Syntax Admiration: p-ISSN 2722-7782 | e-ISSN 2722-5356 Vol. 5, No. 2, Februari 2024

INISIASI PEMBENTUKAN ANGKATAN SIBER DAN DIGITAL DALAM ORGANISASI TENTARA NASIONAL INDONESIA

Nurmaida Delviana
Sekolah Tinggi Hukum Militer"AHM-PTHM", Jakarta, Indonesia
Email: delviananurmaida123@gmail.com

Abstrak

Dalam era transformasi digital, setiap Negara di Dunia harus mampu beradaptasi dan mengadopsi perubahan tersebut sebagai strategi untuk memperkuat pertahanan negara karena ruang siber dalam kaitannya dengan hubungan internasional dapat menjadi sumber berbagai potensi ancaman, kerentanan, dan ketidak-amanan pada tatanan internasional. Tiongkok menyadari pentingnya AI dalam membentuk lingkungan ekonomi, militer, dan geopolitik global di masa depan, lalu meluncurkan "Rencana Pengembangan Kecerdasan Buatan Generasi Berikutnya." yang bertujuan untuk menjadi pemimpin global dalam bidang AI pada tahun 2030. Metode Penelitian yang digunakan adalah preskriptif analisis dan analisa data pendekatan kualitatif. Berdasarkan hasil penelitian, ada 4 (empat) poin penting guna mewujudkan hal tersebut yakni keselarasan peraturan terkait siber dan digital di Indonesia dengan inisiasi tersebut dengan revisi baik dalam bentuk usulan pasal baru dan/atau reviu pada Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia, lalu pembangunan infrastruktur digital di Indonesia, pembinaan literasi digital di Indonesia, dan strategi penggalangan personil dengan tepat berdasarkan keadaan sumber daya manusia di Indonesia.

Kata Kunci: Hukum Militer, Angkatan Siber dan Digital, Tentara Nasional Indonesia

Abstract

In the era of digital transformation, every country in the world must be able to adapt and adopt these changes as a strategy to strengthen national defense because cyberspace in relation to international relations can be a source of various potential threats, vulnerabilities, and insecurity in the international order. China recognized the importance of AI in shaping the future global economic, military and geopolitical environment, and launched the "Next Generation Artificial Intelligence Development Plan." which aims to become a global leader in AI by 2030. The research method used is prescriptive analysis and qualitative data analysis. Based on the results of the study, there are 4 (four) important points to realize this, namely the alignment of regulations related to cyber and digital in Indonesia with the initiation with revisions both in the form of proposed new articles and / or reviews in Law Number 34 of 2004 concerning the Indonesian National Army, then digital infrastructure development in Indonesia, digital literacy development in Indonesia, and appropriate personnel mobilization strategies based on the state of human resources in Indonesia.

Keywords: *Military Law, Cyber and Digital Forces, Indonesian National Army*

How to cite:	Nurmaida Delviana (2024) Inisiasi Pembentukan Angkatan Siber dan Digital dalam Organisasi Tentara Nasional Indonesia, *(5) 2*
E-ISSN:	2722-5356
Published by:	Ridwan Institute

Pendahuluan

Dunia telah menghadapi beberapa tren dalam sepuluh tahun terakhir. Tren ini dikenal sebagai megatren. Megatrends yang dipopulerkan pada tahun 2016 oleh Price waterhouse Coopers (PWC), terdiri dari lima aspek, termasuk kebangkitan teknologi, perubahan demografi, urbanisasi yang pesat, perubahan iklim, dan pergeseran dalam kekuatan ekonomi global. Selain itu, disrupsi teknologi selama pandemi memaksa seluruh pemangku kepentingan untuk berinovasi dan berkreasi (Elisabeth, 2019).

Kemudahan akses, kecepatan dan konektifitas dari internet menjadi suatu hal yang banyak dimanfaatkan oleh masyarakat pada berbagai negara dalam berbagai aspek kehidupan dengan persebaran informasi yang mudah (Lovina, 2022). Seiring dengan pemakaian jaringan sistem komputer yang menggunakan infrastruktur sistem telekomunikasi membuat masyarakat sebagai penggunanya seolah-olah mendapati dunia baru, konsep ini sering dinamakan sebagai *cyberspace* (Sanusi, 2005). *Cyberspace* (ruang siber) adalah tempat maya yang dimana komunikasi tersebut terjadi (John, 2008).

Dalam era transformasi digital ini, setiap negara di dunia harus mampu beradaptasi dan mengadopsi perubahan tersebut sebagai strategi untuk memperkuat pertahanan negara. Terkait perkembangan dunia siber, Tiongkok menyadari pentingnya AI dalam membentuk lingkungan ekonomi, militer, dan geopolitik global di masa depan. Kemampuan menguasainya akan menentukan kekuatan suatu negara di kancah global. Oleh karena itu, pada tahun 2017 Tiongkok meluncurkan "Rencana Pengembangan Kecerdasan Buatan Generasi Berikutnya."

