SIBER, INFORMASI, DAN KEPEMIMPINAN ERA DIGITAL: TRANSFORMASI SUMBER DAYA TEKNOLOGI DALAM DOKTRIN PERTAHANAN INDONESIA

Evi Bayu Priatno[1], Hendra Saputra[2], Tarsisius Susilo[3], Nurhidayat[4], Tuwadi[5]
Sekolah Staf dan Komando Tentara Nasional Indonesia
[1]evibayuprihatnobisnis@gmail.com,[2]hendra.080681@gmail.com,[3]muchus70@gmail.com,

Abstrak - Perkembangan era digital telah menciptakan domain baru dalam peperangan: ruang siber dan informasi. Negara-negara besar seperti Rusia, Amerika Serikat, dan Israel menunjukkan bagaimana kepemimpinan visioner dalam bidang siber mampu mentransformasikan teknologi menjadi kekuatan pertahanan strategis. Rusia mengintegrasikan serangan siber dan disinformasi sebagai instrumen geopolitik, AS membangun doktrin *Defend Forward* serta kemitraan publik–swasta yang luas, sementara Israel melalui Unit 8200 menjadikan siber sebagai komponen utama setiap operasi militer. Indonesia, dengan meningkatnya ancaman siber seperti kebocoran data dan serangan disinformasi, menghadapi urgensi untuk membangun doktrin pertahanan siber nasional yang khas. Artikel ini menganalisis model kepemimpinan global, menilai gap Indonesia, serta menawarkan kerangka doktrin pertahanan siber berbasis Pancasila dan nilai kejuangan TNI. Temuan penelitian menunjukkan bahwa tanpa reformulasi strategi, Indonesia berisiko menjadi target empuk dalam perang siber global. Namun, dengan kepemimpinan transformasional dan kebijakan proaktif, Indonesia dapat mentransformasikan sumber daya teknologi menjadi benteng pertahanan digital yang tangguh, sejalan dengan visi Indonesia Emas 2045.
Kata kunci: pertahanan siber, kepemimpinan digital, disinformasi, TNI, Pancasila, doktrin pertahanan

Abstract *- The digital era has introduced a new domain of warfare: cyberspace and information. Major powers such as Russia, the United States, and Israel demonstrate how visionary leadership in cyberspace can transform technology into strategic defense capabilities. Russia integrates cyberattacks and disinformation as geopolitical tools, the U.S. has established the Defend Forward doctrine alongside broad public–private partnerships, while Israel, through Unit 8200, embeds cyber operations into every military campaign. Indonesia, facing rising threats such as massive data breaches and disinformation campaigns, urgently needs a distinctive national cyber defense doctrine. This article analyzes global leadership models, assesses Indonesia's existing gaps, and proposes a cyber defense framework grounded in Pancasila and TNI's values of struggle. Findings suggest that without doctrinal reform, Indonesia risks becoming a soft target in global cyber warfare. However, through transformational leadership and proactive policies, Indonesia can transform technological resources into a resilient digital defense shield, aligned with the vision of Indonesia Emas 2045.*
Keywords*: cyber defense, digital leadership, disinformation, Indonesian Armed Forces, Pancasila, defense doctrine*

Pendahuluan

Era digital telah mengubah lanskap pertahanan global secara fundamental. Ruang siber dan informasi kini diakui sebagai domain baru peperangan, sejajar dengan domain tradisional (darat, laut, udara, ruang angkasa). Ancaman terhadap kedaulatan tak lagi bersifat fisik semata, melainkan muncul melalui serangan siber, disinformasi, dan manipulasi informasi. Kondisi ini menuntut kepemimpinan pertahanan yang adaptif dan melek teknologi untuk memanfaatkan sumber daya teknologi mutakhir (seperti siber, kecerdasan buatan/AI, dan big data) sekaligus melindungi bangsa dari ancaman digital.

Para pemimpin pertahanan perlu mentransformasi doktrin dan strategi mereka agar relevan di era perang informasi, di mana *bit* dan *byte* bisa sama mematikannya dengan peluru dan bom.

Permasalahan utamanya adalah *bagaimana Indonesia dapat belajar dari kepemimpinan negara maju* (seperti Rusia, Amerika Serikat, dan Israel) dalam mengelola sumber daya digital dan siber sebagai bagian kekuatan pertahanan, serta *mengapa Indonesia mendesak membutuhkan doktrin pertahanan siber nasional* yang berlandaskan nilai dan kepentingan keamanan nasional. Negara-negara besar telah mengintegrasikan kekuatan siber ke dalam strategi militer mereka – contohnya Rusia dengan *hybrid warfare*, AS dengan strategi *"Defend Forward"*, dan Israel dengan unit siber elit. Indonesia perlu menjadikan pendekatan-pendekatan tersebut sebagai teladan, disesuaikan dengan konteks lokal. Saat ini Indonesia rentan terhadap serangan siber, namun belum memiliki *doktrin pertahanan siber terpadu*. Tanpa kerangka doktrin yang jelas, upaya penanggulangan ancaman siber cenderung bersifat ad-hoc dan reaktif, sehingga *tidak menjamin keamanan jangka panjang*. Pertanyaan yang muncul: Bagaimana merumuskan doktrin siber yang "Indonesiawi" – efektif menghadapi ancaman digital tetapi tetap selaras dengan nilai Pancasila dan kepentingan nasional?

Indonesia belakangan mengalami serentetan *serangan siber*: mulai dari peretasan data penduduk (contoh: kasus *Bjorka* yang membocorkan data pejabat 2022), *defacement* situs KPU pada Pemilu 2019 dengan hoaks "server luar negeri", hingga kebocoran 1,3 juta data e-HAC Kemenkes (2021). Insiden-insiden ini menegaskan kerentanan infrastruktur digital kita. Namun, Indonesia *belum memiliki doktrin pertahanan siber nasional* yang memandu respons dan strategi secara menyeluruh. Tanpa doktrin, ruang siber ibarat lahan tak bertuan – berbagai lembaga bergerak sendiri-sendiri tanpa koordinasi strategis. Penyusunan doktrin siber nasional tidak bisa ditunda lagi: ini penting untuk memberikan *kepastian arah* (strategic guidance) bagi TNI, pemerintah, dan aktor terkait dalam menghadapi ancaman siber. Memahami bagaimana para *key players* global membangun kapabilitas dan kebijakan sibernya akan membantu Indonesia merumuskan doktrin yang tepat. Doktrin tersebut harus *khas Indonesia*: memadukan *best practices* internasional dengan nilai lokal, demi melindungi kedaulatan digital dan keamanan nasional kita.

Tinjauan Pustaka

a. Domain Siber dan Informasi sebagai Medan Perang: Literatur pertahanan pasca-2010 menegaskan bahwa *cyber is the fifth domain* – domain kelima peperangan setelah darat, laut, udara, dan antariksa. Artinya, ruang siber diakui secara resmi sebagai arena konflik geopolitik. Konsep *perang informasi* (information warfare) pun mengemuka: mencakup propaganda di media sosial, operasi psikologis, *hack-and-leak* dokumen rahasia, hingga sabotase sistem digital musuh. Sebuah laporan German Marshall Fund (2020) menunjukkan betapa ampuhnya perang informasi modern: intervensi Rusia dalam Pemilu AS 2016 dilaksanakan melalui kampanye disinformasi terorganisir yang berhasil memecah belah masyarakat dan melemahkan demokrasi. Dengan memanfaatkan media sosial, intelijen Rusia menciptakan polarisasi ekstrem di publik AS – *bottom line*-nya: disinformasi masif mampu merusak tatanan politik internal lawan. Kesimpulan ini diperkuat investigasi Mueller dan komite Senat AS yang menyatakan pemerintah Rusia menggelar kampanye terencana untuk melemahkan Amerika dengan berbagai taktik. Jelas bahwa informasi kini menjadi senjata strategis.

b. Kepemimpinan Rusia dalam Perang Siber dan Informasi: Rusia sering disebut *pelopor perang hibrida (hybrid warfare)* – menggabungkan serangan siber, kampanye disinformasi, dan operasi militer konvensional. Contohnya, invasi Rusia ke Georgia (2008) dan Ukraina (2014)

diiringi serangan siber terkoordinasi. Kasus terkenal adalah *serangan siber ke Estonia tahun 2007*: gelombang *Distributed Denial of Service (DDoS)* melumpuhkan situs pemerintah, bank, dan media di Estonia sebagai respon kemarahan Rusia. Serangan 2007 di Estonia ini sering disebut contoh pertama *cyber war* skala nasional. Saat aneksasi Krimea 2014, kelompok *APT Sandworm* Rusia dituduh melumpuhkan jaringan listrik Ukraina pada 2015 (*Ukraine power grid hack*) – menciptakan pemadaman listrik melalui malware BlackEnergy. Serangan ini menunjukkan kemampuan Rusia menjadikan infrastruktur sipil sebagai target siber. Selain itu, menjelang invasi Ukraina 2022, Rusia kembali melancarkan serangan siber (peretasan situs pemerintah Ukraina, penyebaran malware wiper, dan lain-lain.) sebagai bagian pembuka serangan militernya.

