merasa perlu untuk melakukan revisi terhadap UU TNI untuk semakin merefleksikan kebutuhan terkini TNI. Pada Maret 2025, Dewan Perwakilan Rakyat (DPR) berserta pemerintah mengesahkan revisi terhadap UU TNI, meskipun mendapatkan gelombang kecaman dari masyarakat terutama akibat proses pembahasan yang dirasa tertutup dan tidak mengakomodasi masukan dari masyarakat sipil.[1] Revisi tersebut secara mayoritas bersifat teknokratik dan administratif, di mana terdapat penambahan institusi sipil yang bisa diisi oleh perwira aktif TNI maupun perpanjangan usia pensiun bagi prajurit. Menghadapi perubahan dinamika ancaman yang dihadapi oleh negara, revisi tersebut juga menambahkan dua tugas baru dalam melakukan Operasi Militer Selain Perang (OMSP) yang tertuang pada pasal 7 UU TNI, yaitu menanggulangi ancaman pertahanan siber serta membantu dan menyelamatkan warga negara dan kepentingan Indonesia di luar negeri.

Publik lantas menyoroti penambahan OMSP Siber tersebut.[2] Kritik utama terhadap ayat tersebut adalah potensi militerisasi ruang siber di tengah situasi penurunan kualitas demokrasi di Indonesia, seperti yang ditunjukkan oleh beberapa indeks global.[3] Sejarah panjang terkait Dwifungsi ABRI dalam sistem politik-sosial negara ini hingga semakin nyatanya tendensi untuk melibatkan TNI dalam berbagai sektor sipil akhir-akhir ini menjadi landasan utama kritikan tersebut.[4] Hasil revisi UU TNI juga tidak secara jelas mendefinisikan ancaman siber seperti apa yang akan dihadapi oleh TNI, sehingga memungkinkan terjadinya interpretasi yang subjektif dari pemerintah dan dari tubuh TNI sendiri atas cakupan otoritas TNI di ruang siber. Bahkan, revisi tersebut juga meminimalkan peran pengawasan DPR dalam pelaksanaan OMSP dan memberikan wewenang lebih kepada Presiden dalam pengerahan TNI untuk OMSP hanya perlu melalui peraturan turunan, bukan berdasarkan proses politik sesuai yang tertera di UU versi sebelumnya.[5] Dengan begitu, muncul kecemasan bahwa penambahan OMSP Siber tersebut justru berpotensi digunakan untuk kepentingan rezim, mempersempit ruang publik, menarget pihak-pihak yang mengkritik kebijakan pemerintah serta TNI, yang mana akan memperburuk kondisi hubungan sipil-militer serta demokrasi di Indonesia ke depannya.

Di sisi lain, perlu diakui bahwa adalah sebuah keniscayaan bagi angkatan bersenjata di mana pun untuk melakukan integrasi strategi peperangan siber dalam organisasinya serta mempersiapkan diri menghadapi ancaman siber dalam menjalankan tugas-tugasnya. Dibandingkan negara-negara lain, Indonesia bisa dibilang cukup tertinggal dalam pengembangan kapasitas siber di institusi militernya. Untuk organisasi, misalnya, saat ini Indonesia hanya memiliki Satuan Siber (Satsiber) yang berada di bawah Markas Besar (Mabes) TNI yang dikepalai oleh perwira tinggi bintang satu yang didirikan pada tahun 2017. Periode tersebut bersamaan dengan fenomena merebaknya pembentukan organisasi siber serupa secara global, di mana Max Smeets memperkirakan 27 negara melakukan hal tersebut di antara tahun 2014 hingga 2018.[6] Meskipun demikian, TNI belum bisa dibilang mencapai kematangan strategis, setidaknya berdasarkan ketiadaan dokumen khusus mengenai strategi pertahanan siber serta skala Satsiber TNI yang belum sampai level Komando Siber. Dengan pesatnya perkembangan teknologi informasi, situasi geopolitik dunia yang semakin memanas serta proses integrasi siber dalam peperangan modern yang masih terus berjalan, idealnya TNI juga terus memperkuat kapasitas sibernya sehingga mampu menjaga kepentingan nasional Indonesia bahkan di titik tertentu menjadi bagian dari *statecraft* untuk mencapai tujuan strategis bangsa.

Dinamika antara kendali demokrasi dan kepentingan pengembangan kemampuan siber TNI menghadirkan sebuah pertanyaan, bagaimana seharusnya Indonesia mengembangkan kemampuan siber militernya yang sesuai dengan koridor demokrasi? Kepentingan untuk menyiapkan TNI yang mampu beradaptasi terhadap peperangan modern, di mana ruang siber menjadi faktor penggerak utama, semestinya harus sejalan upaya menjaga demokrasi dan supremasi sipil di Indonesia. Isu ini sendiri tidak sesuatu yang spesifik hanya dihadapi oleh Indonesia, tetapi juga hampir semua negara demokrasi berkembang di berbagai belahan dunia. Sejalan dengan perkembangan kapasitas siber, baik pada institusi militer dan intelijen sipil, muncul tren mengkhawatirkan bahwa kemampuan tersebut justru diarahkan ke dalam negeri dan digunakan untuk mengawasi lawan politik pemerintah yang berkuasa.[7] Di sisi lain, standar penggunaan kekuatan siber militer oleh negara-negara demokrasi yang sudah matang, yang juga memiliki kemampuan siber lebih mapan, akan sulit diterapkan sepenuhnya dalam proses pengembangan kebijakan, kapasitas, serta organisasi militer di Indonesia. Mempertimbangkan segala situasi tersebut, Indonesia perlu memikirkan peta jalan yang sesuai dengan konteks dan kebutuhannya sendiri sehingga cita-cita reformasi untuk membentuk TNI yang profesional bisa betul-betul tercapai, termasuk di ruang siber.

## Peperangan Siber dan Integrasinya ke TNI

Umumnya, terdapat tiga pendekatan utama melihat bagaimana berbagai organisasi militer melihat ruang siber dan strategi peperangannya. Pertama, ruang siber dilihat sebagai bagian tidak terpisahkan dari peperangan modern dan menjadi faktor utama melakukan peperangan berbasis jaringan (*network centric*

*warfare*) dan berfungsi sebagai pengganda kekuatan (*force multiplier*). Amerika Serikat dan Israel menjadi negara utama yang memiliki kemampuan di atas dan telah memiliki strategi peperangan siber yang cukup mapan, dengan Tiongkok juga terus berusaha mengembangkan kemampuan serupa.

Kedua, ruang siber diletakkan dalam konteks yang lebih luas dari sekadar ranah peperangan militer tetapi lingkungan di mana kepentingan strategis negara diperjuangkan. Dengan pendekatan ini, strategi peperangan siber tidak hanya dijalankan oleh organisasi militer dan terbatas di medan konflik, tetapi juga instansi lain termasuk intelijen sipil. Operasi siber untuk menginfiltrasi dan merusak jaringan lawan dipahami sebagai salah satu cara untuk mempengaruhi lingkungan informasi untuk mendukung tujuan nasional yang lebih besar. Dengan begitu, peperangan informasi dan penggunaan propaganda menjadi bagian integral dari strategi raya tersebut. Rusia adalah contoh negara utama dengan pendekatan ini.

Ketiga, organisasi militer berfokus pada menjaga keamanan jaringan strategis, baik di masa damai maupun saat perang. Pendekatan ini terutama dipengaruhi oleh belum mapannya kapasitas siber militernya, ketiadaan ambisi strategis besar yang memerlukan kekuatan siber yang ofensif, serta negara tersebut berada dalam payung pertahanan negara adidaya. Mayoritas negara di dunia mengadopsi perspektif ini, dengan tingkat integrasi peperangan siber yang berbeda-beda.

Ketiga pendekatan tersebut bukanlah sesuatu yang kaku dan adopsi negara-negara bisa sangat cair dalam implementasinya. Selain itu, kategorisasi tersebut sangat berfokus pada doktrin dan strategi negara-negara adidaya. Hal ini dipengaruhi oleh dua hal. Pertama, pembangunan kapasitas siber militer berbasis teknologi tinggi cenderung masih dikuasai oleh negara-negara besar tersebut. Proliferasi kemampuan siber sangat ditentukan oleh negara-negara utama, terutama untuk negara Barat dalam payung kerja sama pertahanan seperti NATO dan *Five Eyes*. Kedua, pembangunan kapasitas tersebut harus ditunjang juga oleh pengalaman operasi, baik dalam kerangka operasi multi-ranah (*multi-domain operations*) maupun operasi siber ofensif khusus. Kemampuan ofensif ini juga yang membedakan antara Amerika Serikat, sebagai negara yang dianggap memiliki kemampuan siber paling baik, dengan pesaingnya seperti Rusia dan Tiongkok.[8] Selain ketiga negara tersebut, ada beberapa negara lain yang dianggap telah cukup berkembang kemampuan sibernya, seperti Israel, Korea Utara, Iran, serta negara-negara aliansi NATO. Namun, doktrin dan strategi peperangan siber yang mapan serta mendapatkan banyak perhatian dari peneliti dan akademisi cenderung berfokus kepada tiga negara tersebut.

## Perspektif Peperangan Siber Indonesia

Bagaimana Indonesia melihat peperangan siber maupun proses integrasinya ke dalam kebijakan dan operasi oleh TNI bisa dilihat melalui tiga cara. Pertama, melihat bagaimana pejabat senior serta dokumen strategis kebijakan pemerintah memersepsikan ancaman siber terhadap Indonesia maupun pemanfaatan ruang siber dalam operasi TNI. Kedua, mengkaji kematangan siber di organisasi TNI.

Ketiga, merefleksikan pengalaman operasi siber TNI maupun ancaman dari aktor negara terhadap Indonesia dalam beberapa tahun terakhir. Ketiga pendekatan tersebut diharapkan mampu menjabarkan secara lebih jelas perjalanan perspektif peperangan siber di dalam tubuh TNI.

Tinjauan terhadap berbagai pernyataan pejabat utama Kemhan dan TNI, regulasi dan kebijakan sektor pertahanan menunjukkan bahwa pendekatan pemerintah terhadap peperangan siber mendekati strategi *information confrontation* dari Rusia. Peperangan siber dilihat sebagai sebuah spektrum ancaman informasi dan cenderung tidak terintegrasi penuh dalam operasi militer jika dibandingkan dengan AS. Berbagai dokumen strategis yang dikeluarkan pemerintah sejak tahun 2008 melihat adanya tren konflik kontemporer yang mengedepankan strategi peperangan proksi dan ruang siber menjadi faktor pendukung utama. Pendekatan tersebut kemudian selaras dengan persepsi ancaman yang selama ini dipegang oleh TNI akan bahaya disintegrasi bangsa yang lahir dari pengalaman menghadapi berbagai gerakan separatis sejak kemerdekaan Indonesia.

Pendekatan di atas pertama-tama bisa dilihat dari berbagai pernyataan beberapa pengambil kebijakan utama. Presiden Prabowo Subianto menyebutkan bahwa ada kekuatan asing yang tidak ingin Indonesia menjadi kuat dan mendanai organisasi sipil untuk mengadu domba bangsa.[9] Sebagai purnawirawan jenderal, pernyataan Presiden Prabowo merefleksikan persepsi ancaman terhadap peperangan proksi, meskipun dirinya tidak secara eksplisit menyebutkan ruang siber di dalamnya. Sebelumnya, mantan Menteri Koordinator Politik, Hukum dan Keamanan yang juga Panglima TNI 2017-2021, Hadi Tjahjanto, menyebutkan perang siber sebagai perang informasi untuk membangun opini di masyarakat.[10] Lebih jauh, Hadi juga menyebutkan bahwa Indonesia pernah menghadapi perang siber dengan aktor-aktor yang mendukung kemerdekaan Timor Leste. Argumentasi serupa muncul dalam perdebatan OMSP Siber TNI, di mana Kemhan menyebutkan bahwa salah satu target operasi siber TNI tersebut adalah pihak-pihak yang melakukan operasi informasi untuk melemahkan kepercayaan publik dan berpotensi memecah belah bangsa.[11]

Dalam sejarahnya, TNI memang tidak pernah benar-benar melihat dirinya hanya sebagai alat pertahanan negara saja. Selayaknya banyak negara yang baru merdeka pasca-Perang Dunia II, organisasi militernya merasa memiliki hak dan tanggung jawab untuk terlibat di dalam semua isu keamanan dan menjaga kedaulatan negara. Pendekatan ini sangat mempengaruhi hubungan sipil-militer di Indonesia, dari era perang kemerdekaan hingga pasca-reformasi, termasuk puncaknya melalui doktrin Dwifungsi di masa Orde Baru.[12] Interpretasi akan Doktrin Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata) yang tertuang dalam konstitusi dan tugas TNI yang tertuang di Pasal 6 dan 7 UU TNI untuk menjaga kedaulatan negara kemudian semakin menegaskan bagaimana TNI melihat perannya di ruang siber, yaitu tidak terbatas hanya pada sektor pertahanan siber saja.

Pemahaman peperangan siber tersebut kemudian tertuang dalam regulasi dan berbagai kebijakan sektor pertahanan, setidaknya sejak 2008. UU Pengelolaan

Sumber Daya Nasional (PSDN) tahun 2019 menjadi regulasi setingkat UU pertama yang memasukkan ancaman siber sebagai ancaman pertahanan. UU tersebut menambah ancaman hibrida untuk melengkapi dua jenis ancaman yang dimuat di UU Pertahanan Negara (Hanneg) tahun 2002 serta UU TNI, yaitu ancaman militer dan nonmiliter. Namun, UU PSDN tidak menyebutkan ancaman siber masuk dalam kategori ancaman apa, sehingga merancukan respons yang proporsional dan di mana pelibatan TNI diperlukan. Dalam kerangka hukum Indonesia, ancaman militer menempatkan TNI sebagai komponen utama, sementara ancaman nonmiliter akan terlebih dahulu menempatkan kementerian atau lembaga lain non pertahanan menjadi unsur utama dan TNI menjadi unsur pendukung.

Dalam konteks hubungan sipil-militer Indonesia, pembagian peran ini adalah bagian tidak terpisahkan dari proses reformasi TNI, yang bersamaan dengan jatuhnya Orde Baru di tahun 1998 dan berakhirnya doktrin Dwifungsi. Pemahaman terhadap ancaman hibrida dalam regulasi Indonesia mengusutkan upaya tersebut. Sebelum disebut dalam UU PSDN, terminologi ancaman hibrida sendiri sudah cukup sering dimuat pada dokumen-dokumen strategis sektor pertahanan yang dirilis sebelum tahun 2019. Ancaman hibrida didefinisikan sebagai ancaman yang bersifat campuran dan keterpaduan antara ancaman militer dan nonmiliter. Namun, dalam menghadapi ancaman tersebut, TNI dimandatkan menjadi komponen utama selayaknya menghadapi ancaman militer. Operasionalisasi respons terhadap ancaman siber ini semacam membuka kotak pandora pelibatan TNI di luar sektor pertahanan, selayaknya doktrin Dwifungsi.