Di ranah informasi, Rusia piawai mengeksploitasi media sosial untuk propaganda. Unit seperti Internet Research Agency (IRA) menjalankan operasi disinformasi yang menyasar berbagai kelompok di negara target. Contoh nyata: pada Pilpres AS 2016, operasi disinformasi Rusia menargetkan baik kelompok *konservatif* maupun *liberal* – mulai dari pendukung Ted Cruz, aktivis Black Lives Matter, hingga gerakan separatis Texas dan California – semua ditujukan untuk memperdalam perpecahan internal AS. Tujuan Rusia adalah memecah-belah masyarakat lawan dan mendestabilisasi demokrasinya. Taktik ini sejalan dengan doktrin *"Information Confrontation"* Rusia, di mana perang informasi dianggap bagian integral dari konflik. Presiden Vladimir Putin sendiri memberi prioritas tinggi pada kapabilitas ini: Rusia mulai membentuk pasukan *"information troops"* sejak awal 2010-an. Pada 2017, Menhan Sergei Shoigu mengumumkan militer Rusia telah membentuk unit perang informasi yang *"lebih efektif dari sebelumnya"*, dengan tugas melakukan propaganda pintar dan melindungi kepentingan pertahanan di ranah informasi. Dengan kata lain, Rusia mengintegrasikan operasi intelijen (FSB, GRU) dengan aktor non-negara (hacker patriotik, "troll factory") dalam strategi perang informasi menyeluruh. Ini tampak dalam aksi peretasan (*hack*) data lawan oleh intelijen resmi, yang kemudian *dibocorkan* melalui situs proxy seperti DCLeaks/Guccifer 2.0 atau WikiLeaks untuk efek politis. Kombinasi operasi rahasia dan operasi terbuka semacam ini diakui komunitas intelijen Barat sebagai ciri khas kampanye Rusia.

c. Kepemimpinan AS di Domain Digital: Amerika Serikat merespons perkembangan ancaman siber dengan langkah-langkah strategis sejak awal dekade 2010-an. Tonggak pentingnya adalah pendirian *U.S. Cyber Command (USCYBERCOM)* pada tahun 2010, menandai evolusi doktrin militer AS yang memasukkan operasi siber sebagai elemen kunci pertahanan. USCYBERCOM berfungsi sebagai komando terpadu yang memimpin operasi dunia maya ofensif maupun defensif. Langkah ini kemudian diikuti negara lain (Inggris mendirikan National Cyber Force, dan lain-lain.). Dalam perkembangan doktrin, Departemen Pertahanan AS menerbitkan Strategi Siber 2018 yang memperkenalkan konsep *"Defend Forward"*. Prinsip *Defend Forward* berarti *"bertahan dengan cara menyerang lebih dulu"*, yakni menggagalkan aktivitas siber musuh di sumbernya sebelum sempat menyerang AS. Pendekatan ini proaktif dan agresif: jika suatu *server*, *network*, atau pelaku teridentifikasi merencanakan serangan ke kepentingan AS, maka AS akan melakukan operasi siber ofensif untuk mengacaukannya terlebih dahulu. Implementasinya terlihat menjelang Pemilu 2020, ketika US Cyber Command dan mitra-mitranya melumpuhkan infrastruktur *botnet* TrickBot milik peretas kriminal (diduga berafiliasi dengan Rusia) demi mencegah potensi serangan *ransomware* yang mengganggu pemilu. Operasi preemptif tersebut merupakan bagian dari strategi "persistent engagement" AS – di

mana USCYBERCOM terus menerus *memburu dan mengganggu* aktor siber musuh setiap hari untuk impose costs (memberi biaya/harga mahal) bagi mereka. Selain pendekatan militer, kepemimpinan AS juga menekankan kolaborasi lintas sektor (whole-of-nation) untuk keamanan siber. Pemerintah melibatkan FBI, Departemen Keamanan Dalam Negeri (DHS/CISA), NSA, serta raksasa teknologi (Microsoft, Google, Facebook) dalam melindungi pemilu dari intervensi asing dan memerangi kampanye disinformasi. Sebagai contoh, Microsoft bekerja sama dengan Cyber Command dalam operasi *takedown* botnet, dan platform media sosial meningkatkan koordinasi dengan pemerintah untuk deteksi pengaruh asing. AS juga pionir integrasi Big Data dan AI dalam intelijen pertahanan – misalnya *Project Maven* yang menggunakan AI untuk menganalisis rekaman drone militer, meski menuai kontroversi di kalangan civil society. Upaya ini menunjukkan visi AS: memadukan kemampuan teknologi sipil dengan militer demi mempertahankan keunggulan siber nasional.

d. Kepemimpinan Israel di Teknologi Pertahanan: Israel secara luas diakui sebagai *cyber powerhouse* dunia. Kunci utamanya adalah Unit 8200 – unit intelijen sinyal (SIGINT) Israel yang juga menjadi tulang punggung kapabilitas siber ofensif dan defensif mereka. Unit 8200 bisa disetarakan dengan NSA-nya AS; ini adalah unit terbesar di militer Israel, dibentuk sejak 1948 dan berevolusi dengan kemajuan teknologi. Aktivitas Unit 8200 sangat rahasia dan meliputi penyadapan elektronik, *data mining*, hingga operasi serangan siber ofensif. Beberapa operasi terkenal yang dikaitkan dengan Unit 8200 antara lain: virus Stuxnet (2005-2010) – serangan siber canggih hasil kolaborasi Israel-AS yang berhasil *melumpuhkan ribuan centrifuge nuklir Iran* tanpa perlu menjatuhkan bom. Ini contoh konkret senjata siber yang mencapai tujuan strategis (menghambat program nuklir musuh) dengan presisi tinggi. Contoh lain, media asing melaporkan Unit 8200 terlibat peretasan jaringan telekom Lebanon (Ogero) tahun 2017, dan membantu menggagalkan rencana serangan ISIS terhadap penerbangan sipil Australia tahun 2018. Dalam doktrin militer Israel, operasi siber terintegrasi erat ke setiap operasi militer. Unit 8200 beroperasi di semua medan, termasuk mendukung pasukan tempur garis depan dengan intelijen siber real-time. Pada masa perang, unit ini terkoneksi langsung dengan markas komando tempur untuk memberikan dukungan intelijen dan perang elektronik. Hal ini mencerminkan filosofi Israel bahwa supremasi informasi adalah kunci kemenangan modern. Budaya kepemimpinan di unit siber Israel juga unik: mereka memberi ruang besar bagi talenta muda dan inovasi ala startup. Personel 8200 direkrut dari pemuda berusia akhir belasan atau awal 20-an melalui seleksi ketat (banyak dari program sains unggulan SMA). Setelah berdinas, alumni 8200 banyak yang mendirikan *startup* siber, membuat ekosistem siber Israel sangat maju. Mantan anggota unit ini menyebut budaya kerjanya mirip perusahaan rintisan – tim-tim kecil diberi kebebasan kreatif besar untuk memecahkan masalah, mendorong lahirnya solusi out-of-the-box. Pelajaran dari Israel: kombinasi *teknologi* + *talenta* + *doktrin jelas* dapat menjadikan negara kecil sekalipun pemain siber kelas dunia.

e. Status Indonesia saat ini : Bagaimana dengan Indonesia? Kita baru berada di tahap awal membangun kemampuan pertahanan siber. Secara struktural, sejak 2017 didirikan Badan Siber dan Sandi Negara (BSSN) sebagai lembaga utama keamanan siber nasional, fokus pada sektor sipil. Di militer, TNI membentuk Satuan Siber TNI (Satsiber) per Oktober 2017 sebagai badan pelaksana pusat operasi siber pertahanan. Muncul pula wacana membentuk *Cyber Command* tersendiri di tubuh TNI, namun hingga kini statusnya masih setingkat *satuan* di bawah Mabes TNI (dipimpin perwira bintang satu). Indonesia belum memiliki doktrin pertahanan siber

nasional yang dipublikasikan. Acuan yang ada, misalnya Peraturan Menhan No. 82/2014 tentang Pedoman Pertahanan Siber, lebih bersifat teknis dan belum berkembang menjadi doktrin terpadu lintas matra. Beberapa kajian menilai regulasi ini sudah usang dan perlu pembaruan sesuai dinamika ancaman saat ini. Dari segi kesiapan sumber daya manusia (SDM), penelitian dari Kominfo dan lembaga independen menunjukkan kesenjangan kapasitas siber Indonesia. Indeks Keamanan Siber Global (ITU) sempat menempatkan Indonesia tertinggal dalam hal kemampuan teknis (misalnya pembentukan CERT sektor-sektor). BSSN sudah berdiri – memenuhi pilar *organisasional* – tetapi itu saja tidak cukup. Dibutuhkan SDM yang cakap, koordinasi antarlembaga yang harmonis, regulasi yang jelas, dan perangkat teknologi andal untuk membangun kerangka keamanan siber efektif. Sayangnya, *SDM siber nasional masih minim*, dan koordinasi TNI-sipil kurang erat. Hal ini tampak dalam penanganan insiden siber domestik yang seringkali tumpang tindih: misalnya saat kebocoran data besar terjadi, ada kebingungan apakah BSSN, Kominfo, atau Bareskrim yang memimpin respon. Intinya, Indonesia belum memiliki strategi siber komprehensif – hal ini diakui para analis, terlihat dari *belum adanya doktrin pertahanan siber nasional yang jelas menggambarkan sikap dan strategi digital Indonesia*. Sementara itu, negara-negara besar telah memiliki *cyber military doctrine* tersendiri. Ketiadaan doktrin ini membuat upaya Indonesia cenderung defensif reaktif, belum proaktif. Inilah *gap* yang harus segera ditutup.

Metodologi

Penelitian ini menggunakan metode studi perbandingan strategis dan analisis kebijakan. Pendekatan *benchmarking* diterapkan dengan membandingkan kepemimpinan digital di Rusia, AS, dan Israel sebagai studi kasus global. Data sekunder dikumpulkan dari laporan, strategi, dan literatur otoritatif (laporan think-tank, kebijakan pemerintah, berita media internasional). Sumber data mencakup: kasus serangan siber internasional (misal: peretasan jaringan listrik Ukraina 2015 oleh Rusia, serangan *ransomware* WannaCry 2017, operasi Stuxnet 2010), dokumen strategi siber negara maju (Summary *DoD Cyber Strategy* AS 2018, *National Cyber Force* Inggris, *Cybersecurity Strategy* Singapura 2019, dan lain-lain.), serta insiden siber domestik Indonesia (kasus defacement KPU 2019, kebocoran data e-KTP dan Kominfo 2022, dan sebagainya.).

Analisis dilakukan dalam beberapa tahap: pertama, membandingkan pendekatan Rusia, AS, dan Israel dalam memimpin domain siber – mengidentifikasi kesamaan dan perbedaan (misal: *investasi masif di kapabilitas siber* jadi kesamaan, namun *gaya operasi berbeda* – Rusia cenderung ofensif/agresif dengan disinformasi, AS menekankan kolaborasi publik-swasta, Israel fokus pada intelijen dan *preemptive strikes*). Kedua, menilai posisi Indonesia saat ini: *gap* apa yang ada di aspek doktrin, struktur organisasi, regulasi, dan SDM dibanding negara-negara tersebut. Ketiga, merumuskan rekomendasi kerangka doktrin siber nasional yang sesuai konteks Indonesia, dengan mengacu temuan perbandingan dan kondisi lokal.

Pendekatan kualitatif diterapkan, bersandar pada analisis isi (content analysis) sumber-sumber. Reliabilitas data dijaga dengan mengambil dari sumber kredibel (misal: Reuters untuk info Israel, situs *cybercom.mil* untuk strategi AS, publikasi GMF untuk operasi Rusia, serta paper akademik/kebijakan untuk konteks Indonesia). Hasil analisis diharapkan berbentuk narasi komprehensif mengenai perlunya transformasi sumber daya teknologi dalam doktrin pertahanan Indonesia.

Analisis dan Pembahasan

a. Studi Kasus Global – Kepemimpinan dalam Perang Siber

Rusia – Perpaduan Siber dan Disinformasi: Seperti telah diuraikan, Rusia mempelopori penggunaan kombinasi *cyber attack* dan *information warfare* sebagai instrumen geopolitik. Contoh nyata: Serangan Siber ke Estonia 2007. Setelah pemerintah Estonia memindahkan patung prajurit perunggu Soviet, jaringan internet Estonia dihantam gelombang serangan DDoS yang melumpuhkan layanan perbankan dan situs pemerintah selama berminggu-minggu. Ini dianggap *serangan siber pertama* yang menjatuhkan infrastruktur suatu negara, meski Rusia tak pernah mengakuinya. Lalu, Perang Georgia 2008 juga disertai peretasan situs pemerintah Georgia dan penyebaran propaganda yang mendukung narasi Kremlin. Dunia tercengang melihat Rusia mampu melakukan *cyber-operation* mendukung operasi militer konvensionalnya.

Masuk dekade 2010-an, Ukraina menjadi ajang demonstrasi senjata siber Rusia. Setelah revolusi pro-Barat di Kyiv, Rusia mencaplok Krimea (2014) dan mendukung pemberontakan di Donbas. Pada Desember 2015, di tengah konflik terselubung itu, terjadilah *serangan siber terhadap jaringan listrik Ukraina*: hacker (dikaitkan dengan unit Sandworm, bagian GRU) menyusup ke sistem SCADA operator listrik dan mematikan aliran listrik di beberapa wilayah. Ratusan ribu orang mengalami pemadaman selama jam-jam sibuk musim dingin. Serangan berlanjut dengan varian malware (*Industroyer*) di 2016 dan serangan *NotPetya* 2017 yang menyebar luas (berdampak global). Pelajaran dari kasus Ukraina: Rusia menjadikan infrastruktur sipil kritis sebagai target siber untuk mengganggu stabilitas negara sasaran. Meski efek strategisnya terbatas (lampu padam sementara, tidak menghentikan pemerintah Ukraina), ini menunjukkan kemampuan Rusia untuk melakukan *sabotase jarak jauh*. Namun, perang siber Rusia di Ukraina juga menemukan batasnya: analisis CSIS mencatat serangan siber Rusia kurang terkoordinasi dengan serangan militer konvensional, sehingga dampaknya tidak menentukan hasil perang.

Di domain peperangan informasi, Rusia menjalankan kampanye disinformasi agresif. Sebelum invasi militer, Rusia kerap melancarkan *kampanye propaganda dan operasi psikologis* di negara target. Contoh penting: Interferensi Rusia pada Pemilu AS 2016. Operasi ini terdiri dari dua komponen utama: peretasan (*hack*) dan pembocoran email petinggi Partai Demokrat (oleh unit intelijen GRU) serta operasi disinformasi masif di media sosial (oleh IRA dan proxy lainnya). Intelijen AS mengkonfirmasi Putin sendiri memerintahkan kampanye untuk mempengaruhi pemilu AS, dengan *strategi gabungan operasi intelijen rahasia dan upaya terbuka oleh pemerintah serta proksinya untuk mempolarisasi publik AS dan merusak integritas proses pemilu*. Di media sosial, *ribuan akun palsu dan bot* dikerahkan untuk menyebar isu kontroversial, mengipas emosi kelompok konservatif maupun progresif secara simultan. GMF mencatat target operasi disinformasi Rusia mencakup tokoh sayap kanan *hingga* aktivis sayap kiri – tujuannya memperparah perpecahan yang sudah ada. Rusia sengaja mempermainkan kedua sisi spektrum politik agar masyarakat AS semakin terbelah dan saling curiga, sehingga lembaga demokrasinya melemah. Kampanye ini begitu luas dan canggih hingga disebut sebagai "operasi perang informasi paling serius terhadap AS" sejak Perang Dingin. Meskipun sulit mengukur dampak pastinya terhadap hasil pemilu, efek jangka panjangnya nyata: tingkat kepercayaan publik terhadap sistem pemilu menurun, dan polarisasi politik meningkat tajam setelah 2016.

Rusia juga menggunakan aktor non-negara sebagai kepanjangan tangan. Mereka memanfaatkan *deniability*: misalnya membiarkan kelompok hacker kriminal atau "hacktivist patriotik" melakukan serangan yang menguntungkan kepentingan Rusia, sehingga pemerintah bisa lepas tangan. Tetapi terkadang hubungan itu tampak jelas – contohnya *IRA* (Internet Research Agency) yang berbasis di St. Petersburg, meski berstatus "perusahaan", didanai pemerintah Rusia untuk operasi propaganda online (terbukti dari dakwaan DOJ AS 2018 yang mengungkap anggaran IRA meningkat 70% pasca-2016). Kepemimpinan Putin sangat aktif dalam hal ini: pada 2012 Kementerian Pertahanan Rusia mulai membahas pembentukan pasukan siber/informasi, dan di 2017 diumumkan resmi bahwa unit *Information Operations Troops* telah dibentuk. Shoigu menyatakan tugas pasukan ini mencakup *"propaganda yang cerdas, kompeten, efektif"* serta perlindungan kepentingan nasional di ruang informasi. Dapat disimpulkan, Rusia mencontohkan model kepemimpinan siber yang ofensif dan terintegrasi: menggabungkan kemampuan siber untuk sabotase infrastruktur lawan, operasi peretasan intelijen, hingga kampanye disinformasi skala besar sebagai *satu paket* strategi perang modern.

Amerika Serikat – Membangun Postur Ofensif-Defensif dan Kolaboratif: Berbeda dengan Rusia yang secara *de facto* berperang siber sejak 2007, Amerika Serikat awalnya lebih bersikap defensif karena menjadi target utama berbagai serangan (oleh Rusia, Tiongkok, Iran, Korea Utara, dan sebagainya.). Namun, seiring meningkatnya intensitas ancaman, kepemimpinan AS beradaptasi cepat. Setelah pembentukan US Cyber Command (2010) yang membawa operasi siber masuk ke struktur komando militer, AS mulai merumuskan doktrin yang lebih agresif. Strategi Siber DoD 2018 menjadi tonggak karena mengubah paradigma dari reaktif menjadi proaktif. Konsep "Defend Forward" di dalamnya memperbolehkan militer AS mengeksekusi serangan siber pendahuluan terhadap jaringan atau peretas lawan yang dianggap ancaman, meskipun mereka belum menyerang secara fisik. Hal ini mencerminkan filosofi bahwa menunggu diserang terlebih dahulu di dunia maya terlalu berisiko; lebih baik menyerang hacker di "sarangnya" sebelum mereka beraksi. Implementasi kebijakan ini terlihat nyata menjelang Pemilu 2018 dan 2020: Jenderal Paul Nakasone (Komandan USCYBERCOM) mengonfirmasi bahwa Cyber Command melakukan operasi ofensif terhadap peretas dan infrastruktur siber asing untuk mengamankan pemilu AS. Contohnya, pada 2018 USCYBERCOM melumpuhkan akses internet *"troll farm"* Rusia (IRA) pada hari pemilu paruh waktu, guna mencegah mereka menyebar disinformasi. Lalu, di 2020, gabungan Cyber Command, NSA, FBI dan mitra sipil menggelar operasi kontra-ransomware dengan merusak botnet TrickBot menjelang Pilpres, mengantisipasi kemungkinan serangan ke infrastruktur pemilu. Operasi-operasi ini bersifat *preemptive* dan menunjukkan AS tak segan menggunakan kapabilitas ofensif demi melindungi proses demokratisnya.