**Tabel 1. Kategorisasi Ancaman Siber dalam UU Hanneg, UU TNI, dan UU PSDN dan Ancaman Siber**

| | | UU Hanneg 2002 | UU TNI 2004 | UU PSDN 2019 | UU TNI 2025 |
|---|---|---|---|---|---|
| Jenis Ancaman | Ancaman militer | Masuk dalam kategori spionase dan sabotase | Masuk dalam kategori spionase dan sabotase | - Ancaman siber disebutkan sebagai jenis ancaman<br>- Ancaman hibrida pertama kali disebutkan; TNI menjadi komponen utama | - Masuk dalam kategori spionase dan sabotase<br>- Ancaman Pertahanan Siber sebagai bagian dari OMSP |
| | Ancaman nonmiliter | Membahas tetapi tidak menjelaskan lebih jauh | Tidak membahas ancaman nonmiliter | | Tidak membahas ancaman nonmiliter |
| | Ancaman hibrida | Tidak membahas ancaman hibrida | Tidak membahas ancaman hibrida | | Tidak membahas ancaman hibrida |

Sumber: Olahan tim penulis dari berbagai sumber

Di level UU, ancaman siber sendiri tidak dikategorisasi secara khusus menjadi salah satu dari tiga jenis ancaman di atas. UU PSDN menyebutkan serangan siber sebagai salah satu dari 15 contoh ancaman yang dihadapi Indonesia, namun tidak memasukkannya dalam kategori ancaman tertentu. Di level kebijakan pelaksana, ancaman siber sedikit lebih eksplisit dijelaskan sebagai bagian ancaman hibrida. Misalnya dalam Kebijakan Penyelenggaraan Pertahanan 2015-2019 yang dirilis Kemhan pada tahun 2015, menyebutkan ancaman hibrida berwujud kombinasi antara ancaman konvensional, asimetris, teroris, *cyber warfare*, serta kriminal bersenjata. Meskipun demikian, dokumen tersebut tidak menjelaskan lebih jauh seperti apa contoh riil dari ancaman tersebut serta bagaimana pemerintah mendefinisikan peperangan siber.

Dokumen-dokumen strategis di periode serupa menyebutkan kecenderungan konflik kontemporer yang berusaha menghindari jumlah korban dan biaya perang yang tinggi, sehingga digunakan 'senjata' jenis lain untuk mencapai tujuan strategis sebuah aktor. Strategi Pertahanan Negara 2014 dan Buku Putih Pertahanan Indonesia 2015 secara eksplisit menyebutkan ruang siber bisa dimanfaatkan untuk propaganda untuk memecah belah komponen bangsa dan menghadirkan kekacauan politik, seperti pada fenomena *Arab Spring*. Dalam konteks yang lebih dekat dengan situasi Indonesia, isu pelanggaran hak asasi manusia (HAM) dan proses demokratisasi, dengan contoh kemerdekaan Timor Leste di tahun 1999, menjadi perhatian utama dari ancaman nonmiliter sebagai bagian dari pergeseran konflik modern. Beberapa pejabat tinggi militer juga menyebutkan kemungkinan 'balkanisasi', yaitu perpecahan wilayah di Indonesia, sebagai ancaman utama yang harus dihadapi di ruang siber.[13]

Selain itu, dokumen Buku Putih 2008 dan Kebijakan Umum Penyelenggaraan Pertahanan Negara (Jakumhanneg) 2010-2014 membagi ancaman nonmiliter, sebagaimana disebut dalam UU Hanneg, ke dalam tujuh dimensi. Ketujuh dimensi ini adalah ideologi; politik; ekonomi; sosial budaya; hukum; informasi dan teknologi; serta keamanan, yang mana merupakan pengembangan Panca Gatra dari konsep Wawasan Nusantara.[14] Meskipun demikian, kedua dokumen tersebut tidak secara eksplisit memasukkan ancaman siber dalam dimensi tertentu. Baru pada dokumen-dokumen yang dikeluarkan setelahnya—yang tetap menggunakan pembagian tujuh dimensi ancaman nonmiliter—ancaman siber dimasukkan ke dalam dimensi teknologi, seperti tertuang dalam Pedoman Strategis Pertahanan Nirmiliter 2016. Dokumen tersebut menjelaskan salah satu bentuk ancaman tersebut adalah "penyalahgunaan teknologi informasi melalui berbagi media internet untuk tujuan propaganda, intimidasi, menyesatkan yang dapat mendorong gerakan sosial yang mengancam kedaulatan negara". Penjabaran serupa ditemukan pada Jakumhanneg 2020-2024. Dengan begitu, terlihat bagaimana dokumen-dokumen strategis sektor pertahanan menitikberatkan ancaman di ruang siber yang berpotensi menghadirkan gangguan keutuhan bangsa yang dilakukan oleh aktor luar negeri sebagai wujud dari perang proksi.

Meskipun demikian, beberapa dokumen strategis sudah mencoba menyentuh bagaimana Indonesia mencoba beradaptasi dan mengintegrasikan peperangan

siber k e dalam TNI. Buku Putih 2015, misalnya, menyebutkan siber sebagai domain kelima dalam peperangan. Sebelumnya, terdapat pula dokumen Pedoman Pertahanan Siber di tahun 2014 yang secara umum lebih bersifat sebagai pedoman teknis pengamanan jaringan di lingkungan pemerintah dan sektor pertahanan secara umum. Terbaru dokumen Kebijakan Penyelenggaraan Pertahanan Negara (Jakgarahanneg) 2020-2024 menyebutkan rencana untuk mengembangkan teknologi untuk perang siber, termasuk kemampuan ofensif. Namun, dokumen-dokumen tersebut tidak menjelaskan lebih jauh strategi dan doktrin Indonesia berkaitan dengan perkembangan peperangan siber. Lebih jauh, postur TNI tidak pernah benar-benar dibangun untuk melakukan peperangan siber maupun kemampuan bertempur berbasis jaringan, terutama karena keterbatasan anggaran.[15] Dengan begitu, peperangan siber tidak lebih dari sekadar jargon dalam dokumen-dokumen strategis tersebut, tanpa peta jalan yang jelas bagaimana betul-betul diintegrasikan ke dalam kapasitas TNI.

**Gambar 1. Pemetaan Perspektif Ancaman Siber dalam Dokumen Strategis**


Sumber: Olahan tim penulis dari berbagai sumber

Luasnya interpretasi ancaman siber ditambah ketidakseriusan membangun kapasitas operasi siber TNI di luar jargon menghadirkan tanda tanya akan di mana sejatinya operasi siber TNI bisa dilakukan. OMSP Siber yang diatur melalui revisi UU TNI 2025 menyebutkan ancaman pertahanan siber sebagai 'ancaman siber pada sektor pertahanan'. Dengan begitu, UU TNI 2025 justru bisa mengecilkan ruang operasi siber TNI, yaitu hanya untuk menghadapi serangan terhadap jaringan militer, apalagi jika melihat konteks penggunaan kata 'pertahanan' dan 'keamanan' dalam sistem regulasi Indonesia. Semestinya, terjemahan sempit terhadap ancaman pertahanan siber tersebut sudah bisa diatur melalui ketentuan di UU Hanneg dan UU TNI. Kedua UU tersebut menyebutkan ancaman sabotase dan spionase sebagai bagian dari ancaman militer yang menjadi tanggung jawab TNI. Kedua jenis ancaman tersebut serupa dengan pembagian dua jenis operasi siber ofensif Daniel Moore, yaitu *event-based* (sabotase) dan *presence-based* (spionase).[16] Jika interpretasi ancaman militer berupa spionase dan sabotase bisa juga mencakup ancaman siber ke infrastruktur pertahanan negara, penambahan OMSP Siber

di revisi UU TNI 2025 menjadi tidak signifikan. Operasi siber TNI, terutama yang bersifat defensif, semestinya bisa diatur lebih jauh melalui kebijakan turunan UU Hanneg dan UU TNI.

Terdapat beberapa implikasi dari pemetaan ancaman siber dalam beberapa UU sektor pertahanan. Pertama, pemerintah dan DPR tidak berhasil menjelaskan skenario ancaman siber seperti apa yang harus dihadapi sehingga membutuhkan revisi UU TNI 2025 dan menambahkan operasi menghadapi 'ancaman pertahanan siber' ke dalam OMSP. Naskah Akademik revisi UU TNI, yang sempat dipublikasikan di situs DPR, juga tidak sama sekali membahas ancaman siber untuk memberi penjelasan lebih jauh mengenai penambahan OMSP tersebut. Jika konsisten dalam penggunaan kata pertahanan dalam tata kelola sektor pertahanan terutama pasca reformasi, 'ancaman pertahanan siber' seharusnya merujuk kepada serangan siber yang diarahkan kepada TNI, baik di dalam situasi konflik maupun damai. Dengan interpretasi tersebut, TNI semestinya sudah cukup untuk menggunakan UU Hanneg dan UU TNI 2004 sebagai landasan melakukan operasi siber defensif menghadapi spionase dan sabotase.

Kedua, belum jelasnya kerangka regulasi yang ada dalam mendefinisikan apa itu ancaman hibrida bisa berpengaruh pada kegamangan respons terhadap tingkat ancaman siber yang berbeda-beda. Diperkenalkannya ancaman hibrida sebagai salah satu kategori ancaman semestinya juga diperjelas dengan gradasinya, terutama menghindari simtom menjadikan TNI sebagai jawaban atas berbagai masalah. UU PSDN dan berbagai kebijakan turunan sektor pertahanan sepertinya mendefinisikan ancaman hibrida sebagai ancaman nonmiliter yang dilakukan oleh aktor militer negara lain. Definisi ini menjadikan ancaman hibrida sebagai tanggung jawab TNI, terutama karena faktor pelaku serangan. Tantangan utama memasukkan ancaman siber, di luar pertahanan siber, ke dalam ancaman hibrida adalah sifat dasar konflik di ruang siber di mana atribusi sulit dilakukan.[17] Sulit untuk langsung mengetahui apakah pelaku serangan adalah betul-betul militer negara lain, terafiliasi aparatus keamanan, atau aktor ancaman lainnya. Jika dikaitkan dengan OMSP Siber dalam UU TNI 2025, terdapat jarak antara dengan interpretasi ancaman hibrida, di mana yang pertama berfokus pada objek dari ancaman siber sementara ancaman hibrida berfokus pada aktor ancamannya sendiri. Ketiadaan definisi yang pasti terhadap ancaman hibrida serta faktor interpretasi Kemhan dan TNI terhadap ancaman di ruang siber membuat fokus OMSP Siber juga menjadi tidak jelas, apakah hanya pada peperangan siber (*cyber warfare*) atau ancaman siber yang lebih luas.

**Tabel 2. Otoritas Operasi Siber TNI berdasarkan UU Hanneg, UU TNI, dan UU PSDN**

| | | Sasaran | | | |
|---|---|---|---|---|---|
| | | Jaringan Militer | Jaringan Pemerintahan Sipil | Infrastruktur Kritis | Kepercayaan Publik (melalui peperangan informasi) |
| **Aktor/ Pelaku** | Militer negara lain | Ya | Ancaman Hibrida | Ancaman Hibrida | Ancaman Hibrida |
| | Terafiliasi negara atau instansi intelijen sipil | Ya | Tidak | Tidak | Tidak |
| | Lainnya | Ya | Tidak | Tidak | Tidak |

Sumber: Olahan tim penulis dari berbagai sumber

Ketiga, menjadikan operasi siber, terutama ofensif, sebagai OMSP Siber bisa dipahami sebagai usaha pemerintah untuk mengategorikannya sebagai sebuah operasi di bawah ambang batas perang. Batas antara konflik dan damai di ruang siber sangat kabur, sehingga negara-negara seperti AS melihatnya sebagai ruang yang mengalami kontestasi secara terus menerus. Jika OMSP Siber menggunakan pendekatan yang sama, pemerintah harus bisa mengoperasionalisasikannya melalui kebijakan turunan sektor pertahanan, selayaknya AS melalui dokumen Strategi Siber yang dikeluarkan oleh Departemen Pertahanan yang menyebutkan doktrin *Defend Forward*. Namun, dokumen-dokumen tersebut di Indonesia belum bisa menggambarkan pendekatan yang jelas dari pemerintah Indonesia melihat persaingan di ruang siber. Padahal kerancuan definisi serta cakupan dari ancaman pertahanan siber, operasi siber TNI hingga ancaman hibrida semestinya bisa dijelaskan lebih jauh melalui kebijakan turunan tersebut. Hal ini didukung kenyataan bahwa perubahan ancaman siber dan perkembangan teknologi terjadi sangat cepat, sehingga proses pembuatan dan revisi UU biasanya akan tidak cukup cepat mengantisipasinya. Kebijakan turunan dalam bentuk dokumen-dokumen strategis tersebut bisa dikeluarkan secara berkala ataupun sesuai kebutuhan khusus dari pemerintah.

## Kematangan Siber TNI

Tahapan selanjutnya adalah mengkaji kematangan siber dalam tubuh TNI. Analisis ini bisa dilakukan dengan merujuk kepada kerangka yang diciptakan Blessing dan Austin (2020) di mana terdapat tiga dimensi utama, yaitu strategis, institusional, dan kapabilitas.[18] Dimensi strategis berfokus kepada bagaimana organisasi militer dan pemimpinnya memiliki rencana yang jelas mengenai pengembangan dan penggunaan kemampuan siber. Pengembangan doktrin penggunaan kemampuan siber menjadi indikator utama dalam dimensi ini. Dimensi institusional melihat seberapa efektif organisasi militer menyiapkan kekuatannya, mulai dari perencanaan hingga eksekusi operasi siber untuk mendukung tujuan strategis sebuah negara. Indikator yang bisa digunakan misalnya perkembangan organisasi siber dalam tubuh TNI, termasuk dalam pelatihan dan hubungannya dengan institusi sipil siber lainnya. Terakhir, dimensi kapabilitas menyoroti adanya infrastruktur siber yang memadai untuk melakukan operasi ofensif dan defensif, termasuk personilnya. Dalam kajian ini, kemapanan tersebut dilihat melalui latihan bersama dengan negara lain.

Tentu tidak semua faktor yang ditulis oleh Blessing dan Austin bisa digunakan dalam konteks Indonesia. Dalam dimensi strategis, kebijakan anggaran untuk organisasi militer di tubuh TNI bukanlah sesuatu yang bisa dikaji oleh publik. Berbagai barometer pada dimensi institusional dan kapabilitas juga merujuk kepada transparansi hubungan antara intelijen dan militer dalam melakukan operasi siber ofensif, sesuatu yang belum dikaji dalam konteks Indonesia secara menyeluruh. Meskipun demikian, kerangka keduanya tetap bisa digunakan untuk memandu faktor-faktor utama yang perlu diamati lebih jauh.

Seperti dokumen strategis pemerintah sektor pertahanan yang telah dibahas sebelumnya, terminologi siber juga telah dimuat dalam Doktrin TNI Tri Dharma Eka Karma (TRIDEK) 2018, Doktrin TNI AD Kartika Eka Paksi 2018, Doktrin TNI AU Swu Bhuwana Paksa 2019, dan Doktrin TNI AL Jalesveva Jayamahe 2018. Pembahasan ruang siber di Doktrin TNI umumnya masih menyerupai dokumen-dokumen strategis pertahanan seperti Buku Putih dan Jakumhanneg yang telah dibahas sebelumnya. Terorisme dan perang siber dikategorikan menjadi ancaman nonmiliter berdimensi teknologi, meskipun perang siber kemudian juga disebut sebagai bagian dari ancaman hibrida. Selain itu, penjabaran ancaman nonmiliter berdimensi sosial budaya menyebutkan ancaman berupa “penggunaan teknologi informasi yang dapat memicu terjadinya benturan antar peradaban...”, yang mana kemudian juga disinggung pada Doktrin TNI AD dan Doktrin TNI AU. Uniknya, Doktrin TNI AD juga menempatkan siber dalam jenis ancaman militer non agresi, sebuah kategorisasi baru dibandingkan dokumen-dokumen yang telah dibahas sebelumnya. Adapun Doktrin TNI AL tidak menyinggung tipologi jenis ancaman.

Doktrin TNI AU dan TNI AL menyebut kemampuan siber sebagai bagian dari kemampuan dukungan masing-masing matra, terutama mengingat sifat peperangan di dua domain tersebut sangat bergantung pada teknologi mutakhir. Doktrin dari kedua matra tersebut merefleksikan bagaimana ruang

siber bisa dilihat sebagai 'pengganda kekuatan' dalam peperangan modern. TNI AU, misalnya, menyebutkan terminologi keunggulan informasi (*information superiority*) sebagai prasyarat utama mencapai keunggulan udara (*air superiority*). Disebutkan bahwa keunggulan informasi akan membantu menyasar target secara akurat, sebuah pendekatan yang menjadikan ruang siber sebagai bagian integral dari cara berperang TNI AU. Bahkan, doktrin tersebut menyinggung kemampuan untuk melakukan serangan balik (*counter-measures*) dalam melindungi serangan jaringan TNI AU. Sementara itu, doktrin TNI AL melihat teknologi siber dapat menjadi pengganda kekuatan untuk menyerang pusat kekuatan lawan, meskipun tidak sedalam TNI AU menjelaskan integrasinya dalam cara berperang.