Yang menarik, kepemimpinan AS sangat menekankan kolaborasi lintas lembaga dan sektor – disebut *"whole-of-nation approach"*. Ancaman siber dianggap terlalu luas untuk ditangani militer sendirian. Oleh karena itu, dibentuklah kerangka kerja sama dimana USCYBERCOM berkoordinasi erat dengan lembaga domestik (DHS/CISA untuk infrastruktur kritis, FBI untuk penegakan hukum siber, komunitas intelijen untuk atribusi ancaman), serta menggandeng perusahaan teknologi swasta. Misalnya, Microsoft, Google, Facebook dilibatkan dalam *sharing intelijen ancaman* dan penindakan cepat (seperti menghapus akun-akun disinformasi atau memperbaiki kerentanan sistem) sebagai bagian pertahanan nasional. Hal ini terlihat dalam kasus TrickBot: Microsoft melalui pengadilan AS mengambil alih server botnet

tersebut, sementara Cyber Command melakukan exploit terhadap perangkat komando botnet – kombinasi tindakan hukum-sipil dan operasi militer. Kemitraan publik-swasta ini dipandang krusial mengingat ~85% infrastruktur digital AS dimiliki entitas non-pemerintah. Budaya Amerika yang terbuka juga mendorong transparansi: pejabat siber (seperti Dir. CISA Chris Krebs) secara rutin mengedukasi publik tentang hoaks dan keamanan digital. Upaya *literasi digital* dijalankan agar masyarakat tahan terhadap disinformasi (contoh: program "*Warp Speed*" jelang pemilu 2020 untuk melawan hoaks vaksin/Pemilu bersama perusahaan media sosial).

Dari sisi teknologi, AS memanfaatkan keunggulan inovasi domestik. Proyek-proyek seperti Project Maven (AI untuk analisis rekaman drone) dan inisiatif Big Data dalam intelijen membuktikan militer AS aktif mengadopsi teknologi Silicon Valley. Meskipun sempat ada resistensi (Google menarik diri dari Project Maven karena protes karyawan), Pentagon terus menggaet kontraktor teknologi (misal: Palantir menggantikan Google, dan lain-lain.). Hasilnya, AS relatif unggul dalam *cyber situational awareness* (gambaran situasi siber global real-time) berkat kemampuan analitik big data. Intinya, kepemimpinan AS di domain siber ditandai keseimbangan: *ofensif terukur* (melalui Defend Forward), *defensif mendalam* (melindungi jaringan domestik kritis), dan *kolaborasi luas* (lintas lembaga dan sektor, termasuk internasional dengan sekutu NATO). AS juga mendorong pembentukan *norma internasional di dunia maya* agar perilaku negara bisa diatur (walau tantangannya besar karena Rusia-Tiongkok sering berbeda pandangan).

Israel – Integrasi Teknologi Canggih dan Intelijen di Setiap Operasi: Israel adalah contoh negara kecil yang mampu memiliki *impact* besar di ranah siber karena investasi cerdas pada SDM dan teknologi. Unit 8200 adalah jantungnya. Unit ini secara formal berada di bawah *Military Intelligence Directorate* (Aman), namun perannya lintas fungsi: melakukan signals intelligence (SIGINT) seperti penyadapan komunikasi (mirip NSA), sekaligus operasi siber ofensif (mirip US Cyber Command). Unit 8200 sering disebut "mata dan telinga" Israel – hampir semua operasi militer Israel mendapatkan masukan intelijen dari unit ini. Misalnya, sebelum pesawat tempur Israel menyerang target di Suriah, tim 8200 mungkin sudah meretas sistem pertahanan udara lawan untuk mematikan radar (seperti dalam serangan ke lokasi nuklir Suriah 2007, diduga dibantu operasi *cyber/electronic warfare*). Demikian pula, serangan *Stuxnet* ke fasilitas nuklir Natanz, Iran, menunjukkan keberanian dan kecanggihan operasi siber Israel bekerja sama dengan AS. Stuxnet berhasil merusak 1.000+ mesin sentrifugal uranium Iran melalui malware kompleks yang sangat spesifik – ini memperlambat program nuklir Iran beberapa tahun tanpa menembakkan satu peluru pun. Dunia baru sadar betapa dahsyat efek serangan siber fisik tersebut ketika terungkap tahun 2010.

Budaya kepemimpinan di Israel menekankan inovasi dan kewirausahaan. Unit 8200 merekrut banyak *programmer* muda berbakat, sering langsung dari bangku SMA melalui program Talpiot atau beasiswa militer khusus TI. Mereka dilatih intensif, diberi akses teknologi terbaru, lalu dipercaya memimpin proyek kritikal di usia sangat muda. Hierarki unit ini relatif datar – ide brilian dari prajurit yunior bisa langsung diimplementasikan jika terbukti efektif. Mantan anggota menggambarkan *atmosfer* di sana mirip *startup garage*, tidak kaku birokratis. Hal ini disengaja agar Israel tidak kalah cepat dari inovasi teknologi lawan. Hasilnya, alumni 8200 mendirikan puluhan perusahaan siber terkemuka (Check Point, Palo Alto Networks, NSO Group, dan lain-lain.), menjadikan Israel pemain dominan di industri sekuriti siber global. Pemerintah Israel pun mengintegrasikan siber ke doktrin nasional: pada 2017 Israel merilis *National*

Cybersecurity Strategy dengan pendekatan "Cyberdefense as a national mission", melibatkan *whole-of-society*. Bahkan, konsep *"digital Iron Dome"* pernah dicetuskan untuk menggambarkan betapa seriusnya mereka ingin melindungi ruang siber layaknya sistem pertahanan rudal.

Saat konflik militer, kemampuan siber Israel dioptimalkan. Contoh, selama pertempuran dengan Hamas/Hezbollah, Unit 8200 menjalankan SIGINT intensif untuk mengidentifikasi lokasi target (HP lawan disadap untuk intel posisi, dan sebagainya.), meretas komunikasi musuh untuk *psywar* (pernah ada laporan ribuan telepon pejuang Hezbollah tiba-tiba *meledak* karena malware Israel, membuat panik). Ini menggarisbawahi doctrine Israel bahwa *tidak ada perbedaan garis depan dan belakang di perang modern* – cyberspace menembus semuanya, maka kontrol atas informasi menentukan kemenangan. Dengan mengawinkan teknologi AI (misal: 2023 terungkap Unit 8200 pakai AI untuk memilih target Hamas secara lebih presisi) dan intelijen manusia, Israel mampu *punching above its weight* dalam hal kekuatan siber.

Singkatnya, tiga studi kasus di atas memberi spektrum pendekatan: Rusia (ofensif agresif, disinformasi tinggi, menghalalkan segala cara demi tujuan strategis), AS (ofensif terukur + defensif kuat, kolaboratif, berbasis aturan), Israel (inovatif, preemptive strikes, integrasi siber di setiap level operasi). Ketiganya berinvestasi besar di sumber daya teknologi siber, menunjukkan *leadership* adaptif di era digital. Pembelajaran bagi Indonesia: kita perlu memadukan elemen terbaik (misal: *proaktif dan visioner* seperti AS/Israel, *kesiapsiagaan terhadap disinfo* seperti menghadapi Rusia, *pembinaan SDM unggul* seperti Israel) sambil menghindari ekses (misal: jangan mencontoh penggunaan siber untuk pelanggaran hukum internasional atau represi domestik ala Rusia/Tiongkok).

b. Urgensi Doktrin Pertahanan Siber Indonesia

Melihat dinamika global tersebut, Indonesia berada pada posisi rawan jika tidak segera berbenah. Di satu sisi, tingkat ancaman siber terhadap Indonesia terus meningkat; di sisi lain, *kapabilitas dan kerangka kebijakan kita belum memadai*. Berikut beberapa poin yang menegaskan urgensi penyusunan *doktrin pertahanan siber nasional*:

1) Lonjakan Ancaman Siber Terhadap Indonesia: Berbagai insiden terkini menunjukkan kelemahan pertahanan digital kita. Kebocoran data 279 juta penduduk dari BPJS (Mei 2021) mengejutkan publik – data sensitif dijual bebas di forum gelap. Lalu *Bjorka* (2022) muncul menantang pemerintah dengan membocorkan surat menyurat Presiden, data registrasi SIM card, DAN LAIN-LAIN. Situs-situs kementerian dan BUMN berkali-kali diretas/dideface (contoh: situs KPU 2019 diubah tampilannya dan disisipkan hoaks soal server pemilu). Serangan ransomware juga pernah melanda RS dan instansi lokal. Ini menandakan bahwa musuh (state maupun non-state) telah aktif beroperasi di ruang siber Indonesia, entah untuk spionase, sabotase, kriminal, atau propaganda. Tanpa doktrin dan koordinasi kuat, respons kita selalu *kewalahan* dan terlambat. Misalnya, saat *data Kominfo 1,3 juta pengguna* bocor (2022), terjadi saling lempar tanggung jawab antara Kominfo dan BSSN karena ketiadaan aturan jelas siapa berwenang.

2) Ketiadaan Doktrin = Strategi Defensif Lemah: Hingga kini Indonesia belum punya *national cyber defense doctrine* yang menjadi acuan seluruh komponen. Para pakar mencatat hal ini membuat strategi kita cenderung reaktif dan defensif semata, *tidak proaktif* mencegah ancaman. Tanpa doktrin eksplisit, ruang siber Indonesia ibarat "grey area" tanpa kepemilikan jelas (lack of strategic ownership). Setiap lembaga

berjalan sendiri: BSSN fokus proteksi (defensif), TNI mulai bangun satuan siber (tapi kewenangan terbatas), Polri punya direktorat siber untuk penegakan hukum, BIN mungkin lakukan intelijen siber – namun *tanpa sinergi strategis*. Dampaknya, potensi tumpang tindih dan kebingungan sangat besar. Analis Lab45, Christian Guntur, menegaskan perlunya segera membentuk Komando Siber Terpadu agar kekuatan siber Indonesia punya struktur komando jelas dan terintegrasi. Ia menyoroti bahwa di Inggris ada National Cyber Force, di AS ada US Cyber Command – keduanya menggabungkan kekuatan militer dan intelijen siber dalam satu komando. Indonesia belum punya struktur serupa, sehingga upaya pertahanan digital kita tercerai-berai. Doktrin siber nasional akan menjadi *landasan konseptual dan operasional* untuk menyatukan berbagai elemen (TNI, BSSN, Polri, intelijen, kementerian, sektor swasta) menghadapi ancaman bersama, dengan peran dan kewenangan yang dibagi tegas.

3) Kerentanan Infrastruktur Kritis dan Ekonomi Digital: Indonesia sedang giat membangun ekonomi digital (e-commerce terbesar di Asia Tenggara, layanan digital publik, fintech, dan lain-lain.). Namun infrastruktur pendukungnya – pusat data, jaringan telekomunikasi, sistem SCADA PLN, dsb – rawan diserang. Tanpa doktrin, tidak jelas *siapa* melindungi sektor apa dalam skenario serangan terkoordinasi. Misal, jika jaringan listrik Jawa-Bali kena *cyberattack* (seperti dialami Ukraina 2015), apakah ini domain BSSN, atau TNI, atau PLN sendiri? Doktrin pertahanan siber akan menetapkan *Critical Infrastructure Protection (CIP)* skala nasional: mencakup identifikasi objek vital, standar keamanan minimum, mekanisme respon insiden terpadu. Ini sangat mendesak mengingat beberapa insiden: serangan ransomware WannaCry 2017 melumpuhkan Rumah Sakit Dharmais dan Harapan Kita; serangan ke satelit Telkom-1 (2017) ganggu 15 ribu ATM; serangkaian pemadaman listrik Jabodetabek (2019) diduga juga diwarnai serangan siber. Dengan doktrin siber, penanganan insiden akan lebih terstruktur dan cepat.

4) Dimensi Pertahanan Informasi (Disinformasi/Hoaks): Selain serangan teknis, Indonesia rentan terhadap *peperangan informasi*. Tahun 2019, menjelang Pemilu, beredar hoaks ada "server KPU di Singapura" untuk memenangkan paslon tertentu; ini nyaris memicu krisis kepercayaan publik. Begitu pula banjir misinformasi soal COVID-19, gerakan anti-vaksin di medsos, hingga ujaran kebencian SARA yang diperkeruh bot asing – semua contoh *information warfare* yang bisa melemahkan kohesi nasional. Tanpa doktrin/info ops yang jelas, upaya penangkalan hoaks sporadis dan kurang efektif. Pertahanan siber Indonesia harus mencakup pertahanan informasi: edukasi literasi digital massal, kemampuan deteksi dini kampanye disinformasi (mungkin lewat satuan khusus), serta protokol respon terkoordinasi (antara Kominfo, BSSN, Polri, komunitas media). Doktrin siber akan menegaskan hal ini sebagai bagian integral strategi pertahanan semesta.

5) Nilai-Nilai Nasional dan Legalitas: Doktrin siber nasional perlu berlandaskan nilai Pancasila, UUD 1945, dan komitmen terhadap hukum internasional. Dengan doktrin, Indonesia bisa menegaskan *posisi etis* di kancah siber global: misalnya kita tidak akan menggunakan kapabilitas siber untuk agresi melawan negara lain kecuali untuk pertahanan sah (sejalan politik luar negeri damai), tidak melakukan mata-mata atas warga sendiri secara melanggar hukum, serta menjunjung HAM di ruang digital. Ini

penting agar transformasi teknologi untuk pertahanan tidak kebablasan melanggar prinsip. Nilai Pancasila (seperti kemanusiaan, keadilan) dapat menjadi rambu dalam aturan engagement siber. Misal, meski punya kemampuan ofensif, Indonesia tidak akan meniru Rusia yang sembrono menyebar malware tak terkendali (NotPetya menyebar ke banyak negara tak terkait). Landasan nilai ini sekaligus memberi legitimasi domestik: rakyat perlu diyakinkan bahwa doktrin siber bertujuan melindungi mereka, bukan mengawasi mereka. Doktrin bisa memasukkan *prinsip transparansi dan akuntabilitas* operasi siber, pengawasan parlementer, dan sebagainya., sesuai koridor demokrasi Pancasila.

Singkatnya, ketiadaan doktrin siber nasional saat ini adalah celah strategis serius. Indonesia mendesak perlu menutup celah tersebut sebelum terjadi serangan besar yang melumpuhkan negara. Doktrin ini akan menjadi pedoman menghadapi ancaman baru, seperti halnya doktrin Sishankamrata menjadi pedoman ancaman militer-konvensional di masa lalu. Taruhannya adalah kedaulatan dan keamanan nasional di era digital.

c. Kerangka Doktrin Pertahanan Siber Berbasis Nasional

Berdasarkan studi banding dan kebutuhan lokal, berikut elemen-elemen utama yang diusulkan untuk Doktrin Pertahanan Siber Indonesia:

1) Pendekatan Pertahanan Siber Aktif (Active Cyber Defense): Doktrin harus mengadopsi strategi *pertahanan aktif*, artinya tidak sekadar bersifat pasif-menunggu serangan. *Active defense* mencakup deterrence (penangkalan) dan preemption (penindakan pendahuluan). Penangkalan dicapai dengan memperkuat keamanan sistem nasional sehingga musuh ragu menyerang (misal: sistem perbankan dilengkapi *intrusion prevention* berlapis). Namun, deterrence saja tidak cukup menghadapi ancaman yang tidak kenal batas. Maka perlu preemption: operasi intelijen siber ofensif terbatas untuk mencegah serangan sebelum terjadi. Contoh, jika terdeteksi kelompok hacker APT merencanakan sabotase PLTN, kita dapat (dengan otorisasi jelas) melakukan *counter-hack* ke infrastruktur mereka untuk mengganggu rencana tersebut. Prinsip *"serang sebelum diserang"* ini selaras konsep AS *Defend Forward*, namun disesuaikan dengan aturan Indonesia. Tentu, preemption hanya untuk ancaman serius yang terverifikasi intelijen. Dengan pertahanan aktif, Indonesia menunjukkan sikap tegas: bahwa ruang siber kita bukan *soft target*.

2) Implementasi pertahanan aktif melibatkan *cyber threat intelligence* canggih, pemantauan proaktif jaringan (threat hunting), dan tim reaksi cepat 24/7. Selain itu, perlu disiapkan kapabilitas *"hack back"* secara legal. Saat ini hukum kita belum mengatur boleh tidaknya aparat meretas balik server penyerang di luar negeri. Doktrin siber nasional harus memberikan landasan kebijakan: misal, Presiden selaku Panglima Tertinggi dapat mengotorisasi operasi siber ofensif terbatas di luar yurisdiksi Indonesia bila serangan terhadap kepentingan nasional sudah terjadi atau *imminent*. Tentunya hal ini tetap mengacu hukum internasional (prinsip *retorsion* atau *self-defense* dalam kerangka PBB). Pendekatan aktif juga mencakup penyebaran *cyber deception* (umpan jebakan honeypots) untuk menjebak peretas yang masuk, serta langkah-langkah kontra intelijen di dunia maya.

3) Struktur Komando dan Organisasi Terpadu: Doktrin siber harus menetapkan struktur kelembagaan pertahanan siber yang jelas. Mengacu praktik terbaik (AS,

Inggris), idealnya Indonesia membentuk Komando Siber Terpadu di bawah TNI yang menyatukan unsur militer dan intelijen siber. *Cyber Command* Indonesia ini akan memimpin operasi pertahanan siber militer (misal: melindungi network TNI, melakukan operasi siber ofensif terhadap target militer lawan) sekaligus berkoordinasi dengan badan sipil (BSSN, Bareskrim, BIN) untuk keamanan siber nasional. Komando Siber Terpadu sebaiknya dipimpin perwira tinggi minimal bintang 3 agar selevel komando utama lain (Kopassus, Kostrad, dan lain-lain.). Hal ini juga mengatasi masalah saat ini di mana Satsiber TNI masih bintang 1 – kurang strategis posisinya dibanding ancaman siber yang kian besar. Dengan menaikkan statusnya, talenta siber di TNI punya jalur karier jelas sehingga TNI tidak kehilangan SDM hebat ke sektor swasta.