Doktrin TNI AD, di sisi lain, menyebut ruang siber dan peperangan siber sebagai bagian yang tidak terpisahkan dari perang masa depan untuk menunjang peperangan berbasis jaringan dan operasi multi-ranah. Doktrin tersebut juga membagi tiga jenis operasi siber TNI AD, yaitu siber persandian (defensif pasif), siber penangkalan (defensif aktif), dan penindakan siber (ofensif). Pembagian jenis-jenis operasi siber ini tidak ditemukan dalam dokumen doktrin lainnya. Sebagai matra yang akan menjadi tumpuan utama dalam melakukan perang berlarut, Doktrin TNI AD juga sudah memasukkan dimensi siber dalam pembinaan teritorial meskipun tidak ditarik ke dalam penangkalan menghadapi operasi informasi dari aktor-aktor ancaman. Doktrin tersebut jika tidak menjelaskan bagaimana TNI AD akan melakukan perang gerilya dalam kondisi ruang siber dikuasai lawan secara utuh sehingga harus bergantung kembali kepada teknologi analog untuk melakukan komunikasi dan koordinasi.

Dengan begitu, telaah doktrin di TNI memperlihatkan bahwa terdapat aspirasi mengintegrasikan peperangan siber dalam cara berperang TNI, terutama pada TNI AU dan AD. Interpretasi ancaman dari ruang siber yang bisa mengakibatkan perpecahan juga tetap ditemukan dalam doktrin-doktrin tersebut. Meskipun begitu, tidak dijabarkan lebih jauh seperti apa respons TNI menghadapi ancaman operasi informasi, meski tingginya perhatian kepada isu tersebut. Situasi ini menghadirkan kondisi yang berpotensi bisa menjadi permasalahan dalam interpretasi batas operasi siber TNI dalam ruang siber, terutama yang berhubungan dengan masyarakat sipil.

Untuk dimensi institusional, dinamika organisasi TNI telah mengalami perkembangan yang cukup berarti dalam beberapa tahu terakhir. Salah satu yang cukup menyita perhatian publik adalah wacana pembentukan angkatan siber menjadi matra ke-empat TNI. Ide ini pertama kali diutarakan pada tahun 2023 oleh Gubernur Lemhannas saat itu, Andi Widjajanto. Terinspirasi dari pembentukan *Digital and Intelligence Service* (DIS) sebagai matra siber dalam angkatan bersenjata Singapura (SAF), Andi membayangkan proses transisi untuk pembentukan angkatan siber memerlukan waktu setidaknya lima tahun. Selanjutnya, Bambang Soesatyo selaku Ketua Majelis Permusyawaratan Rakyat (MPR) 2019-2024, mengingatkan kembali pentingnya rencana pembentukan angkatan siber dalam rapat tahunan MPR tahun 2024. Bambang sendiri sebelumnya menggarisbawahi keperluan melakukan amandemen Undang-

Undang Dasar (UUD) 1945 untuk mendorong hal tersebut, dikarenakan konstitusi Indonesia menyebutkan TNI terdiri dari tiga matra.[19]

Jelang pergantian pemerintahan, Presiden Joko Widodo (Jokowi) menyebutkan bahwa dirinya akan menyerahkan pembentukan angkatan siber tersebut kepada Presiden Prabowo. Sebelumnya, Panglima TNI Agus Subiyanto dan Menkopolhukam Hadi Tjahjanto menyebutkan persiapan dan studi dari wacana tersebut sudah dilakukan, mengikuti instruksi dari presiden.[20] Namun, Menteri Pertahanan Sjafrie Sjamsoeddin sepertinya tidak melihat kegentingan pembentukan angkatan siber dan berfokus pada penguatan satuan siber yang sudah ada.[21] Presiden Prabowo sendiri tidak pernah secara eksplisit menyebutkan ketertarikannya untuk melanjutkan ide dari pemerintahan Presiden Jokowi tersebut.

Meskipun demikian, kesadaran untuk pengembangan organisasi dan personil siber di tubuh TNI tetap kuat. Saat ini, Kemhan, Mabes TNI, TNI AD, TNI AL dan TNI AU memiliki satuan sibernya sendiri dengan kematangan kapasitas, kuantitas personil, serta level unitnya masing-masing. Pushansiber, Satsiber TNI, Pusansiad, Pusanal, serta Satsiberau seluruhnya dipimpin oleh bintang satu. Organisasi siber di tubuh TNI, baik di Mabes maupun masing-masing matra, merupakan Badan Pelaksana Pusat (Balakpus) yang berada langsung di bawah Panglima TNI dan kepala staf masing-masing. Untuk Mabesad terdapat Pusat Komunikasi dan Elektronika (Puskomlek) TNI AD yang dipimpin oleh Bintang 2 dan juga memiliki fokus terhadap isu siber. Lebih jauh, Mabesad telah mengubah korps Perhubungan (CHB) menjadi Komunikasi dan Elektronika (CKE), menyerupai AL dan AU yang menggunakan korps Elektronika, yang menunjukkan adaptasi matra tersebut terhadap isu peperangan siber dan upaya mendorong personil untuk memiliki kekhususan pada bidang tersebut. Sementara TNI AU merupakan satu-satunya mabes yang sudah memiliki skuadron pendidikan siber.[22]

Untuk TNI AL dan AU, organisasi sibernya baru saja mengalami validasi organisasi, di mana sebelumnya dipimpin oleh Kolonel dan berada di bawah Pusat Pengamanan Sandi (Puspamsan) masing-masing.[23] Namun, perkembangan tersebut terasa minor jika dibandingkan dengan perubahan organisasi militer yang telah dilakukan oleh pemerintahan Presiden Prabowo, seperti penambahan jumlah Komando Distrik Militer (Kodam) serta ekspansi pasukan khusus di masing-masing matra. Validasi organisasi siber di Mabesal dan Mabesau juga tidak bisa dilihat sebagai terobosan, karena sejatinya hanya menyeragamkan dengan Mabes TNI dan Mabesad. Hal ini menunjukkan bahwa fokus penguatan TNI belum betul-betul menyentuh organisasi siber, bahkan sangat dipengaruhi faktor Presiden Prabowo yang berusaha mendorong pelibatan TNI di isu-isu sipil seperti membantu program Makan Bergizi Gratis (MBG) hingga penertiban lahan kehutanan untuk perkebunan sawit.[24]

**Gambar 2. Organisasi Siber Kemhan dan TNI**

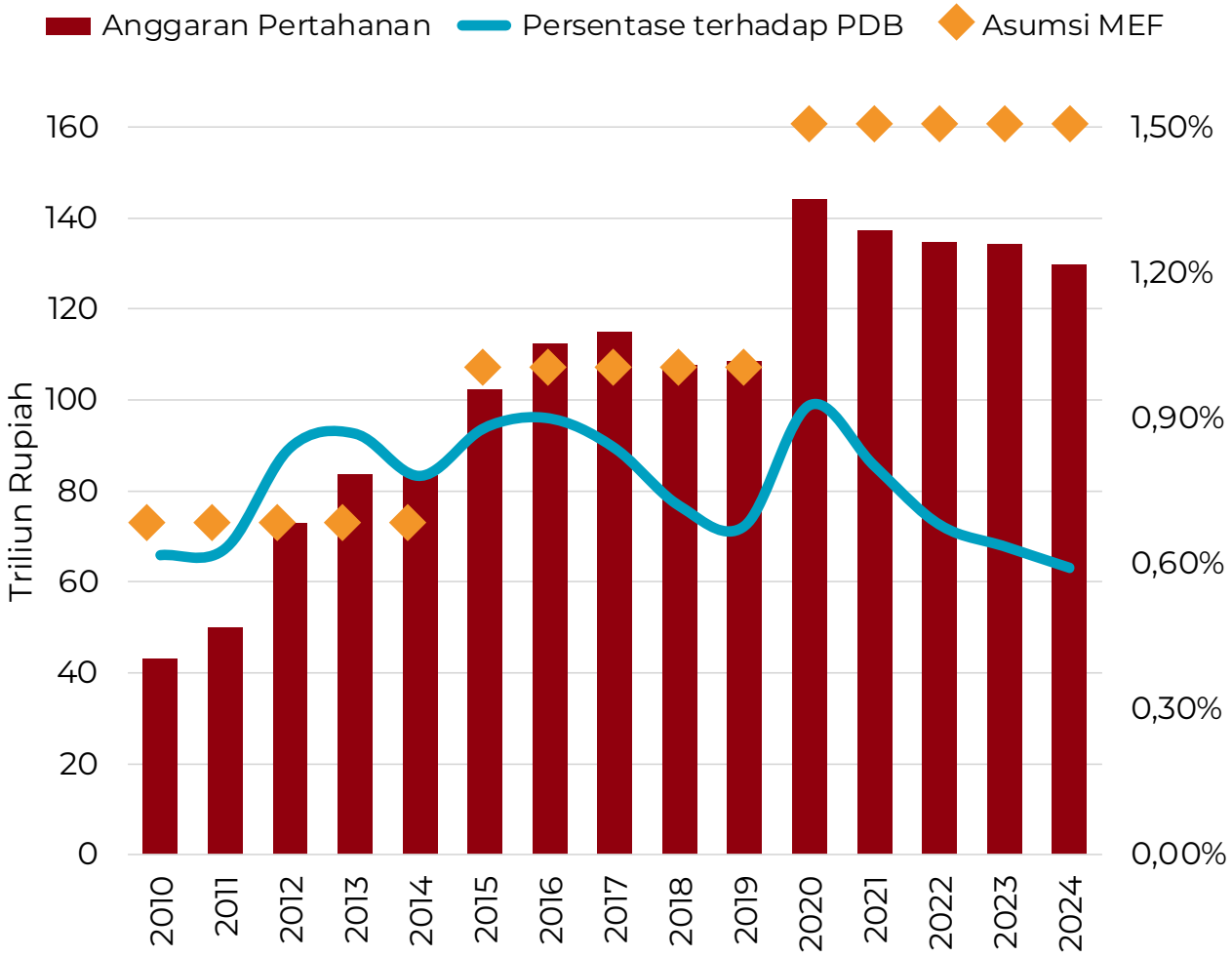

Sumber: Olahan tim penulis dari berbagai sumber

Sementara itu, Pushansiber adalah instansi penjuru untuk pengamanan jaringan di sektor pertahanan. Hal ini didasari oleh Peraturan Presiden tentang Perlindungan Infrastruktur Informasi Vital, di mana sektor pertahanan menjadi salah satu dari delapan sektor strategis dan Kemhan menjadi koordinatornya. Pushansiber sendiri didirikan sejak tahun 2014 oleh Menteri Pertahanan Purnomo Yusgiantoro sebagai respons terhadap berita peretasan Presiden Susilo Bambang Yudhoyono (SBY) oleh intelijen Australia. Awalnya, satuan ini bahkan dibentuk untuk mengkoordinasikan pengamanan seluruh jaringan pemerintah, tugas yang kemudian diemban oleh Badan Siber dan Sandi Negara (BSSN) yang didirikan tahun 2017 sebagai perkembangan dari Lembaga Sandi Negara (Lemsanneg).[25] Namun, operasional Pushansiber sendiri sempat terhambat akibat ketiadaan dukungan pendanaan dan baru dalam beberapa tahun terakhir meningkatkan kapasitas infrastruktur dan menambah jumlah personilnya. Tantangan yang serupa juga dihadapi oleh Satsiber TNI. Didirikan sejak tahun 2017, satuan tersebut hanya mampu mengisi 35,9% kebutuhan personalianya sebanyak 178. Sebagai perbandingan, DIS Singapura memiliki pasukan kurang lebih 1000 prajurit.[26] Hal ini, sekali lagi, menunjukkan belum adanya prioritas dari pemerintah dan pimpinan Mabes TNI untuk membangun kapasitas siber yang mumpuni di tubuh organisasinya.

Tertatih-tatihnya pembangunan kemampuan siber TNI tidak bisa dipisahkan dari mandeknya modernisasi TNI secara umum. Pemenuhan Kekuatan Pertahanan Minimum (*Minimum Essential Force* atau MEF) yang seharusnya selesai di tahun 2024 yang lalu tidak pernah betul-betul tercapai akibat ketiadaan komitmen anggaran dari pemerintah terhadap sektor pertahanan.[27] Faktor ekonom makro membuat Indonesia tidak bisa mencapai target pengeluaran sektor pertahanan

sebesar 1.5 % dari PDB, prasyarat utama untuk melakukan modernisasi. Hal ini juga disinggung oleh Blessing dan Austin, di mana proses modernisasi militer sangat mempengaruhi kematangan siber suatu organisasi militer, di mana keduanya mencontohkan proses modernisasi angkatan bersenjata Tiongkok (PLA) sebagai bagian tidak terpisahkan dari pengembangan kekuatan sibernya.[28]

**Gambar 3. Proporsi Anggaran Pertahanan Terhadap PDB 2010-2024[29]**




Bagian lain yang tidak bisa dipisahkan dar dimensi ini adalah isu personil dan jenjang karier prajurit di bidang siber. Satsiber TNI, sebagai sebuah unit di bawah Mabes TNI, diisi oleh personil yang berasal dari matra darat, laut, maupun udara karena bentuknya yang bukan matra independen. Dampaknya, personil Satsiber akan mengalami mutasi kembali sesuai dengan jenjang karier di Mabes masing-masing angkatan. Hal ini berakibat tidak adanya keberlanjutan pengalaman organisasi, terutama di level pimpinan. Perbedaan melihat isu peperangan dan operasi siber pada doktrin masing-masing markas besar juga menjadi tantangan tersendiri bagi Satsiber untuk mengembangkan kemampuan siber yang ideal. Dalam merespons tantangan personil ini, Panglima TNI telah mengeluarkan kebijakan untuk melakukan rekrutmen masyarakat sipil ke dalam TNI untuk bertugas di satuan siber tersebut.[30] Namun, perekrutan tersebut justru memperlihatkan permasalahan lain dalam isu talenta siber di tubuh TNI, di mana Satsiber bergantung kepada matra

lain dalam hal pembinaan personil di mana pendidikan bagi rekrutan sipil tersebut dilakukan di Skuadron Pendidikan Siber AU.

Dimensi institusi ini juga melihat bagaimana hubungan organisasi militer dengan institusi sipil dalam melakukan misi operasi siber. Dalam konteks Indonesia, hal ini cenderung tidak relevan. Namun, terdapat beberapa kondisi yang perlu menjadi pertimbangan. Pertama, isu tata kelola keamanan siber di Indonesia yang belum terselesaikan tanpa adanya regulasi level UU yang secara jelas mendefinisikan peran masing-masing institusi dalam ruang siber Indonesia. Meskipun sektor pertahanan sudah jelas menjadi ranah TNI, ketiadaan regulasi yang jelas membuat batasan keterlibatan TNI menghadapi ancaman siber lainnya menjadi buram. Kedua, institusi utama dalam ruang siber seperti BSSN dan Badan Intelijen Nasional (BIN) sudah diisi oleh prajurit TNI aktif seperti diatur oleh UU TNI. Hal ini membuat koordinasi di level menengah cenderung lebih baik karena dilakukan oleh sesama prajurit TNI. Ketiga, pemerintahan Prabowo menghadirkan wadah yang bisa menjadi pusat fusi siber dan sarana melakukan pertukaran informasi, yaitu Dewan Pertahanan Nasional dan Satuan Tugas Siber dan Kecerdasan Artifisial Terpadu. Kedua organisasi tersebut diharapkan bisa menjadi substitusi koordinasi kebijakan dan operasi siber antar institusi di Indonesia. Berbagai kondisi di atas memperlihatkan bahwa masih ada batasan-batasan dalam tata kelola ruang siber di Indonesia.

Dimensi terakhir yang juga paling sulit untuk diukur adalah kapabilitas. Blessing dan Austin menyebutkan komponen penting dalam dimensi ini adalah bergerak dari kemampuan mengambil data dari jaringan lawan (spionase) menuju ke kemampuan untuk merusak jaringan lawan (sabotase).[31] Dalam konteks Indonesia, tentu hal ini akan sangat sulit dikaji, terutama dengan alasan terbatasnya informasi mengenai kemampuan tersebut. Sejauh ini kajian terhadap kemampuan siber Indonesia mengisyaratkan adanya kemampuan pengawasan siber untuk kebutuhan keamanan domestik.[32] Pada tahun 2016-2019 Indonesia mengalami berbagai kejadian serangan teror dari kelompok teror berbasis agama yang direspons oleh pemerintah saat itu dengan berbagai kebijakan, termasuk merevisi UU Pemberantasan Tindak Pidana Terorisme pada tahun 2018, yang mencoba mengatur tata kelola lembaga dan pelibatan TNI dalam menghadapi aksi teror.[33] Tidak lama berselang, pemerintah membentuk Komando Operasi Khusus (Koopsus) TNI yang berfokus menghadapi terorisme.[34] Keadaan tersebut menjadi konteks utama pembentukan Satsiber TNI pada tahun 2017, sekaligus menjadi gambaran bagaimana kapasitas siber TNI dikembangkan dengan pendekatan ancaman yang *inward-looking*. Meskipun demikian, sifat operasi siber yang sangat klandestin membuat kajian mendalam mengenai kapabilitas siber TNI menjadi sulit dilakukan.

Namun, Blessing dan Austin juga menyebutkan bahwa indikator lain yang bisa digunakan adalah berbagai latihan siber oleh militer. Di luar latihan-latihan internal, TNI telah melakukan berbagai latihan bersama dengan berbagai negara, terutama negara yang telah memiliki kematangan siber pada institusi militernya.

**Tabel 3. Latihan Siber TNI dengan Negara Lain**

| Nama Kegiatan | Tahun | Jenis | Mabes | Unit Peserta | Negara Lain |
|---|---|---|---|---|---|
| Gema Bhakti | 2017-2022 | Latihan Gabungan | TNI | Mabes TNI dan 3 matra | Amerika Serikat |
| Information System and Technology Exchange (ISTX) | 2018-2019 | Pelatihan Bilateral | TNI | Mabes TNI dan 3 matra | Amerika Serikat |
| BAE Systems Applied Intelligence (BAEs-AI) | 2019 | Pelatihan Bilateral | Kemhan | Pushansiber Bainstrahan | Inggris |
| Command, Control, Communications and Computer System (C4S) Subject Matter Expert Exchange (SMEE) | 2021 | Pertemuan Bilateral | AD | AD | Filipina |
| Cyber SMEE (Subject Matter Expert Exchange) | 2022 | Pertemuan Bilateral | AD | Mabes AD | Amerika Serikat |
| Army Cyber Commander Training Course | 2023 | Pelatihan Bilateral | AD | Pusat Sandi dan Siber TNI Angkatan Darat (Pussansiad) | Inggris |
| Super Garuda Shield | 2024 | Latihan Gabungan | TNI | Semua unit | Amerika Serikat |
| Cobra Gold | 2025 | Latihan Gabungan | AD | Staf Latihan TNI AD (Slatad) | Thailand, Amerika Serikat |
| Defense Cyber Marvel | 2025 | Pelatihan Bilateral | TNI | Pussansiad | Inggris |

Sumber: Olahan tim penulis dari berbagai sumber

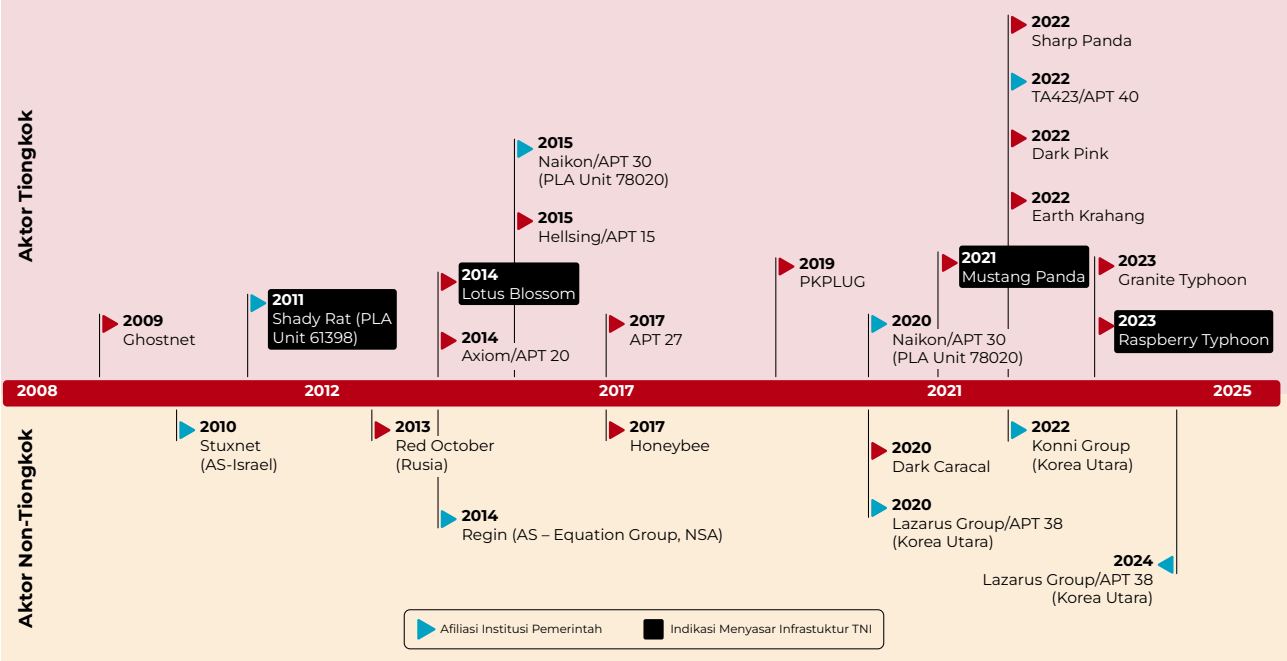
Latihan dengan berbagai negara lain sebagian besar berfokus pada latihan gabungan dengan isu yang cenderung lebih umum dibanding siber, namun ruang siber memiliki peran penting di dalamnya. Latihan seperti Cobra Gold dan Super Garuda Shield mendorong lebih jauh lagi adaptasi ruang siber sebagai pelipat ganda kekuatan dalam operasi militer modern.[35] Selain itu, terdapat juga berbagai latihan dan pertemuan spesifik secara bilateral yang berfokus pada seminar, berbagi informasi, dan penguatan kebijakan dengan skala yang lebih kecil. Defense Cyber Marvel maupun ISTX menjadi contoh dari jenis latihan ini, di mana lebih berfokus kepada operasi siber defensif untuk mengamankan dan mendeteksi ancaman terhadap jaringan militer.[36]

Sejauh ini, mayoritas partner utama dalam latihan-latihan tersebut adalah negara Barat ataupun negara yang secara geopolitik dekat dengan blok Barat. Amerika Serikat dan Inggris menjadi negara mitra utama bagi TNI untuk melakukan latihan siber, merefleksikan sejarah panjang penguatan kapasitas serta menunjukkan komitmen diplomasi pertahanan siber yang dilakukan oleh kedua negara. Meskipun demikian, terdapat dua hal yang harus diperhatikan dalam melihat pengaruh latihan-latihan tersebut dalam pengembangan kapasitas operasi siber maupun integrasi peperangan siber ke dalam tubuh TNI. Pertama, kebijakan luar negeri bebas aktif Indonesia dan upaya Indonesia untuk 'mengayuh di antara dua karang' membuat proses latihan serta pembangunan kapasitas dari negara-negara utama tidak akan maksimal. Misalnya, latihan gabungan antar negara-negara aliansi AS bisa lebih fokus ke dalam penggunaan siber sebagai bagian dari peperangan berbasis jaringan dengan skenario musuh yang jelas.[37] Skenario serupa tidak bisa diterapkan di Indonesia, sehingga latihan-latihan bersama dengan komponen siber cenderung tidak terlalu mendalam, seperti latihan *Capture The Flag* (CTF) ataupun *tabletop exercise* (TTX) dengan skenario yang tidak terlalu kompleks. Kedua, faktor personil peserta latihan gabungan yang cenderung selalu berganti membuat sulitnya membangun keberlanjutan dari latihan tersebut. Spesialisasi siber yang belum menjadi sesuatu yang umum di dalam tubuh TNI, sehingga prajurit yang terlibat dalam sebuah latihan gabungan sangat mungkin akan mengalami mutasi ke satuan hingga unit lain yang tidak berhubungan dengan operasi dan peperangan siber. Dengan begitu, latihan-latihan bersama tersebut bisa menjadi tidak terlalu efektif dalam membangun kapasitas siber TNI.

## Pengalaman Ancaman Pertahanan Siber Indonesia

Faktor lain yang mempengaruhi kapabilitas siber adalah pengalaman menghadapi ancaman siber sebelumnya. Posisi geopolitik strategis membuat Indonesia mengalami serangan siber yang konstan dari berbagai grup yang didukung atau terafiliasi aktor negara. Berdasarkan beragam laporan dari berbagai institusi dan perusahaan swasta, spionase menjadi jenis serangan yang paling sering dialami Indonesia, dengan Tiongkok sebagai aktor negara yang paling sering tercatat melakukan operasi.

**Gambar 4. Berbagai Operasi Siber Terafiliasi Negara Lain Terhadap Indonesia**



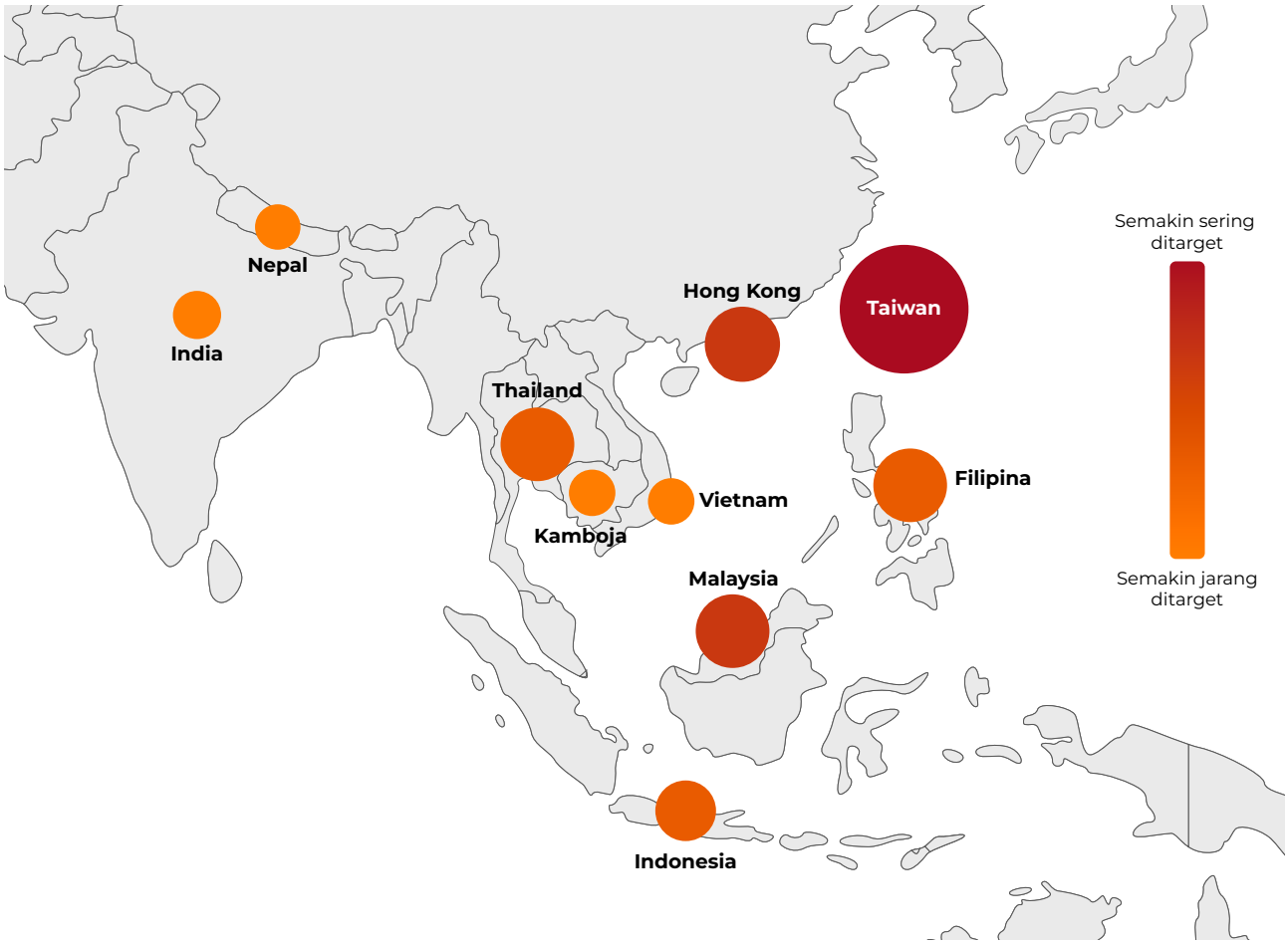

Sumber: Olahan tim penulis dari berbagai sumber

Hal ini juga didukung oleh dokumen Laporan Tahunan BSSN yang selama beberapa tahun terakhir melaporkan temuan aktivitas kelompok *Advanced Persistent Threat* (APT) di dalam jaringan Indonesia.[38] Beberapa serangan bahkan dilaporkan dilakukan oleh aktor yang terafiliasi dengan satuan tertentu dalam angkatan bersenjata negara lain. Meskipun demikian, pemerintah dan TNI cenderung tidak transparan terhadap adanya serangan tersebut. Hal ini cukup besar dipengaruhi oleh secara umum Indonesia tidak mengadopsi kebijakan atribusi terhadap serangan yang dilakukan oleh aktor negara lain.[39] Selain itu, faktor negara asal serangan dari negara-negara yang memiliki sejarah hubungan historis ataupun kedekatan ekonomi dengan Indonesia, yaitu Tiongkok dan Rusia, memiliki peranan penting dalam respons pemerintah dan TNI yang tidak terbuka. Hal ini berbeda jika misalnya dibandingkan dengan bagaimana perseteruan maritim antara Tiongkok dan Filipina yang merembes ke ruang siber mendorong Filipina mengadopsi kebijakan siber yang lebih kuat terhadap Tiongkok.[40]

Konteks lain dari minimnya respons pemerintah terhadap serangan dari kelompok peretas terafiliasi negara lain adalah Indonesia tergolong sebagai negara yang tidak terlalu mendapatkan serangan jika dibandingkan dengan negara-negara lain. Berdasarkan data Juli 2024-Juni 2025, Microsoft menemukan bahwa Taiwan, Korea Selatan dan India menjadi tiga negara utama di kawasan Indo-Pasifik yang ditarget oleh kelompok terafiliasi negara sementara Indonesia berada di peringkat 10.[41] Temuan di tahun sebelumnya juga menunjukkan hal yang sama, bahwa aktivitas kelompok-kelompok tersebut cenderung moderat di Indonesia. Temuan ini sekali lagi menunjukkan bagaimana hubungan geopolitik dan tensi bilateral memiliki pengaruh besar kepada ruang siber dan respons negara-negara kepada aktivitas serangan dari negara lain. Dalam hal ini, ketiadaan persepsi ancaman dan

musuh yang jelas dari kebijakan Indonesia selama ini menghasilkan respons yang terbatas juga terhadap aktivitas berbagai kelompok peretas terafiliasi negara.