4) Selain Komando Siber TNI, doktrin harus mengatur pembagian peran antarlembaga yang tegas. Misal: TNI Cyber Command bertanggung jawab pada *pertahanan siber strategis dan ofensif militer*, BSSN bertanggung jawab *keamanan siber nasional (defensif, proteksi infrastruktur kritis, koordinasi CERT)*, Polri menangani *penegakan hukum siber (cybercrime)*, BIN fokus pada *intelijen siber luar negeri*, Kominfo pada *regulasi dan literasi digital*, dan lain-lain. Regulasi nasional perlu diterbitkan (UU atau Perpres) untuk membagi peran dan wewenang ini secara hukum. Hal ini penting agar tidak ada overlap dan setiap entitas tahu batasannya (contoh: serangan siber oleh aktor negara => ranah TNI/BIN; serangan kriminal ransomware => ranah Polri/BSSN; hoaks domestik => ranah Kominfo/Polri; dan seterusnya, dengan kolaborasi tentunya). Doktrin juga bisa membentuk mekanisme koordinasi, semacam Cybersecurity Coordination Council gabungan TNI-sipil yang diketuai langsung Presiden atau Menkopolhukam, untuk mengambil keputusan cepat saat krisis siber nasional.

5) Dalam struktur komando, doktrin dapat mengusulkan integrasi elemen siber ke setiap matra angkatan. Misal, Angkatan Darat, Laut, Udara membentuk *unit siber organik* yang mendukung operasi masing-masing (AD melindungi kendaraan tempur digitalnya, AL melindungi kapal dari hacking, AU melindungi sistem radar/pesawat, dan lain-lain.), di bawah komando teknis Cyber Command. Model Israel bisa jadi acuan: mereka tempatkan operasi siber di intelijen militernya agar koordinasi sentral, mungkin Indonesia bisa taruh Cyber Command di bawah BAIS TNI (Badan Intelijen Strategis) namun dengan *mandat operasional luas*. Intinya, struktur harus menjamin unity of command di ruang siber.

6) Kolaborasi Publik–Swasta (Whole-of-Nation Cyber Defense): Doktrin siber nasional perlu mengakui bahwa pemerintah saja tak bisa melindungi seluruh ruang siber. Sebagian besar infrastruktur internet dan data berada di tangan swasta: mulai dari ISP, operator telekomunikasi, platform media sosial, fintech, perbankan, pembangkit energi, dan sebagainya. Diperkirakan >80% infrastruktur siber nasional dimiliki/dioperasikan entitas non-pemerintah. Oleh sebab itu, strategi pertahanan siber harus *inklusif*, melibatkan sektor swasta sebagai mitra. Cara konkretnya: membangun Public-Private Partnership (PPP) di bidang keamanan siber. Pemerintah bisa membentuk *Cybersecurity Information Sharing Forum* di mana BSSN/TNI rutin berbagi intelijen ancaman dengan perusahaan critical infrastructure, dan sebaliknya perusahaan memberi masukan situasi lapangan. *Trust* perlu dibangun agar swasta mau melapor insiden dengan cepat tanpa takut sanksi atau malu (mirip model ISAC di AS). Selain itu,

standarisasi keamanan perlu dibuat untuk sektor-sektor (misal standar minimal keamanan untuk bank, bandara, PLN, dan lain-lain.). Perusahaan raksasa teknologi (Google, Microsoft, etc.) yang beroperasi di Indonesia juga harus dirangkul dalam ekosistem pertahanan siber – bisa melalui MoU untuk bantu penanggulangan hoaks, phishing, serangan supply chain, dan lain-lain.

7) Doktrin juga perlu memasukkan *insentif* bagi swasta dalam partisipasi pertahanan siber. Contoh, memberikan *tax incentive* bagi perusahaan yang berinvestasi besar di cybersecurity. Atau membentuk Cadangan Siber (Cyber Reserve): merekrut para profesional TI di industri menjadi komponen cadangan TNI yang bisa dikerahkan saat krisis (mirip konsep *Komcad* tetapi khusus siber). Ini win-win: talenta swasta bisa berkontribusi bela negara secara paruh waktu; TNI terbantu ahli terbaik. Beberapa negara seperti Estonia sudah melakukan ini dengan sukses.

8) Pemberdayaan Masyarakat dan Literasi Siber: Mengikuti konsep *pertahanan semesta*, rakyat harus jadi bagian pertahanan siber. Doktrin mesti memasukkan program peningkatan literasi digital dan ketahanan informasi masyarakat sebagai salah satu pilar. Singapura memberikan contoh baik dengan menambah *Digital Defence* sebagai pilar ke-6 *Total Defence* mereka. Mereka menjalankan kampanye agar setiap warga "Be Secure, Alert, and Responsible Online" – artinya setiap orang berperan menjaga keamanan siber pribadi, waspada hoaks, dan bertindak bertanggung jawab di internet. Indonesia dapat melakukan hal serupa: memasukkan *edukasi literasi siber* dalam kurikulum sekolah, pelatihan di kalangan PNS/TNI/Polri, hingga kampanye publik melawan hoaks. Dengan masyarakat yang melek digital, musuh akan lebih sulit menyebar disinformasi atau melakukan rekayasa sosial.

9) Selain literasi, keterlibatan masyarakat dalam deteksi dini juga penting. Misal, membuat kanal aduan serangan siber nasional di mana siapa pun bisa melapor jika menemukan anomali (phishing massal, indikasi data bocor, dan lain-lain.), yang terhubung ke CSIRT nasional. Seperti konsep *siskamling digital*. Masyarakat juga perlu diajak melindungi dirinya: contohnya BSSN bisa menginisiasi gerakan pakai *password manager* dan 2FA secara nasional. Walau terkesan sepele, jika jutaan orang mengamankan akunnya, ruang serang musuh mengecil.

10) Penegakan Hukum dan Kerangka Legal: Doktrin pertahanan siber tak lengkap tanpa dukungan hukum. Perlu segera disahkan regulasi komprehensif – misalnya UU Keamanan dan Ketahanan Siber – yang menjadi *payung hukum* segala aktivitas pertahanan siber. Regulasi ini mengatur kewenangan TNI dalam operasi siber (agar jelas legalitasnya saat melakukan misal exploit ke server luar yang menyerang Indonesia), tugas BSSN secara rinci, sanksi bagi *cybercrime*, serta koordinasi. Saat ini payung hukum masih tersebar: UU ITE (untuk kejahatan siber umum), PP Security System, dan lain-lain. Perpres No.82/2022 sudah mengatur perlindungan infrastruktur informasi vital, namun perlu ditingkatkan jadi UU agar lebih kuat. Doktrin siber nasional sebaiknya merekomendasikan pemerintah dan DPR untuk menyusun regulasi khusus pertahanan/keamanan siber. Tanpa landasan hukum, aksi-aksi pertahanan siber berisiko dipersoalkan (baik di dalam negeri oleh LSM, maupun di fora internasional).

11) Kerangka legal juga mencakup *Standard Operating Procedures (SOP)* lintas instansi. Misal, bila terjadi serangan siber besar: SOP A1 dijalankan – BSSN memimpin

teknis penanganan, TNI siaga jika eskalasi antar negara, Polri amankan situasi publik, Kominfo atur komunikasi publik, dan sebagainya. Semua diatur sebelumnya dalam doktrin.

12) Kerja Sama Internasional dan Diplomasi Siber: Doktrin harus menempatkan pertahanan siber Indonesia dalam konteks global. Artinya, Indonesia perlu aktif membangun kerja sama internasional dalam keamanan siber. Kawasan ASEAN misalnya, telah memiliki *ASEAN Cybersecurity Cooperation Strategy* dan forum-forum seperti ASEAN Ministerial Conference on Cybersecurity. Doktrin kita sebaiknya memasukkan komitmen ikut serta dalam Confidence Building Measures (CBMs) regional – tujuannya mengurangi risiko miskalkulasi antar negara di ruang siber. Misal, bertukar poin kontak penanggulangan insiden antar negara, latihan bersama menangani serangan, dan sebagainya. Juga, Indonesia bisa dorong *Norms of Responsible State Behavior in Cyberspace* di PBB (kita pernah aktif di OEWG PBB soal siber).

13) Diplomasi siber juga berguna untuk *transfer teknologi*: menjalin kemitraan dengan negara maju (AS, Estonia, Singapura) untuk pendidikan dan peningkatan kapasitas. Doktrin bisa mengamanatkan pembentukan *Cyber Defense Center of Excellence* di Indonesia bekerja sama dengan NATO CCDCOE atau sejenis, agar TNI dan BSSN bisa belajar taktik terkini. Selain itu, harus ada strategi melindungi kepentingan Indonesia di fora global – misal, menolak prakarsa yang bisa merugikan kebebasan digital warga (seperti dominasi aturan siber negara otoriter).