**Gambar 5. Aktivitas Kelompok Peretas dari Tiongkok di Sekitar Laut Tiongkok Selatan[42]**




Di luar serangan siber yang bersifat menyerang jaringan strategis, pemerintah dan TNI juga memersepsikan ancaman operasi informasi sebagai fokus, selayaknya tertuang dalam pembahasan dokumen-dokumen strategis serta doktrin di bagian sebelumnya. Pengalaman TNI di Timor Leste, misalnya, menjadi contoh yang acapkali digunakan, bahkan cukup kuat mempengaruhi perspektif peperangan siber TNI hingga sat ini.[43] Di periode tersebut, misalnya, terdapat serangan *web defacements* terhadap situs pemerintah Indonesia, termasuk militer, dengan pesan pro kemerdekaan Timor Leste oleh kelompok peretas Toxyn dari Portugal.[44] Serangan tersebut dianggap berhasil menarik perhatian media internasional dan menyoroti konflik tersebut. Pemerintah serta militer Indonesia kemudian berpandangan bahwa terjadi informasi operasi yang dilakukan oleh kelompok-kelompok tertentu yang ingin memecah belah Indonesia, terutama dari negara-negara Barat, dan berhasil mendukung kemerdekaan Timor Leste melalui operasi di ranah siber.

Uniknya, perspektif terhadap operasi informasi tersebut tidak berlaku untuk semua aktor ancaman. Misalnya, sejauh ini tidak ada respons pemerintah

Indonesia terhadap beberapa laporan mengenai operasi dari Rusia untuk memengaruhi pandangan publik Indonesia mengenai Perang Rusia-Ukraina.[45] Rusia sendiri memiliki rekam jejak yang panjang mengenai operasi informasi, termasuk mempengaruhi hasil referendum Inggris untuk keluar dari Uni Eropa (Brexit) serta Pemilihan Presiden AS tahun 2016 yang lalu.[46] Aktor utama lainnya, seperti Tiongkok, juga dianggap melakukan operasi informasi menarget komunitas muslim di Indonesia terkait perlakuannya terhadap etnis minoritas Uighur.[47] Pemerintah Indonesia dianggap tidak cukup lantang memperjuangkan isu tersebut, terutama jika dibandingkan dengan upaya memperjuangkan kemerdekaan Palestina.[48] Perbedaan respons kepada operasi informasi Rusia dan Tiongkok jika dibandingkan dengan bagaimana peristiwa Timor Leste dan isu hak asasi manusia yang bisa digaungkan oleh negara-negara Barat bisa jadi dipengaruhi oleh sentimen anti Barat yang cukup tinggi di Indonesia, terutama sejak kampanye 'War on Terror' AS yang dianggap menyasar agama Islam.[49] Sehingga, meskipun memberikan perhatian lebih terhadap adanya operasi informasi—sebagai bagian dari spektrum ancaman siber—pemerintah Indonesia cenderung tidak memiliki respons yang cukup kuat, sejalan dengan respons terhadap serangan siber yang menyasar jaringan strategis.

## Kendali Demokrasi dalam Operasi Siber

Terdapat dua pendekatan yang bisa dipakai untuk melihat bagaimana operasi siber dilakukan dalam koridor demokrasi. Pertama, merujuk kepada norma internasional terkait ruang siber. Saat ini, kerangka utama yang telah dikembangkan oleh PBB dikenal sebagai "UN norms of responsible state behaviour in cyberspace" yang terdiri dari 11 norma. Selain itu, terdapat beberapa interpretasi terhadap hukum internasional untuk konflik kinetik yang bisa diterapkan di ruang siber. Sementara pendekatan kedua memperhatikan bagaimana berbagai negara melakukan operasi siber yang bisa dianggap keluar dari koridor demokrasi. Dalam hal ini, fenomena yang akan diamati adalah penggunaan kemampuan siber terhadap aktor berasal dari dalam negeri, sejalan dengan persepsi ancaman Indonesia seperti yang telah dijelaskan sebelumnya. Analisis terhadap kedua pendekatan tersebut akan membantu menciptakan kerangka operasi siber yang berada dalam koridor demokrasi sesuai dengan konteks Indonesia saat ini.

### Tinjauan Norma Internasional

Saat ini tidak ada hukum internasional yang secara khusus mengatur terkait operasi siber. Rezim utama yang kerap menjadi rujukan adalah pembahasan norma internasional tentang perilaku negara yang bertanggung jawab dalam domain siber atau yang dikenal sebagai norma siber yang bersifat sukarela dan tidak mengikat, serta mencerminkan standar harapan masyarakat internasional di tingkat PBB. Saat ini terdapat sebelas norma tanggung jawab negara di ruang yang merupakan prinsip-prinsip non-mengikat yang disepakati dalam forum United Nations Group of Governmental Experts (UN GGE) untuk mendorong stabilitas dan mencegah konflik di dunia maya. UN GGE pertama kali dibentuk

pada 2004, dan hingga 2021 telah berlangsung enam siklus diskusi utama, dengan laporan penting pada 2013, 2015, dan 2021, yang merumuskan 11 norma tersebut.

Meskipun mendapat dukungan luas, norma-norma ini belum secara resmi diadopsi oleh seluruh negara, dan implementasinya bersifat sukarela dengan tingkat komitmen yang bervariasi antar negara.[50] Norma-norma tersebut secara umum berfokus perilaku negara dengan negara lainnya, penegasan bahwa negara tidak boleh dengan sengaja membiarkan wilayah mereka digunakan untuk melakukan tindakan yang salah secara internasional, sekaligus mendorong adanya keputusan yang terukur dapat diambil sebagai tanggapan terhadap serangan siber di mana negara harus mempertimbangkan semua informasi yang relevan, termasuk potensi konsekuensinya sebelum bertindak sebagai sebuah respons.[51]

**Gambar 6. 11 Norma Tanggung Jawab Negara di Ruang Siber[52]**


Dalam konteks Indonesia, kesebelas norma tersebut kurang mendapatkan perhatian dalam proses formulasi kebijakan di Indonesia. Salah satu alasan utamanya adalah fokusnya terhadap pengaruh ruang siber ke kontestasi geopolitik global, sehingga negara berkembang dengan kemampuan siber yang belum mapan seperti Indonesia tidak melihat urgensinya.[53] Namun, dalam pengembangan kebijakan pertahanan siber serta kapasitas operasi siber TNI, terdapat norma utama yang perlu mendapatkan perhatian oleh Indonesia, yaitu norma kelima yang berfokus kepada penghargaan terhadap hak asasi manusia (HAM) dan privasi. Norma tersebut berfokus kepada perlindungan terhadap hak-hak dasar di ranah digital, termasuk kebebasan berpendapat.[54]

Norma ini menekankan bahwa negara harus menjamin penghormatan penuh terhadap hak asasi manusia dalam penggunaan teknologi digital, termasuk hak atas kebebasan berekspresi dan hak atas privasi, sebagaimana diatur dalam

resolusi Dewan HAM dan Majelis Umum PBB. Dalam implementasinya, negara didorong untuk memastikan bahwa hak-hak yang berlaku secara luring juga diterapkan secara daring, serta menghindari praktik seperti pengawasan massal yang sewenang-wenang atau penyensoran yang tidak sah. Lebih jauh, negara juga diharapkan merespons isu keamanan di ruang internet sesuai dengan kewajiban-kewajiban yang tertuang dalam hak asasi secara internasional untuk kebebasan berekspresi, kebebasan berkelompok, serta privasi, yang mana sejalan dengan nilai-nilai utama demokrasi.

Norma-norma lain dalam dokumen tersebut berfokus kepada tata kelola ruang siber secara umum serta kebijakan dan kerja sama internasional dengan berbagai aktor. Selain itu, terdapat dua norma yang berfokus kepada batasan target dari operasi siber. Meskipun relevan dalam diskusi yang lebih luas, kemampuan siber Indonesia saat ini belum mencapai level di mana melakukan operasi ofensif ke jaringan negara lain, sehingga kedua norma tersebut belum relevan dalam kasus Indonesia. Meskipun demikian, Kemhan dan TNI perlu memberikan perhatian lebih dalam proyeksi pengembangan kemampuan siber di Indonesia ke depannya. Norma pertama berfokus kepada tidak menarget infrastruktur kritis, sementara yang kedua menekankan untuk tidak menyerang tim tanggap darurat (CERTs) dari negara lain.

Selain norma di atas, hukum internasional juga menjadi kerangka penting dalam mengatur operasi siber antarnegara. Penerapan prinsip-prinsip hukum internasional yang sudah ada dipercaya dapat mengurangi risiko eskalasi dan meningkatkan stabilitas global, khususnya dengan memberi panduan kapan tindakan balasan terhadap serangan siber dapat dibenarkan secara hukum.[55] Dalam masa damai, prinsip seperti *state responsibility* dan *due diligence* menegaskan bahwa negara bertanggung jawab atas aktivitas siber yang berasal dari wilayahnya. Sementara itu, prinsip non-intervensi dan kedaulatan negara melarang negara melakukan operasi siber yang merusak atau mengganggu urusan internal negara lain, termasuk infrastruktur teknologi informasi yang vital.

Dalam konteks konflik bersenjata, Hukum Humaniter Internasional (HHI) atau dikenal juga Law of Armed Conflict juga berlaku di domain siber. Prinsip-prinsip seperti *distinction*, *proportionality*, *precaution*, dan *humanity* wajib diterapkan untuk mencegah kerugian terhadap warga sipil dan objek non-militer.[56] Pelanggaran terhadap prinsip-prinsip ini dapat dikategorikan sebagai kejahatan perang. Dengan demikian, hukum internasional menetapkan batas dan tanggung jawab jelas dalam penggunaan kekuatan di ruang siber. Meskipun demikian, penerapan hukum internasional dalam domain siber secara praktik cukup sulit karena sifat dasar konflik siber yang sangat tinggi anonimitas serta buramnya batasan antara sektor militer dan sipil.

## Operasi Siber di luar Koridor Demokrasi

Di sisi lain, negara-negara demokratis memiliki masalah penyalahgunaan kapasitas sibernya yang tidak sesuai dengan nilai-nilai demokrasi liberal meskipun dengan skala yang berbeda dibandingkan dengan negara non-demokrasi.

Contoh utamanya adalah penggunaan aplikasi khusus untuk memata-matai (dikenal dengan nama *spyware*) aktor domestik yang bahkan terjadi di berbagai negara di Eropa seperti Polandia, Hungaria, dan Yunani. Ketiganya dilaporkan menggunakan *spyware* terhadap jurnalis, aktivis, dan politisi oposisi dalam rentang 2019 hingga 2022.[57] Kasus serupa juga terjadi di Spanyol, di mana pemerintah mengakui penggunaan *spyware* Pegasus milik perusahaan Israel, NSO Group, untuk memantau pemimpin separatis Catalonia pada 2017–2020.[58] Praktik ini telah memicu diskursus serius di Uni Eropa mengenai kemungkinan pelarangan penuh *spyware* bagi negara-negara anggotanya.[59] Perusahaan seperti NSO Group bahkan mendirikan anak usaha di Siprus dan Bulgaria untuk menghindari kontrol ekspor yang lebih ketat di negara Eropa Barat.[60]

Negara demokratis berkembang di wilayah dunia lainnya pun menunjukkan pola serupa. Di Meksiko, laporan tahun 2017–2021 mengungkap penggunaan Pegasus terhadap jurnalis, pengacara, dan aktivis HAM yang menyelidiki kasus korupsi dan penyalahgunaan wewenang oleh negara.[61] Di Kenya, antara tahun 2017–2023, *spyware* FinFisher dan Pegasus digunakan untuk memantau organisasi masyarakat sipil, disertai kekerasan terhadap jurnalis selama protes besar-besaran di tahun 2023.[62] Permasalahan serupa juga terjadi di kawasan Asia Tenggara. Di Thailand, laporan pada 2022 mencatat penggunaan Pegasus terhadap sedikitnya 30 aktivis pro-demokrasi dan pemimpin mahasiswa.[63] Di Malaysia, penyelidikan pada 2023 mengungkap pembelian *spyware* asal Israel dari Quadream dan Candiru untuk memantau oposisi dan kelompok masyarakat sipil, yang kemudian mendapatkan kritik keras dari publik atas komitmen pemerintah terhadap prinsip-prinsip demokrasi.[64]

Di luar operasi siber menggunakan *spyware*, pemerintah demokratis juga sering memutus akses internet dan sensor digital dalam situasi dianggap krisis untuk menjaga stabilitas politik. Pada awal 2025, pemerintah India memberlakukan lima kali pemutusan akses internet regional selama protes nasional, menggunakan regulasi dari tahun 1885.[65] Selain itu, tindakan sensor dilakukan terhadap pengguna platform X (Twitter) dengan memblokir lebih dari 8.000 akun tanpa penjelasan spesifik terkait konten pelanggaran selama puncak konflik militer India dan Pakistan di tahun yang sama.[66] Hal ini bukanlah sesuatu yang unik dilakukan oleh India, karena pemutusan akses internet merupakan salah satu mekanisme utama negara-negara demokrasi berkembang dan autokrasi untuk menjaga kestabilan politik. Tahun 2024 dicatat sebagai tahun terburuk dalam jumlah pemutusan akses internet dalam setahun sejak pertama kali dihitung pada tahun 2016, di mana terjadi 296 kejadian di 52 negara.[67] Selain karena situasi konflik dan perang, kebijakan pemutusan akses tersebut juga dilakukan oleh berbagai negara ketika terjadi protes ataupun di masa pemilihan umum, di mana negara demokrasi mapan seperti Prancis serta demokrasi berkembang seperti Malaysia dan Thailand pertama kalinya masuk ke dalam daftar negara yang melakukan hal tersebut.

Berbagai contoh di atas menunjukkan bahwa adanya fenomena umum bagi negara-negara demokratis untuk menyalahgunakan kemampuan sibernya dan

menyasar aktor domestik dengan alasan politik. Ruang digital dipersepsikan menjadi sumber ancaman keamanan terhadap kedaulatan dan dalam prosesnya meminggirkan nilai-nilai utama demokrasi seperti privasi dan kebebasan berpendapat. Penurunan kualitas demokrasi secara global sangat dipengaruhi oleh peningkatan berbagai serangan digital terhadap aktor yang dianggap menjadi musuh rezim yang berkuasa; mulai dari penggunaan *spyware*, penyebaran informasi pribadi, serta pengerahan pasukan siber tidak generik; terutama di tengah minimnya mekanisme kontrol terhadap kapabilitas siber tersebut.[68]

## Refleksi terhadap Indonesia

Berdasarkan dua pendekatan tersebut, terdapat beberapa poin utama bagaimana hubungan antara nilai-nilai demokrasi dengan operasi dan perilaku Indonesia di ruang sibernya. Pertama, penghormatan terhadap hak asasi manusia belum menjadi perhatian utama. Salah satu yang menjadi sorotan adalah penggunaan *spyware* terhadap aktor domestik cukup masif terjadi dalam beberapa tahun terakhir. Sejauh ini, institusi utama yang dilaporkan menjadi pengguna *spyware* adalah POLRI, BIN dan BSSN. Belum ada laporan penggunaan *spyware* oleh institusi TNI, meskipun sempat ada pemberitaan Komando Pasukan Khusus (Kopassus)—satuan elite TNI untuk melakukan operasi-operasi khusus—menggunakan teknologi pengawasan terhadap pemimpin politik, tradisional, agama dan kelompok masyarakat sipil yang ada di Papua.[69] Di sisi lain, anggota TNI pernah menjadi target dari *spyware*. Di tahun 2022 dilaporkan adanya jejak *spyware* Pegasus pada dua pejabat senior TNI serta penasihat Kemhan, bersama dengan Menteri Koordinator bidang Perekonomian Airlangga Hartarto serta sejumlah pejabat Kementerian Luar Negeri. [70] Hingga saat ini tidak jelas motif dari penggunaan *spyware* tersebut, apakah ada kepentingan politik atau bagian dari spionase oleh aktor luar negeri.