14) Kesemua elemen di atas harus disusun dalam doktrin tertulis yang disahkan otoritas (Menhan/Panglima TNI) dan diumumkan ke publik (setidaknya secara umum). Doktrin ini menjadi panduan jangka panjang (5-10 tahun) pembangunan kekuatan siber Indonesia. Dengan kerangka tersebut, diharapkan sumber daya teknologi yang kita miliki dapat dioptimalkan sebagai kekuatan pertahanan, bukan sekadar infrastruktur pasif.

d. Studi Perbandingan Regional: Belajar dari Negara Tetangga

Sebelum menyusun kebijakan final, ada baiknya melihat pendekatan negara kawasan dalam keamanan siber, agar Indonesia bisa mengambil yang relevan dan menghindari yang tidak cocok.

Singapura – "Total Defence" termasuk Digital Defence: Singapura merupakan contoh pemimpin regional dalam strategi keamanan siber. Pada 2019, Singapura menambahkan *Digital Defence* sebagai pilar keenam konsep *Total Defence* mereka. Ini pengakuan bahwa ancaman digital sama nyata dengan ancaman fisik. *Digital Defence* di Singapura melibatkan program lintas masyarakat: kampanye literasi, simulasi serangan nasional, dan latihan tanggap insiden. Pemerintah Singapura giat mengedukasi warga untuk *"jadi aman, waspada, dan bertanggung jawab online"*. Misalnya, mereka mengajarkan publik cara mengenali hoaks dan melaporkannya, serta pentingnya *cyber hygiene* (password kuat, update antivirus, 2FA). Singapura juga membentuk Cyber Security Agency (CSA) tersendiri, terpisah dari militer, tetapi bekerjasama erat dengan *Defense Science dan Technology Agency* untuk hal pertahanan. *Lesson learned:* pendekatan Singapura menekankan kesadaran publik dan keterlibatan seluruh elemen. Ini patut dicontoh Indonesia, mengingat tantangan hoaks dan rendahnya literasi digital di masyarakat kita. Program seperti Media Literacy Council atau *Better Internet Campaign* Singapura bisa diadaptasi oleh Kominfo/BSSN di sini.

Singapura juga rutin mengadakan *EX cybersecurity exercises* berskala nasional**, melibatkan sektor publik dan privat dalam simulasi serangan terhadap infrastruktur penting (air, listrik, transportasi). Hal ini melatih koordinasi dan kesiapsiagaan. Indonesia sebaiknya melakukan hal serupa (latihan *Cyber Garuda* misalnya) untuk menguji protokol dan kemampuan kita.

Vietnam – "Force 47" dan Operasi Opini Dunia Maya: Vietnam mengambil pendekatan berbeda, yang lebih kontroversial. Pemerintah Vietnam secara terselubung membentuk *"Force 47"*, yaitu unit perang informasi dunia maya di bawah Tentara Rakyat Vietnam. Force 47 terdiri dari ribuan tentara siber yang ditugasi memantau dan memoderasi diskursus online, khususnya di Facebook, demi menjaga citra rezim. Mereka mendirikan ratusan grup Facebook pro-pemerintah, melakukan *counter-narrative* terhadap kritik, dan bahkan berusaha mengoordinir *mass-report* untuk menutup akun pengkritik. Singkatnya, Force 47 adalah *"cyber army"* domestik yang fokus pada propaganda dan sensor. Sementara dari sisi pertahanan siber teknis, Vietnam juga membentuk *Cyber Command* (diresmikan 2017) namun infonya minim. Pendekatan Vietnam ini efektif membendung oposisi online (bagi rezim mereka), namun dari kacamata demokrasi, jelas tidak sejalan dengan kebebasan berekspresi. Bagi Indonesia, yang berlandaskan demokrasi Pancasila, model Force 47 tidak cocok. Kita tidak ingin militer digunakan untuk membungkam pendapat warga di dunia maya. Namun, ada hal yang bisa diambil: misalnya, Vietnam berhasil mengorganisir ribuan *cyber warriors* muda. Indonesia juga bisa merekrut ribuan talenta muda TI tapi diarahkan ke hal positif – bukan sensor, melainkan *membanjiri ruang maya dengan konten narasi Pancasila* yang mencerahkan atau melawan hoaks teroris. Intinya, *the spirit* mobilisasi orang muda digital bisa ditiru untuk hal baik.

Malaysia dan Thailand relatif belum menonjol kebijakan sibernya, meski pasti mereka juga meningkatkan kapasitas. Malaysia punya National Cyber Security Policy (NCSP) sejak 2006, mengutamakan perlindungan infrastruktur kritis dan pembentukan CyberSecurity Malaysia (mirip BSSN). Baru-baru ini Malaysia membahas RUU Keamanan Siber. Thailand membentuk *Cyber Operation Center* di bawah militernya, juga sempat kontroversial dengan UU Kejahatan Komputer ketat.

Kesimpulan perbandingan regional: Indonesia bisa banyak belajar dari Singapura soal strategi komprehensif dan literasi publik, serta mengambil *cautionary tale* dari Vietnam – bahwa *cyber force* sebaiknya difokuskan ke pertahanan, bukan propaganda domestik. Model kerjasama publik-swasta Singapura (mereka libatkan perusahaan Singtel, Tokopedia, dan lain-lain. lokal dalam Cybersecurity Advisory Group) sangat relevan. Selain itu, ada inisiatif ASEAN yang bisa dimanfaatkan: ASEAN sudah menyepakati 11 norma perilaku di ruang siber mengikuti rekomendasi PBB. Indonesia perlu memastikan doktrin nasional sejalan dengan norma ini agar kita tak terisolasi. Contoh norma: *tidak membiarkan teritori kita dipakai untuk aktivitas siber berbahaya*, *harus menolong negara lain jika diminta pasca-serangan siber*, dan sebagainya. Doktrin Indonesia bisa memasukkan komitmen mematuhi norma ini.

e. Rekomendasi Kebijakan dan Roadmap Implementasi

Berdasarkan seluruh analisis, berikut rekomendasi langkah konkret bagi Indonesia untuk mentransformasi sumber daya teknologi menjadi kekuatan pertahanan:

1) Segera Susun dan Sahkan Doktrin Pertahanan Siber Nasional: Pemerintah (Kemenhan) bersama TNI, BSSN, Kominfo, BIN, Polri, akademisi, dan pakar harus duduk bersama merumuskan *National Cyber Defense Doctrine*. Doktrin sebaiknya

disahkan dalam bentuk Peraturan Presiden atau setidaknya Peraturan Menteri Pertahanan, agar mengikat lintas instansi. Target waktu: dalam 1-2 tahun ke depan doktrin sudah terbit. Isi doktrin mencakup visi, prinsip, struktur komando, pembagian peran, aturan penggunaan kekuatan siber, proteksi infrastruktur vital, hingga kolaborasi publik-swasta. Keterlibatan banyak pihak dalam perumusan penting agar doktrin komprehensif. Setelah disahkan, lakukan *sosialisasi* ke seluruh aparatur dan pemangku kepentingan.

2) Tingkatkan Status dan Kapasitas Organisasi Siber TNI: Dorong pemerintah menerbitkan Keppres/Perpres peningkatan Satuan Siber TNI menjadi Komando Madya (setara Kogabwilhan) di bawah Panglima TNI. Lengkapi dengan peningkatan anggaran, personel, dan sarana. Rekrut talenta IT nasional ke dalamnya – bisa dengan skema *wajib militer siber* bagi lulusan TI atau program beasiswa ikatan dinas. Selain itu, bentuk Cyber Reserve (Komponen Cadangan Siber) berisi profesional swasta yang dilatih dan bisa dimobilisasi. Belajar dari pengalaman, tanpa jenjang karier jelas, tentara siber akan keluar; maka berikan prospek karier (jabatan *Panglima Komando Siber* bintang 3 misalnya). Pastikan juga setiap matra TNI punya detasemen siber sendiri yang terhubung komando pusat.

3) Perkuat Kerangka Hukum: Selesaikan dan sahkan Undang-Undang Keamanan dan Pertahanan Siber. Jika RUU sempat ada (dulu pernah diusulkan Komisi I tapi ditolak 2019), perlu diperbarui dan diajukan lagi. UU ini minimal mengatur: kewenangan operasi siber oleh aparat negara, perlindungan data strategis, kewajiban keamanan bagi penyelenggara sistem elektronik kritikal, koordinasi antar lembaga siber, dan partisipasi sektor privat. Juga memuat sanksi pidana bagi pelaku serangan siber negara lain (untuk memudahkan dasar tuntutan secara *in absentia* jika perlu). Selain itu, revisi UU ITE untuk mengakomodasi hal-hal terkait *cyberwarfare* (karena UU ITE sekarang fokus transaksi elektronik dan konten ilegal, belum cover cyber espionage/war). Regulasi turunan juga perlu: misal Perpres tentang Komando Siber, Inpres tentang Tanggap Insiden Siber, dan sebagainya., mengikuti garis doktrin. Dengan payung hukum kuat, langkah pertahanan siber tidak ragu dan punya legitimasi.

4) Investasi SDM: Pendidikan dan Pelatihan: Program peningkatan SDM siber harus berskala nasional. Kemenhan dan TNI bisa bekerja sama dengan Kemendikbud mengembangkan kurikulum *Cybersecurity* di universitas (mungkin kelas khusus di Universitas Pertahanan atau Institut Pertahanan Siber). Buka program beasiswa TNI untuk bidang TI di kampus-kampus top, dengan imbalan dinas beberapa tahun. Adakan *kompetisi bakat siber* (CTF – Capture The Flag) rutin tingkat nasional untuk menjaring bakat dari usia dini. BSSN sendiri perlu memperluas Diklat bagi aparat pemerintah di daerah agar semua instansi punya personel mahir siber. Pembentukan Cyber Academy tersendiri patut dipertimbangkan – semacam Akmil tapi fokus perang siber (bisa berupa sekolah pasca-akademi khusus perwira muda TNI/Polri/ASN belajar strategi siber). *Roadmap* 5 tahun: target melatih setidaknya 1000 "*Cyber First Responders*" di tiap sektor (energi, keuangan, transportasi, dan lain-lain.). Juga, libatkan komunitas hacker *white-hat* lokal (Defcon groups, ID-CERT, dan sebagainya.) sebagai *civilian cyber corps*. Mereka bisa membantu audit keamanan lembaga pemerintah secara sukarela (tentu dengan aturan).

5) Proteksi Infrastruktur Kritis: Lakukan audit menyeluruh terhadap Critical Information Infrastructure (CII) negara: pembangkit listrik, sistem perbankan (ATM, RTGS), transportasi (ATC bandara, sistem KA), dan lain-lain. Identifikasi kerentanan dan tingkatkan keamanannya segera (update sistem, patch, segmentasi jaringan). Bentuk *Public-Private Working Group* per sektor untuk merumuskan SOP darurat. Simulasi serangan siber skala nasional minimal 1 kali setahun melibatkan sektor-sektor ini. Contoh skenario: serangan malware ke jaringan PLN – latih koordinasi BSSN, PLN, Siber TNI, Polri dalam pemulihan. Hasil latihan dijadikan umpan balik memperbaiki doktrin/plan. Selain itu, pertimbangkan adopsi *prinsip keamanan siber by design* dalam proyek infrastruktur baru (seperti rencana pembangunan ibu kota baru: sejak awal jaringan di sana harus secure by design). Doktrin siber perlu menegaskan infrastruktur vital = objek pertahanan layaknya wilayah teritorial, sehingga sumber daya TNI bisa dikerahkan untuk melindunginya jika diserang (misal tim siber TNI membantu restore layanan Telkom jika kena serang masif).

6) Literasi dan Kesadaran Publik: Luncurkan Gerakan Nasional Literasi Digital untuk Keamanan. Bisa diintegrasikan dengan program *literasi digital* Kominfo yang sudah ada, namun diperkuat aspek pertahanan. Kampanye nasional bisa mengusung slogan semisal *"Jaga Ruang Siber, Jaga Indonesia"*. Libatkan influencer positif, komunitas IT, pramuka, ormas kepemudaan, dan tokoh masyarakat. Materi edukasi: cara hindari phishing, verifikasi berita sebelum share, etika bermedia sosial, dan sadar akan adanya *operasi informasi asing*. Pemerintah daerah didorong buat program lokal (misal: Pemprov bikin *Cyber Hygiene Day* sebulan sekali). Secara jangka panjang, masukkan topik keamanan siber dalam pendidikan formal (misal di mapel PKN atau TIK di SMA ada bab "Pembelaan Negara di Ruang Siber"). Tujuannya membentuk budaya keamanan sejak dini. Doktrin siber semestinya menyatakan bahwa rakyat adalah lapisan pertahanan pertama di ruang siber – setiap individu yang peduli keamanan digitalnya berarti memperkuat keamanan nasional. Sebagai contoh keberhasilan, *Studi Microsoft* menunjukkan faktor manusia (password lemah, tertipu hoaks) adalah penyebab 90% insiden siber; ini yang harus kita tanggulangi lewat literasi.

7) Kerja Sama Internasional yang Proaktif: Kemenlu bersama BSSN/TNI perlu meningkatkan profil Indonesia dalam kerja sama siber. Join ASEAN Cybersecurity Cooperation Strategy dengan aksi nyata (tawarkan Indonesia jadi tuan rumah latihan siber ASEAN, misalnya). Jalin *cyber dialogue* bilateral dengan negara sahabat untuk tukar info ancaman (sudah ada dengan Australia, perluas ke Jepang, India, dan sebagainya.). Gabung inisiatif global: *Cybersecurity Tech Accord*, *Paris Call for Trust and Security in Cyberspace* – untuk menunjukkan komitmen Indonesia pada ekosistem siber yang damai. Selain itu, kirim perwira/ahli kita untuk magang di unit siber negara maju (banyak program fellowship tersedia). Sebaliknya, undang pakar internasional melatih personel kita. Doktrin siber harus membuka ruang untuk diplomasi siber, termasuk opsi aliansi pertahanan siber regional jika diperlukan di masa depan.

Roadmap implementasi dari rekomendasi di atas dapat disusun berjenjang: *jangka pendek* (1-2 tahun: susun doktrin, bentuk struktur komando, audit infrastruktur), *jangka menengah* (3-5 tahun: UU disahkan, peningkatan SDM signifikan, integrasi latihan rutin, partisipasi aktif di forum internasional), *jangka panjang* (>5 tahun: kemandirian teknologi

pertahanan siber, misal produk dalam negeri untuk keamanan, serta reputasi Indonesia diakui sebagai negara tangguh siber).

Kesimpulan

Di era digital ini, kepemimpinan pertahanan ditantang untuk mampu *mengintegrasikan sumber daya teknologi ke strategi keamanan nasional*. Negara-negara seperti Rusia, AS, dan Israel telah menunjukkan contoh konkret. Mereka membangun unit siber khusus, mengembangkan talenta digital unggul, dan menyusun doktrin jelas yang menjadikan siber dan informasi bagian tak terpisahkan dari postur pertahanan. Rusia memanfaatkan siber dan disinformasi untuk melumpuhkan lawan sebelum tank masuk; AS merumuskan strategi proaktif *Defend Forward* dan *persistent engagement* untuk melindungi kepentingannya di domain maya; Israel mengasimilasikan kecanggihan teknologi ke setiap operasi militer.

Bagi Indonesia, pelajaran ini sangat berharga. Tanpa adaptasi, kita berisiko menjadi korban perang siber dan informasi yang dapat melemahkan kedaulatan tanpa satu pun musuh menjejakkan kaki di wilayah kita. Sudah terbukti kita rentan: data warga bocor, situs pemerintah diretas, hoaks mengaduk emosi publik. Karena itu, penyusunan Doktrin Pertahanan Siber Nasional tidak bisa ditunda lagi. Doktrin tersebut harus dirancang *khas Indonesia*: melindungi kepentingan nasional di ruang siber, memperkuat ketahanan informasi masyarakat, namun tetap berpegang pada nilai Pancasila dan prinsip hukum internasional yang kita junjung.

Transformasi sumber daya teknologi (siber, AI, big data) menjadi kekuatan pertahanan akan meningkatkan daya tangkal Indonesia di era digital. Dengan kepemimpinan visioner yang berani berubah dan kebijakan proaktif, Indonesia dapat beralih dari posisi rentan menjadi bangsa tangguh di ruang siber – siap menghadapi ancaman apa pun terhadap integritas dan keamanan nasional. Langkah-langkah konkrit seperti yang direkomendasikan (peningkatan struktur, SDM, doktrin, kolaborasi) harus segera diambil agar *"keamanan nasional siber"* tidak tertinggal dari keamanan konvensional. Pada akhirnya, pertahanan siber adalah bagian dari mempertahankan kedaulatan NKRI di abad ke-21. Jika kita berhasil mengelola transformasi ini, Indonesia bukan hanya mampu melindungi diri, tapi juga berkontribusi positif pada terciptanya tatanan dunia maya yang aman dan damai sesuai amanat kemerdekaan kita.

Daftar Pustaka:

German Marshall Fund. (2020). *Fact Sheet: What We Know about Russia's Interference Operations* – Laporan yang merinci operasi intervensi Rusia pada Pemilu AS 2016, menunjukkan kampanye disinformasi terorganisir melemahkan demokrasigmfus.orggmfus.org.

U.S. Department of Defense. (2018). *Summary: Department of Defense Cyber Strategy* – Dokumen strategi siber DoD AS yang memperkenalkan konsep "Defend Forward", yaitu menyerang peretas lawan sebelum mereka menyerang AScybercom.mil.

Reuters. (2024). *What is Israel's secretive cyber warfare unit 8200?* – Artikel Reuters tentang Unit 8200 Israel, menjelaskan operasi dan peran unit siber elit tersebut, termasuk keberhasilannya seperti serangan Stuxnet terhadap program nuklir Iranreuters.com.

BSSN dan Kemenhan RI. (2020). *Strategi Keamanan Siber Nasional* – (Rencana strategi keamanan siber nasional Indonesia yang diharapkan; hingga kini belum ada doktrin siber nasional resmi, menunjukkan urgensi kekosongan iniejournal.appihi.or.id).

Konsep Doktrin Siber TNI (Wacana, dokumen internal) – Konsep doktrin pertahanan siber yang tengah dibahas di lingkungan TNI sebagai acuan format penyusunan doktrin resmi di masa mendatang.