**Tabel 4. Jejak Penggunaan *Spyware* oleh Indonesia**

| ***Spyware*** | **Periode Penggunaan** | **Perusahaan Perantara** | **Institusi Negara Pengguna** | **Target** |
|---|---|---|---|---|
| FinFisher (Jerman) | 2004, 2010, 2013, 2015, 2021 | - Gamma TSE Group<br>- Readarius M8 Sdn Bhd (Malaysia)<br>- PT. Digital Solusi Prima | Lemsanneg/ BSSN, BNPT | - Aktivitas dan Masyarakat di Papua<br>- Organisasi non-pemerintah, aktivis/ oposisi politik secara global |

| | | | | |
|---|---|---|---|---|
| Wintego Systems (Israel) | 2019 | - Ataka Enterprises PTE Ltd (Singapura<br>- ESW Systems (Singapura) | POLRI | Target tidak jelas, jejak *spyware* ditemukan dalam situs yang meniru tribunnews.com |
| Intellexa Consortium (Berbasis di beberapa negara Eropa) | 2021-2023 | Tidak ditemukan | Tidak jelas penggunanya di Indonesia | Kemungkinan menyasar aktivis Papua karena jejak *spyware* ditemukan dalam situs seperti ewestpapua.org dan nindonesia.news |
| Candiru/ Saito Tech (Israel) | 2020-2021 | HeHa PT Ltd (Singapura) | POLRI | Target tidak jelas, jejak *spyware* ditemukan dalam situs menyerupai media daring seperti Tirto, Tribunnews, Media Indonesia dan ANTARA |
| NSO Group - Circles, Q Cyber (Israel) | 2018-2022 | Radika (PT. Radika Karya Utama) | BIN, POLRI | - Menteri Airlangga Hartarto<br>- Penasihat Kemhan dan Kemlu<br>- Dua pejabat senior TNI<br>- Dua diplomat regional |

Sumber: Olahan tim penulis dari berbagai sumber

Selain penggunaan *spyware*, penghormatan terhadap nilai-nilai penting lainnya seperti kebebasan berekspresi serta hak atas akses digital juga kerap kali masih menjadi catatan minor dalam kebijakan ruang digital di Indonesia. Pemerintah Indonesia pernah melakukan pemutusan akses internet di provinsi Papua dan Papua Barat pada Agustus 2019 ketika terjadi protes besar-besaran yang berujung terjadinya kerusuhan. Keputusan pemerintah tersebut, atas dasar keamanan nasional dan menjaga ketertiban publik, mendapatkan kritik keras sebagai gangguan atas proses demokrasi serta meminggirkan hak untuk berekspresi dan mendapatkan informasi.[71] Pada akhirnya, pengadilan memutuskan bahwa tindakan tersebut melanggar hukum dan tidak sesuai dengan hukum hak asasi manusia internasional.[72] Hal tersebut tidak menghalangi pemerintah untuk tetap menjadikan pemutusan akses internet sebagai kebijakan yang dilirik untuk menghadapi situasi tertentu, seperti tertuang dalam upaya revisi UU POLRI sejak tahun 2004 yang berupaya memberikan mewenang POLRI untuk melakukan hal tersebut.[73] Regulasi dan kebijakan kontroversial dari pemerintah Indonesia untuk mengelola ruang siber bukanlah hal yang baru. Di tahun 2020, Menteri Komdigi (kala itu bernama Komunikasi dan Informatika atau Kominfo) mengeluarkan kebijakan yang mengatur bagaimana pemerintah bisa meminta

konten tertentu di media sosial diturunkan atas dasar mengganggu ketertiban publik, sebuah barometer yang tidak jelas dan berpotensi disalahgunakan oleh pemerintah.[74]

Contoh di atas memang tidak berhubungan langsung dengan operasi siber TNI. Namun demikian, TNI sendiri memiliki rekam jejak yang hampir serupa dalam menghadapi kritikan dari masyarakat. Kepala Pusat Penerangan (Kapuspen) TNI, misalnya, meyakini bahwa ada aktor intelektual yang mendesain gelombang demonstrasi penolak terhadap revisi UU TNI.[75] Sebelumnya, Presiden Prabowo juga mempertanyakan apakah aksi demonstrasi tersebut merupakan massa bayaran atau tidak, serta menuding adanya lembaga swadaya masyarakat (LSM) yang menerima dana dari luar negeri untuk mengadu domba masyarakat Indonesia dengan isu HAM.[76] Sentimen ini sejalan dengan persepsi ancaman terhadap keutuhan bangsa dan bagaimana operasi siber TNI menarget pihak-pihak yang memiliki motif melemahkan kepercayaan publik terhadap institusi pertahanan yang telah dibahas di bagian awal. Sehingga meskipun Kemhan menegaskan bahwa operasi siber TNI tidak akan dilakukan untuk memata-matai sipil, muncul pertanyaan lebih jauh bagaimana memastikan hal tersebut betul-betul tidak terjadi jika berkaca kepada perspektif dan sentimen di atas.

## Pengembangan Peperangan Siber di TNI

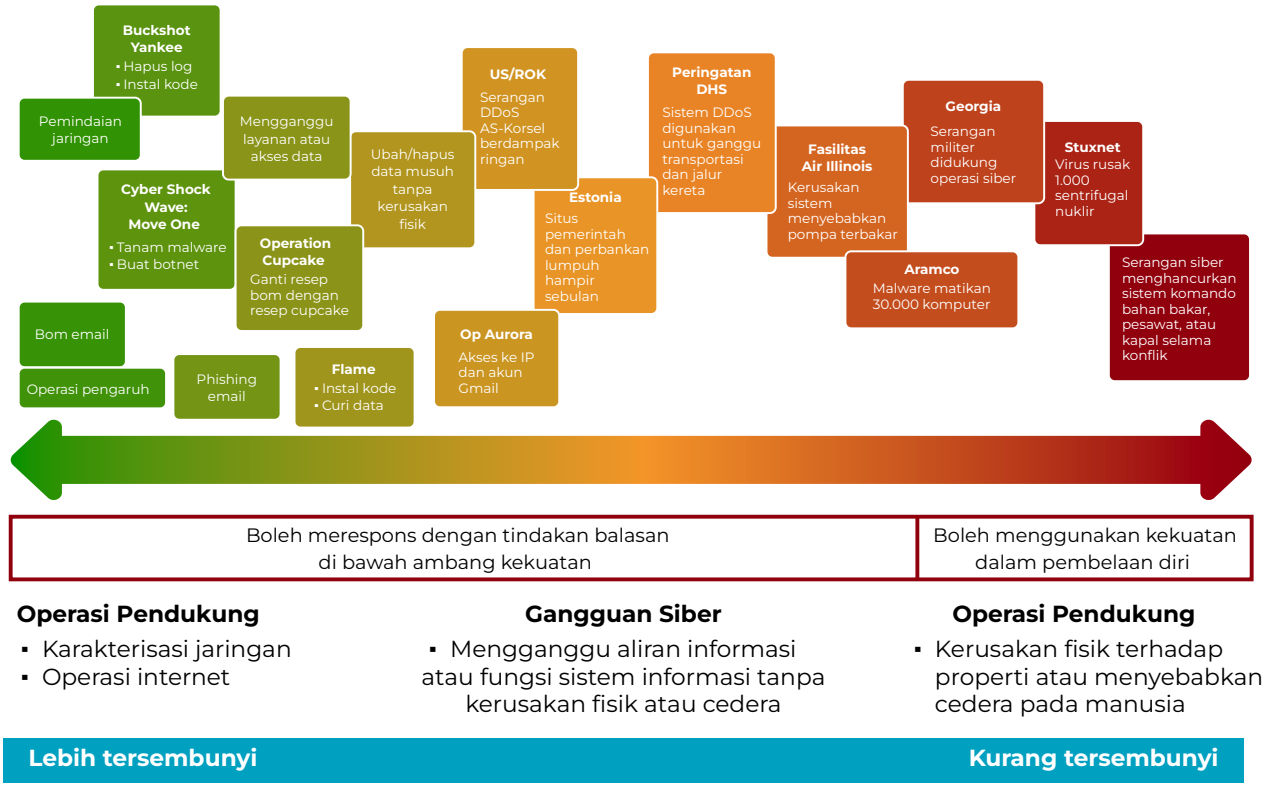
Berdasarkan evaluasi di atas, terdapat beberapa hal yang harus dipertimbangkan oleh pemerintah Indonesia dan TNI dalam mengembangkan kapasitas operasi sibernya dalam koridor demokrasi. Ada empat bagian utama dalam proses tersebut, yaitu doktrin dan strategi; kelembagaan organisasi siber militer; personil atau talenta siber; dan hubungan sipil-militer. Pengembangan keempat bagian tersebut pada praktiknya akan sangat terhubung satu sama lain, sehingga seharusnya diperlukan sebagai sesuatu yang harus dikembangkan secara paralel dan tidak terfokus pada satu bagian saja.

Pertama, doktrin pertahanan siber merupakan fondasi utama dalam membangun kekuatan militer modern yang mengadaptasi teknologi serta peperangan siber dalam organisasinya. Dalam konteks negara demokratis, penyusunan doktrin siber tidak hanya bertujuan mengoptimalkan kekuatan tempur di domain digital, tetapi juga menjadi instrumen penting untuk memastikan akuntabilitas dan transparansi terhadap operasi siber militer. Dokumen tersebut bisa ditujukan untuk menjawab hal-hal mendasar dalam menyiapkan doktrin siber, seperti bagaimana mendefinisikan ruang siber, apakah domain tersebut setara dengan domain militer lainnya, serta bagaimana suatu negara akan membedakan antara aktivitas militer, intelijen, dan pertahanan sipil.[77]

Dokumen-dokumen pertahanan siber di Indonesia seperti Pedoman Pertahanan Siber (2014) dan Pedoman Strategis Pertahanan Non-Militer (2016) dikeluarkan hampir satu dekade lalu sehingga banyak kebaharuan dalam ruang siber yang belum masuk dan tidak cukup menjawab tantangan pertahanan siber yang dihadapi TNI saat ini. Dalam konteks demokrasi, definisi ancaman siber dalam

regulasi Indonesia, terutama dalam kerangka ancaman hibrida, mendorong proses militerisasi ruang siber. Definisi ancaman hibrida yang dipakai oleh pemerintah saat ini perlu ditinjau ulang dan tidak secara otomatis menempatkan TNI sebagai kekuatan utama dalam responsnya. Spektrum ancaman ruang siber yang luas semestinya bisa dibahas dalam aturan yang lebih besar dan dengan jelas menempatkan institusi-institusi sipil untuk isu yang tidak langsung berhubungan dengan pertahanan.[78] Misalnya, untuk menghadapi informasi operasi negara lain, Komdigi serta POLRI menjadi entitas utama, di mana TNI tidak berusaha menjadi penegak hukum untuk isu tersebut. Hal tersebut bisa diperkuat dengan aturan level UU, seperti UU Keamanan Siber bahkan Keamanan Nasional untuk menjadi landasan regulasi yang jelas mengenai hubungan antar-lembaga dalam mengelola ruang siber di Indonesia.

**Gambar 7. Ilustrasi Spektrum Ancaman Siber[79]**




Dengan menggunakan gradasi jenis ancaman siber di atas, pemerintah bisa mengeluarkan dokumen turunan dari revisi UU TNI mengenai OMSP Siber yang menjelaskan bahwa pengerahan TNI hanya untuk ambang batas tertentu yang sudah dianggap penting dan kritis. Hal ini juga sejalan dengan implementasi Doktrin Sishanrata, di mana institusi sipil pun juga dilibatkan dalam menghadapi ancaman. Maka dari itu, pemerintah juga bisa menjelaskan definisi ancaman hibrida, jenis-jenis ancamannya dan tidak semata-mata mendorong TNI untuk menjadi komponen utama dalam menghadapinya.

Di tingkat organisasi, reformasi kelembagaan juga perlu dilakukan oleh TNI. Tidak ada barometer pasti mengenai bentuk organisasi siber macam apa yang merupakan jawaban untuk kebutuhan peperangan siber sebuah unit militer,

di mana hal tersebut sangat bergantung kepada tujuan strategis dari negara masing-masing.[80] Diskusi terkait perlu tidaknya TNI membentuk matra siber cenderung telah mereda terutama dengan tidak adanya dukungan politik dari pemerintahan Presiden Prabowo untuk hal tersebut.[81] Meskipun demikian, bentuk organisasi Satsiber TNI saat ini tetap memerlukan peningkatan, apalagi jika ke depannya TNI akan mencoba mengintegrasikan kemampuan operasi ofensif. Mabes TNI perlu membayangkan sebuah komando gabungan untuk melakukan operasi siber, dengan status Komando Utama (Kotama) Operasi, di mana saat ini Satsiber TNI masih berstatus Badan Pelaksana Pusat (Balakpus).

Di sisi lain, terdapat kekhawatiran mengenai pengembangan organisasi Satsiber saat ini. Sebelumnya, terdapat empat satuan di dalam organisasi, yaitu Penangkalan, Pemulihan, Bantuan dan Penindakan, selain keberadaan asisten operasi dan administrasi logistik. Keempat satuan tersebut menunjukkan pendekatan yang konvensional dalam tubuh Satsiber yang mencerminkan *business process* normal dalam operasi siber, selayaknya BSSN ketika pertama kali dibentuk di tahun 2017. Berdasarkan arahan Panglima TNI, Satsiber kini mengalami reorganisasi di mana keempat satuan di atas berganti nama menjadi Pusat Kecerdasan Buatan, Infrastruktur Digital, Perlindungan Data, serta Pengendalian Konten. Perubahan tersebut mencerminkan persepsi ancaman oleh TNI di ruang siber. Satuan Infrastruktur Digital dan Perlindungan Data cenderung memiliki fungsi normal dalam operasi siber defensif, sementara Pusat Kecerdasan Buatan menunjukkan upaya TNI untuk melalukan adaptasi terhadap teknologi termutakhir dalam operasinya.

Dalam konteks koridor demokrasi, keberadaan Satuan Pengendalian Konten menghadirkan pertanyaan peran TNI di dalam ruang digital. Unit tersebut lahir dari kebutuhan Satsiber untuk merespons ancaman berupa narasi di media sosial dan berita daring, mulai dari melakukan upaya pemblokiran akun dan konten hingga melakukan kontra opini.[82] Permasalahannya, upaya TNI untuk mendapatkan otoritas tersebut akan bertabrakan dengan institusi pemerintah lainnya, seperti wewenang penurunan konten yang adalah tugas Kementerian Komdigi berdasarkan UU Informasi dan Transaksi Elektronik (ITE). Operasi kontra narasi juga menghadirkan kekhawatiran akan bayang-bayang dwifungsi, sebagaimana yang ditakutkan publik dalam proses revisi UU TNI.

TNI semestinya berfokus kepada penguatan Satsiber untuk integrasi peperangan siber ke dalam tubuh TNI, bukan berfokus kepada konten di media sosial. Nantinya, pengembangan tersebut juga perlu mempertimbangkan hubungan antara organisasi siber di Mabes TNI dengan masing-masing angkatan. Diskusi di berbagai negara terkait pembentukan matra siber biasanya merujuk kepada personil yang mengisi komando siber di level tertinggi, di mana ada kebutuhan untuk memiliki prajurit yang secara reguler harus kembali ke matra masing-masing.[83] Menaikkan level unit siber hingga ke level Kotama Operasi, yang kemungkinan dipimpin oleh perwira tinggi bintang tiga, juga akan menghadirkan insentif tangga promosi yang jelas bagi perwira-perwira yang memiliki kekhususan di bidang siber.

Hal ini berhubungan dengan bagian ketiga, yaitu personel. Salah satu dimensi penting lainnya dalam membangun kekuatan siber militer adalah kualitas personel. Skema penerimaan dari sipil yang kini tengah dicanangkan oleh Panglima TNI bisa menjadi jawaban untuk masalah kekurangan personil, namun dalam jangka panjang hal tersebut tidak cukup untuk membangun kapasitas siber TNI yang betul-betul mumpuni. Tantangan utama saat ini adalah minimnya skema karier, kurangnya insentif struktural, serta belum adanya kurikulum pelatihan terpadu yang mengintegrasikan pengetahuan teknis dan etika operasional. Lebih dari itu, ke depannya pengembangan personil di tubuh TNI tidak hanya terfokus kepada prajurit dengan kemampuan teknis dan mampu melakukan pengembangan sistem serta eksploitasi guna menunjang operasi. Lebih dari itu, diperlukan juga analis intelijen, ahli hukum, dan pengambil kebijakan dengan pemahaman strategis.[84] Ahli hukum, secara khusus, menjadi bagian penting untuk menjaga bagaimana operasi siber TNI berada dalam koridor demokrasi dan patuh dengan berbagai norma-norma internasional. Kurikulum latihan siber terpadu juga perlu diperhatikan oleh Mabes TNI untuk memastikan prajurit-prajurit yang kemudian ditempatkan di Satsiber memiliki standar dan persepsi yang sama, di mana nantinya juga akan menunjang dalam pelaksanaan operasi gabungan.

TNI juga perlu mendorong lahirnya pemimpin-pemimpin visioner yang mendukung pengembangan kapasitas siber dan integrasinya terhadap cara berperang TNI, sebuah katalisator utama dalam kematangan siber sebuah organisasi militer.[85] Hal ini bisa dimulai dengan memastikan perwira-perwira tinggi yang memiliki kemampuan siber serta pengalaman di bidang tersebut, baik di dalam tubuh TNI maupun di institusi sipil, mengalami proses mutasi serta promosi yang konsisten ke jabatan yang bersinggungan dengan ruang siber. Ketika dimutasi untuk memimpi pasukan, perwira-perwira tersebut bisa dipertimbangkan untuk memegang posisi yang mengedepankan *jointness* lintas matra, di mana ruang siber memiliki peranan penting, seperti di Komando Gabungan Wilayah Pertahanan (Kogabwilhan). Begitu juga untuk mengisi posisi unsur pembantu pimpinan di mabes maupun lembaga pendidikan, penempatan perwira berlatar siber akan mendorong integrasi peperangan siber yang lebih baik lagi di dalam tubuh TNI. Dengan begitu, diharapkan semakin banyak perwira yang sejak dini menekuni dan mendalami siber karena ada kejelasan jenjang karier untuk prajurit dengan kemampuan tersebut, yang mana sejatinya adalah cita-cita awal rencana pembentukan angkatan siber.[86]

Terakhir, hubungan sipil-militer menjadi bagian yang tidak terpisahkan, bukan hanya karena pengaruh faktor demokrasi tetapi juga dalam rangka mengumpulkan kapasitas siber yang tersebar di berbagai institusi. Hubungan kuat antara kapasitas siber di badan intelijen maupun di militer sangat kuat mewarnai dinamika tata kelola siber di berbagai negara, bahkan dianggap menjadi salah satu faktor utama proses transformasi integrasi ranah siber dalam pertempuran modern.[87] Organisasi intelijen, dengan tugas utama mengumpulkan informasi strategis, cenderung enggan untuk mengeksploitasi kerentanan dalam jaringan musuh secara terburu-buru. Preferensi mereka adalah untuk menjaga posisi

mereka di dalam sistem lawan. Di sisi lain, kebutuhan melakukan operasi ofensif membuat satuan siber di militer akan lebih agresif dalam memanfaatkan kerentanan tersebut. Hubungan ini menghadirkan dinamika tersendiri dalam pengembangan kapasitas operasi siber sebuah negara yang harus dicermati oleh Indonesia.[88] Contoh integrasi yang efektif adalah bagaimana US Cyber Command (militer) dan NSA (intelijen) dipimpin oleh pejabat yang sama guna menjalankan strategi *Persistent Engagement* AS.[89] Konteks ini masih belum relevan dalam konteks Indonesia yang tidak memiliki ancaman luar negeri yang nyata ataupun kapabilitas operasi ofensif. Namun, pembentukan Dewan Pertahanan Nasional di akhir tahun 2024 seharusnya bisa mendorong dinamika yang lebih baik di Indonesia untuk kerja sama antara sipil dan militer dalam pengembangan serta gelar kapasitas siber Indonesia ke depannya.

Di sisi lain, hubungan sipil-militer juga merujuk kepada akuntabilitas operasi siber yang dilakukan oleh militer. Revisi UU TNI 2025 yang membuat OMSP, termasuk OMSP Siber, tidak lagi memerlukan proses politik di DPR membuat ke depannya operasi siber di Indonesia cenderung lebih susah untuk diketahui secara publik. Dalam koridor demokrasi dan konteks sejarah penggunaan kekuatan pertahanan dalam politik Indonesia, hal ini sangat membuka pintu penyalahgunaan kemampuan operasi siber TNI.[90] DPR, dalam hal ini Komisi I, tetap harus bisa mengawal pengembangan dan penggunaan kemampuan operasi siber TNI tidak melenceng dari tugas-tugas pokok TNI, terutama dalam menghadapi ancaman luar negeri. Untuk membangun akuntabilitas, TNI bahkan bisa mengajukan diadakan tinjauan berkala oleh DPR terhadap operasi sibernya, mengadopsi pendekatan serupa di AS terhadap regulasi di bidang pertahanan dan intelijen. Hal ini juga berhubungan dengan bagian pertama terkait kejelasan persepsi ancaman siber yang seharusnya bisa didefinisikan baik di level Panglima Tertinggi maupun di Kemhan, melalui regulasi dan kebijakan yang relevan. Perlu dihindarkan menjadikan ancaman siber, dalam hal ini operasi informasi, dijadikan sebagai alasan untuk melindungi rezim politik tanpa kejelasan faktor intervensi dari aktor-aktor luar negeri.

Pemerintah dan TNI bisa membangun akuntabilitas terhadap operasi siber TNI dengan menyusun ulang doktrin dan strategi peperangan siber TNI yang lebih jelas mendefinisikan batasan wewenang TNI, merujuk kembali ke bagian pertama. Untuk membangun kepercayaan publik, pemerintah bisa mempertimbangkan membuat dokumen versi yang bisa dipublikasikan ke masyarakat luas. Perlu disadari bahwa praktik ini belum lazim dilakukan oleh negara-negara demokrasi berkembang lainnya. Sejauh ini, hal tersebut seakan-akan menjadi privilese negara-negara dengan kapasitas siber yang sudah mapan, seperti AS, Inggris serta pakta pertahanan macam NATO, yang secara terbuka mendokumentasikan operasi siber ofensifnya. Singapura, yang telah memiliki matra siber sendiri dan dekat dengan AS secara politik, juga tidak melakukan praktik serupa. Bahkan Australia, Kanada, serta Selandia Baru, yang merupakan negara anggota aliansi intelijen Five Eyes seperti AS dan Inggris, juga tidak memiliki dokumen sejenis. Dalam hal ini, ketiadaan dokumen serupa di Indonesia bisa dipahami. Namun,

konteks sejarah penggunaan militer di Indonesia untuk kepentingan politik rezim serta interpretasi ancaman pertahanan siber yang acapkali bersinggungan dengan aktor-aktor domestik membuat ketiadaan dokumen strategis serupa menghadirkan tanda tanya di publik terkait penggunaan kapasitas operasi siber TNI. Fokus kepada konten dan narasi di media sosial oleh Satsiber TNI semakin menghadirkan keraguan terkait komitmen Indonesia dalam membangun kapasitas siber dalam koridor demokrasi.

**Tabel 5. Saran Pengembangan Peperangan Siber di TNI**

| Doktrin dan Strategi | Kelembagaan Organisasi Siber | Personil dan Talenta Siber | Hubungan Sipil Militer |
|---|---|---|---|
| 1. Dokumen strategis baru mengenai gradasi ancaman siber dan batasan pelibatan TNI<br>2. Definisi ulang ancaman hibrida<br>3. Mendorong UU Keamanan Siber dan Keamanan Nasional | 1. Meningkatkan Satsiber menjadi Kotama Ops, hingga nantinya Komando Gabungan<br>2. Mengkaji ulang fokus pengendalian konten dalam pengembangan Konten | 1. Tangga karier yang jelas bagi perwira siber<br>2. Mendukung lahirnya perwira-perwira tinggi berlatar siber dengan pola mutasi dan promosi<br>3. Standarisasi kurikulum latihan terpadu<br>4. Rekrutmen talenta siber non teknis, seperti ahli hukum | 1. Penguatan koordinasi operasi siber dengan institusi sipil<br>2. Mekanisme akuntabilitas dan pengawasan oleh DPR<br>3. Mempublikasikan dokumen strategi dan doktrin untuk diakses publik |

# Kesimpulan

Integrasi kemampuan siber dalam tubuh TNI merupakan keniscayaan di era peperangan modern. Namun, tanpa batasan hukum yang jelas dan mekanisme pengawasan yang kuat, perluasan peran ini berisiko membuka ruang penyalahgunaan kekuasaan di tengah menurunnya kualitas demokrasi di Indonesia. Tantangan utama yang dihadapi Indonesia adalah keterbatasan personil, perkembangan organisasi siber di tubuh TNI yang tertatih-tatih, serta kaburnya batasan operasi siber TNI akibat definisi ancaman yang terlalu luas. Upaya integrasi peperangan siber kemudian justru didominasi oleh persepsi ancaman operasi informasi serta bagaimana ruang siber digunakan oleh aktor luar untuk mengganggu kesatuan bangsa.

Ke depan, penguatan operasi siber TNI harus dirancang dengan visi yang menyeimbangkan kesiapan teknis dan profesionalisme militer dengan prinsip supremasi sipil, transparansi, serta perlindungan hak asasi manusia. Partisipasi masyarakat sipil dan kontrol legislatif menjadi kunci untuk memastikan ruang siber tidak menjadi wajah baru dwifungsi militer. Penguatan kapasitas serta

kematangan siber TNI harus seiring dengan komitmen penguatan demokrasi sehingga dapat dipastikan operasi siber TNI sejatinya hanya dikerahkan untuk menghadapi ancaman eksternal dan bukan untuk menghadapi warga negara Indonesia.

## Catatan Akhir


1. "Koalisi Masyarakat Sipil Keluarkan Petisi Tolak RUU TNI," Detik.com, diakses pada 4 April 2025, https://news.detik.com/berita/d-7827638/koalisi-masyarakat-sipil-keluarkan-petisi-tolak-ruu-tni.
2. "Kontroversi Pelibatan Tentara Hadapi Ancaman Siber dalam UU TNI," Tempo, diakses pada 11 Juni 2025, https://www.tempo.co/politik/kontroversi-pelibatan-tentara-hadapi-ancaman-siber-dalam-uu-tni-1224841.
3. "Satu Dekade Tren Indeks Demokrasi Indonesia Menurun," Kompas.id, diakses pada 12 Juni 2025, https://www.kompas.id/artikel/satu-dekade-tren-indeks-demokrasi-indonesia-menurun.
4. Azifah Astrina, "Indonesia's Quite Militarization Under President Prabowo Subianto." The Diplomat. 2 April 2025. https://thediplomat.com/2025/04/indonesias-quiet-militarization-under-president-prabowo-subianto/.
5. Dizar Ramadhan Sabana dan Pratama Putra Prasetya, "Revisi UU TNI: Pekerjaan Rumah Sektor Pertahanan Tetap Belum Selesai," Laboratorium Indonesia 2045 (LAB 45), 18 Maret 2024, https://www.lab45.id/detail/299/revisi-uu-tni-pekerjaan-rumah-sektor-pertahanan-tetap-belum-selesai.
6. Max Smeets, No Shortcuts: Why States Struggle to Develop a Military Cyber-Force (Oxford: Oxford University Press, 2022), 27.
7. Carlos Solar, "Cybersecurity and Cyber Defence in the Emerging Democracies," Journal of Cyber Policy 5, no. 3 (2020): 392–412, https://doi.org/10.1080/23738871.2020.1820546; Bill Marzcak et al. 'Running in Circles: Uncovering the Clients of Cyberespionage firm Circles,' Citizen Lab, 1 Desember 2020, https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.
8. The International Institute for Strategic Studies, Cyber Capabilities and National Power: A Net Assessment (London: The International Institute for Strategic Studies, 2021).
9. "Di balik retorika 'waspadai kekuatan asing' ala Presiden Prabowo Subianto – 'Prabowo adu domba warga dengan warga'," BBC Indonesia, 5 Juni 2025, https://www.bbc.com/indonesia/articles/cgq3k5gxy21o.
10. "Hadi Tjahjanto Sebut Angkatan Siber Penting: Perang Sudah Masuk Ke Ranah Siber," Tempo, 4 September 2024, https://www.tempo.co/politik/hadi-tjahjanto-sebut-angkatan-siber-penting-perang-sudah-masuk-ke-ranah-siber-12747.
11. "Kemhan Tegaskan Tugas Siber TNI untuk Pertahanan," Kompas, 27 Maret 2025, https://www.kompas.id/artikel/kemhan-tegaskan-tugas-siber-tni-untuk-pertahanan.
12. Jun Honna, Military Politics and Democratization in Indonesia (Abingdon, Oxfordshire: Routledge, 2003).
13. "Webinar IPCRA-IKA Unhan-KBRI Beograd, "Perang Balkan: Konflik Bersenjata di Negara Pecahan Yugoslavia", Indonesia Defense Magazine, 10 September 2020, https://indonesiadefense.com/webinar-ipcra-ika-unhan-kbri-beograd-perang-balkan-konflik-bersenjata-di-negara-pecahan-yugoslavia/.
14. "Apa Saja Aspek Trgatra dan Pancagatra dalam Wawasan Nusantara?", Tirto.id, 26 Juli 2023, https://tirto.id/apa-saja-aspek-trigatra-dan-pancagatra-dalam-wawasan-nusantara-gaZQ.
15. Gatra Priyandita dan Christian Guntur Lebang, "Indonesia's cyber soldier: armed without compass", The Strategist – ASPI Blog, 11 April 2025, https://www.aspistrategist.org.au/indonesias-cyber-soldiers-armed-without-a-compass/.
16. Daniel Moore, Offensive Cyber Operations: Understanding Intangible Warfare (Oxford:

Oxford University Press, 2022), 4-5.
17. Lennart Maschmeyer; The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. International Security 2021; 46 (2): 51–90. doi: https://doi.org/10.1162/isec_a_00418
18. Jason Blessing dan Greg Austin, "Assessing military cyber maturity: strategy, institutions and capability", IISS, 3 Februari 2022, https://www.iiss.org/research-paper/2022/02/assessing-military-cyber-maturity/.
19. "Bamsoet tekankan pentingnya pembentukan Angkatan Siber", Antara, 9 November 2023, https://www.antaranews.com/berita/3815934/bamsoet-tekankan-pentingnya-pembentukan-angkatan-siber.
20. "Panglima TNI akui sudah diperintah Presiden bentuk Angkatan Siber," Antara, 3 September 2024, https://www.antaranews.com/berita/4305343/panglima-tni-akui-sudah-diperintah-presiden-bentuk-angkatan-siber.
21. "Menhan jelaskan bahwa TNI memiliki Satuan Siber, bukan matra siber," Antara, 5 Februari 2025, https://www.antaranews.com/berita/4626969/menhan-jelaskan-bahwa-tni-memiliki-satuan-siber-bukan-matra-siber.
22. "KSAU resmikan skuadron pendidikan khusus untuk pelajari siber", Antara, 11 Oktober 2024,https://www.antaranews.com/berita/4390478/ksau-resmikan-skuadron-pendidikan-khusus-untuk-pelajari-siber.
23. Presiden Republik Indonesia. Peraturan Presiden Republik Indonesia Nomor 84 Tahun 2025 tentang Perubahan atas Peraturan Presiden Nomor 66 Tahun 2019 tentang Susunan Organisasi Tentara Nasional Indonesia, 2025
24. "Kembalinya Dwifungsi TNI dan Corak Militeristik Pemerintahan Prabowo-Gibran", Siaran Pers Koalisi Masyarakat Sipil untuk Reformasi Sektor Keamanan, 20 Februari 2025,https://imparsial.org/kembalinya-dwifungsi-tni-dan-corak-militeristik-pemerintahan-prabowo-gibran/.
25. Wawancara tertutup dengan petinggi Kemhan di Jakarta, 26 Agustus 2024.
26. "Chapter Five: Asia," The Military Balance 125, no. 1 (2025): 206–311, https://doi.org/10.1080/04597222.2025.2445477.
27. Evan Laksmana, "What Indonesia's retail approach to defense modernization means," International Institute of Strategic Studies (IISS) Military Balance Online Blog, 18 September 2023, https://www.iiss.org/online-analysis/military-balance/2023/09/what-indonesias-retail-approach-to-defence-modernisation-means/.
28. Blessing dan Austin, 22.
29. Christian Guntur Lebang dan Reine Prihandoko, "Modernisasi TNI di Bawah Jokowi: Profesional dan Politis" (presentasi pada Seminar Nasional Evaluasi Kebijakan Pemerintahan Joko Widodo Bidang Politik Keamanan, Ekonomi, dan Media, 8 Oktober 2024), diakses 9 Agustus 2025, https://img.lab45.id/files/event_file/43/8373Slide-Presentasi-Sesi-1.pdf.
30. "TNI seeks to turn cyber experts into soldiers", The Jakarta Post, 2 Februari 2025, https://www.thejakartapost.com/indonesia/2025/02/02/tni-seeks-to-turn-cyber-experts-into-soldiers.html.
31. Blessing dan Austin, 11.
32. The International Institute for Strategic Studies, Cyber Capabilities and National Power: A Net Assessment (London: IISS, 2021), 143-148.
33. Kementerian Sekretariat Negara, "Pemerintah Tertibkan Undang-undang Nomor 5 Tahun 2018 Tentang Pemberantasan Tindak Pidana Korupsi", Pemerintah Republik Indonesia, 27 Juni 2018, https://setneg.go.id/baca/index/pemerintah_terbitkan_undang_undang_nomor_5_tahun_2018_tentang_pemberantasan_tindak_pidana_

terorisme.
34. "Mengenal Koopsus TNI, Satuan Gabungan Pasukan Elite Atasi Terorisme", Kompas.com, 5 Oktober 2021, https://nasional.kompas.com/read/2021/10/05/08462331/mengenal-koopssus-tni-satuan-gabungan-pasukan-elite-atasi-terorisme.
35. "Indonesia, U.S. host joint drills with first cybersecurity agenda", Nikkei Asia, 26 Agustus 2024, https://asia.nikkei.com/politics/defense/indonesia-u.s.-host-joint-drills-with-first-cybersecurity-agenda.
36. British Embassy Jakarta (@ukinindonesia), "Strengthening cyber defence, together. For the first time, Indonesia joined the UK-led…", Instagram, 9 Juni 2025, https://www.instagram.com/reel/DKrWIBJT4SY/.
37. "Philippine, U.S. Troops Kick off Exercise Balikatan 2025", US Department of Defense, 7 April 2025, https://www.dvidshub.net/news/494797/philippine-us-troops-kick-off-exercise-balikatan-2025.
38. Laporan Tahunan sejak tahun 2018 bisa diakses melalui: https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html.
39. Gatra Priyandita dan Louise Marie Hurel, Responsible Cyber Behaviour in the Indo-Pacific: Views from Cambodia, Fiji, India, Indonesia, Japan, Pakistan and Taiwan (Canberra: Australian Strategic Policy Institute dan RUSI, Januari 2025), 51.
40. 40 "Philippines steps up defences against Chinese hackers after 'cyberwar' warning from telecoms security chief", South China Morning Post, 10 April 2024, https://www.scmp.com/week-asia/politics/article/3258419/philippines-steps-defences-against-chinese-hackers-after-cyberwar-warning-telecoms-security-chief.
41. "Microsoft Digital Defense Report 2024", Microsoft, Oktober 2024,12-13, https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024#modal-dialog.
42. Microsoft, 21.
43. Letkol Chb Ir. Bagus Artiadi Soewardi, M.Si., "Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia", Media Informasi Ditjen Pothan Kemhan, Maret 2013, https://www.kemhan.go.id/pothan/wp-content/uploads/migrasi/admin/Cyber%20Defence.pdf.
44. Jacob Judah, "How East Timor Blazed the Way for Hacktivism," New Lines Magazine, 27 Desember 2024, https://newlinesmag.com/essays/how-east-timor-blazed-the-way-for-hacktivism/.
45. Mykyta Taratorin, "Unraveling Russia's propaganda web: a closer look at Russian disinformation mechanisms in Indonesia", WeAreUkraine.info, 6 Mei 2024, https://www.weareukraine.info/special/unraveling-russias-propaganda-web-a-closer-look-at-russian-disinformation-mechanisms-in-indonesia/.
46. Nikolas K. Gvosdev, "Is Russia Sabotaging Democracy in the West?" Orbis 63, no. 3 (2019): 321–333, https://doi.org/10.1016/j.orbis.2019.05.010.
47. "Indonesia Muslim groups deny China lobbying sways views on Uighurs", Reuters, 17 Desember 2019, https://www.reuters.com/article/world/indonesia-muslim-groups-deny-china-lobbying-sways-views-on-uighurs-idUSKBN1YL1GB/.
48. Maya Wang dan Andreas Harsono, "Indonesia's Silence over Xinjiang", Human Rights Watch, 31 Januari 2020, https://www.hrw.org/news/2020/01/31/indonesias-silence-over-xinjiang.
49. Sidney Jones, "Why Indonesians Distrust the U.S.", International Crisis Group, 13 November 2003, https://www.crisisgroup.org/asia/south-east-asia/indonesia/why-indonesians-distrust-us.
50. UN GGE. Report of the Group of Governmental Experts on Developments in the Field

of Information and Telecommunications in the Context of International Security. New York: UNGA, 2015.
51. Marcus Willett, "Responsible Cyber Power." Adelphi Series 64 (511–513): 191–230. 2024. doi:10.1080/19445571.2024.2417545.
52. Bart Hogeveen, The UN Norms of Responsible State Behaviour in Cyberspace: Guidance on Implementation for Member States of ASEAN (Canberra: Australian Strategic Policy Institute, Maret 2022).
53. Priyandita dan Hurel, 7.
54. Hogeveen, 46.
55. Marcus Willett, "Responsible Cyber Power." Adelphi Series 64 (511–513): 191–230. 2024. doi:10.1080/19445571.2024.2417545.
56. Ibid, hlm. 196
57. How EU countries spy on their citizens', VSquare.org, 28 Agustus 2023, https://vsquare.org/pegasus-spyware-poland-hungary-slovakia-romania/.
58. Antoaneta Roussi, 'How Europe became the Wild West of spyware', Politico, , 25 Oktober 2023, https://www.politico.eu/article/how-europe-became-wild-west-spyware/.
59. 'Spyware and state abuse: The case for an EU-wide ban', European Digital Rights (EDRi), posisi kertas, 16 Juni 2025, https://edri.org/wp-content/uploads/2025/06/EDRi_Spyware-position-paper.pdf.
60. Steven Feldstein dan Brian Kot, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses." Carnegie Endowment for International Peace. 14 Maret 2023. https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en.
61. "Mexican president denies spying on journalists, lawyers and activists", BBC, 23 Juni 2017, https://www.bbc.com/news/world-latin-america-40376891.
62. Feldstein dan Kot, 2023.
63. 'Pegasus Spyware: A Grave Threat to Journalists in Southeast Asia', Al Jazeera Media Institute, 5 Februari 2024, https://institute.aljazeera.net/en/ajr/article/2525.
64. 'Malaysia Uses Israeli Spyware to Monitor Citizens', Malaysia Today, 8 November 2023, https://www.malaysia-today.net/2023/11/08/malaysia-uses-israeli-spyware-to-monitor-citizens/.
65. "India leads the 10 countries restricting internet access in 2025", Tech Radar, 3 Juli 2025, https://www.techradar.com/vpn/vpn-privacy-security/india-leads-the-10-countries-restricting-internet-access-in-2025.
66. "Lack of Cyber Attribution a Major Challenge for India: Lt Gen Pant," CSO Online, 2 September 2020, https://www.csoonline.com/article/569797/lack-of-cyber-attribution-a-major-challenge-for-india-lt-gen-pant.html.
67. "Emboldened Offenders, Endangered Communities: Internet shutdowns in 2024", Access Now, Februari 2025, https://www.accessnow.org/wp-content/uploads/2025/02/KeepItOn-2024-Internet-Shutdowns-Annual-Report.pdf.
68. "Freedom on The Net 2024: The Struggle for Trust Online", Freedom House, diakses 30 Agustus 2025, https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online.
69. "Indonesia: Military Documents Reveal Unlawful Spying in Papua", Human Rights Watch, 14 Agustus 2011, https://www.hrw.org/news/2011/08/14/indonesia-military-documents-reveal-unlawful-spying-papua.
70. M. Khory Alfarizi, "Ramai Spyware Pegasus Masuk Indonesia, Menko Airlangga Pernah Jadi Target?" Tempo.co, 20 Juni 2023. diakses pada 2 Juli 2025. https://www.tempo.co/

ekonomi/ramai-spyware-pegasus-masuk-indonesia-menko-airlangga-pernah-jadi-target--175145.
71. Ika Karlina Idris, "The internet shutdown in Papua threatens Indonesia's democracy and its people's right to free speech", The Conversation, 23 Agustus 2019, https://theconversation.com/the-internet-shutdown-in-papua-threatens-indonesias-democracy-and-its-peoples-right-to-free-speech-122333.
72. "Court Ruling on Internet Blackout Is A Rare Victory For Freedom of Expression in Papua", Amnesty International, 3 Juni 2020, https://www.amnesty.id/kabar-terbaru/siaran-pers/court-ruling-on-internet-blackout-is-a-rare-victory-for-freedom-of-expression-in-papua/06/2020/#:~:text=%E2%80%9CIn%20light%20of%20this%20ruling%2C%20the%20President,in%20a%20context%20of%20discrimination%20and%20militarization.
73. Afra Hanifah Prasastiwi, "Superbody Digital: Ambisi RUU Polri dalam Dunia Siber", Center for Digital Society, 29 April 2025, https://digitalsociety.id/2025/04/29/superbody-digital-ambisi-ruu-polri-dalam-dunia-siber/19704/.
74. Christian Guntur Lebang dan Gatra Priyandita, "Indonesia's controversial tech licensing scheme", The Strategist – ASPI Blog, 9 Agustus 2022, https://www.aspistrategist.org.au/indonesias-controversial-tech-licensing-scheme/.
75. "Militer cari sosok di balik petisi tolak RUU TNI, tuduh gerakan sipil dibayar", BBC, 27 Juni 2025, https://www.bbc.com/indonesia/articles/cj617kep8n5o.
76. "Prabowo Tanggapi Maraknya Unjuk Rasa: Itu Murni atau Ada yang Bayar?", Tempo, 8 April 2025, https://www.tempo.co/politik/prabowo-tanggapi-maraknya-unjuk-rasa-itu-murni-atau-ada-yang-bayar--1228552; "Prabowo Tuding LSM Dibiayai Asing untuk Mengadu Domba", Tempo, 2 Juni 2025, https://www.tempo.co/politik/prabowo-tuding-lsm-dibiayai-asing-untuk-mengadu-domba-1622885.
77. David Ormrod dan Benjamin Turnbull, "The Cyber Conceptual Framework for Developing Military Doctrine," Defence Studies 16, no. 3 (2016): 270–298, https://doi.org/10.1080/14702436.2016.1187568.
78. Christian Guntur Lebang, "Perubahan Ancaman dan Sesat Pikir Revisi UU TNI", Media Indonesia, 9 April 2025, https://mediaindonesia.com/opini/758450/perubahan-ancaman-dan-sesat-pikir-revisi-uu-tni.
79. Gary Brown dan Owen Tullos, "On the Spectrum of Cyberspace Operations," 11 Desember 2012, tersedia di SSRN, https://ssrn.com/abstract=2400536 atau http://dx.doi.org/10.2139/ssrn.2400536.
80. Blessing dan Austin, 9, 2022, hal xx.
81. "Menhan Sebut TNI Tidak Perlu Bentuk Angkatan Siber", CNN Indonesia, 5 Agustus 2025, https://www.cnnindonesia.com/nasional/20250805172038-20-1259062/menhan-sebut-tni-tidak-perlu-bentuk-angkatan-siber.
82. SAFENet (@safenetvoice), "Kalo nih RUU TNI beneran lolos kali ini, serius dah...", X, 18 Maret 2025, https://x.com/safenetvoice/status/1902208413175615772.
83. Erica Lonergan, Todd Arnold, dan Nick Strack, "The Case for a Prospective U.S. Cyber Force", War on The Rocks, 22 Mei 2024, https://warontherocks.com/2024/05/the-case-for-a-prospective-u-s-cyber-force/.
84. Max Smeets, 91, No Shortcuts: Why States Struggle to Develop a Military Cyber-Force (London: C. Hurst & Co. Publishers Ltd, 2022).
85. Blessing dan Austin, 5.
86. Christian Guntur Lebang, "Navigating the cyber future: Does Indonesia need a cyber military force?", 6 Januari 2024, https://www.thejakartapost.com/opinion/2024/01/06/navigating-the-cyber-future-does-indonesia-need-a-cyber-military-force.html.

87. The International Institute for Strategic Studies, Cyber Capabilities and National Power: A Net Assessment (London: IISS, 2021), 8.
88. Smeets, 107.
89. Saat ini tengah muncul diskusi untuk memecah sistem 'Dual Hat' kepemimpinan US Cyber Command dan NSA, selaras dengan diskursus pembentukan Angkatan Siber di AS. Lebih jauh bisa lihat: "Unfinished business for Trump: Ending the Cyber Command and NSA 'dual hat'", The Record, 12 Desember 2024, https://therecord.media/cyber-command-nsa-dual-hat-trump; Jason Blessing, "Trump 2.0 and the fracture of US cyber power", Defense News, 30 Januari 2025, https://www.defensenews.com/opinion/2025/01/29/trump-20-and-the-fracture-of-us-cyber-power/.
90. "Indonesia: Rejection Amendments to Law on the Indonesian National Armed Forces", SAFENet, 17 Maret 2025, https://safenet.or.id/2025/03/indonesia-rejection-amendments-to-law-on-the-indonesian-national-armed-forces/.

# Ucapan Apresiasi

Tim penulis berterima kasih kepada Ali Abdullah Wibisono dan Andi Widjajanto yang telah memberikan masukan yang sangat berharga dalam penyempurnaan Cakrawala Strategis ini. Masukan kedua mitra bestari mampu menajamkan analisis dari kajian ini serta membantu tim penulis menemukan bagian-bagian tertentu yang harus diperjelas. Selain itu, apresiasi sebesar-besarnya diberikan kepada setidaknya sepuluh pejabat senior, perwira tinggi, dan perwira menengah di lingkungan TNI dan Kemhan yang berkontribusi dalam memberikan pandangan, informasi, dan komentar secara anonim dalam proses penulisan yang memastikan kajian ini tetap memperhatikan konteks Indonesia serta membumi terhadap kondisi riil di tubuh TNI.