Rencana tersebut bertujuan untuk mengubah Tiongkok menjadi pemimpin global dalam bidang AI pada tahun 2030. Untuk mencapai tujuan ini, Tiongkok telah merekrut raksasa teknologinya, termasuk Baidu, Tencent, Alibaba, dan iFlytek. Alibaba, misalnya, ditugaskan untuk membangun Xiongan New Area, sebuah zona ekonomi baru sekitar 60 mil barat daya Beijing, menjadi 'kota pintar' AI yang meniru kota Hangzhou. Di Hangzhou, Alibaba menyerap data dari ribuan kamera jalanan dan menggunakannya untuk mengoptimalkan arus lalu lintas di kota melalui AI.

AI dapat menjadi alat yang sangat berguna dalam menyaring data dalam jumlah besar, termasuk dalam memproyeksikan kekuatan tajam atau diplomasi manipulatif. Dengan kemampuan analisis yang canggih, AI dapat membantu mengidentifikasi kebijakan diplomatik yang mungkin digunakan oleh suatu negara untuk mempengaruhi dan melemahkan sistem politik negara target. Sementara itu di Amerika Serikat pada tanggal 9 Agustus 2023, Pemerintahan Biden-Harris meluncurkan kompetisi besar berdurasi dua tahun yang akan menggunakan kecerdasan buatan (AI) untuk melindungi perangkat lunak paling penting di Amerika Serikat, seperti kode yang membantu menjalankan internet dan infrastruktur penting.

"AI *Cyber Challenge*" (AIxCC) akan menantang pesaing di seluruh Amerika Serikat, untuk mengidentifikasi dan memperbaiki kerentanan perangkat lunak menggunakan AI. Dipimpin oleh *Defense Advanced Research Projects Agency* (DARPA), kompetisi ini akan mencakup kolaborasi dengan beberapa perusahaan AI

terkemuka–Anthropic, Google, Microsoft, dan OpenAI – yang menyumbangkan keahlian mereka dan menyediakan teknologi mutakhir untuk tantangan ini.

Kompetisi ini, yang akan berhadiah hampir 20 juta Dolar Amerika Serikat, akan mendorong penciptaan teknologi baru untuk meningkatkan keamanan kode komputer secara cepat, yang merupakan salah satu tantangan keamanan siber yang paling mendesak. Hal ini menandai langkah terbaru Pemerintahan Biden-Harris untuk memastikan kemajuan teknologi baru yang bertanggung jawab dan melindungi warga Amerika.

Dalam konteks operasi militer dalam konflik bersenjata, Amerika Serikat percaya bahwa Hukum Humaniter Internasional (IHL) memberikan kerangka kerja yang kuat dan tepat untuk mengatur semua senjata, termasuk senjata yang menggunakan fungsi otonom yang disediakan oleh teknologi seperti AI. Di sisi lain, nampaknya Singapura telah memitigasi ancaman akibat adanya transformasi digital yang sedang dan/atau akan datang, dengan meluncurkan *Digital Intelligence Service* (DIS) yang didirikan pada parade pengukuhan yang diresmikan oleh Presiden Halimah Yacob di Institut Militer SAFTI pada 28 Oktober 2022.

Hal tersebut merupakan kekuatan militer baru di Angkatan Bersenjata Singapura (SAF) yang fokus pada peperangan digital, elektronik, dan informasi. DIS menggabungkan berbagai kemampuan komando, kontrol, komunikasi, komputer, dan intelijen (C4I) ke dalam satu entitas yang dapat mengatasi ancaman yang belum sepenuhnya tercakup oleh layanan militer lainnya. DIS memiliki misi mempertahankan dan mendominasi domain digital. Sebagai bagian dari SAF yang terintegrasi, DIS akan meningkatkan keamanan Singapura, dari masa damai hingga perang.

DIS Training Command bertugas untuk berkolaborasi dengan sekolah-sekolah pelatihan untuk mengembangkan tenaga kerja DIS, mengadakan pelatihan kompetensi kejuruan dan lanjutan di berbagai bidang seperti pertahanan siber dan intelijen. SAF C4 Command bertugas untuk membangun, mengoperasikan dan menjaga kemampuan Komando, Kontrol, Komunikasi, dan Komputer (C4) untuk MINDEF/SAF, sambil mendorong digitalisasi angkatan bersenjata.

Digital Defence Command bertugas untuk mengembangkan kemampuan perlindungan elektronik dan pertahanan psikologis untuk mengatasi ancaman keamanan yang terus berkembang. Joint Intelligence Command bertugas untuk memberikan intelijen yang akurat, relevan, dan tepat waktu untuk peringatan dini dan pengambilan keputusan untuk operasi SAF. Digital Ops-Tech Centre tugasnya adalah untuk meningkatkan tenaga kerja digital yang menerapkan praktik teknik yang kuat dan mengembangkan solusi digital bagi SAF untuk memenuhi kebutuhan operasional yang terus berubah, dan bermitra dengan digital.

DIS Training Command bertugas untuk berkolaborasi dengan sekolah-sekolah pelatihan untuk mengembangkan tenaga kerja DIS, mengadakan pelatihan kompetensi kejuruan dan lanjutan di berbagai bidang seperti pertahanan siber dan intelijen. SAF C4 Command bertugas untuk membangun, mengoperasikan dan menjaga kemampuan

Komando, Kontrol, Komunikasi, dan Komputer (C4) untuk MINDEF/SAF, sambil mendorong digitalisasi angkatan bersenjata.

Digital Defence Command bertugas untuk mengembangkan kemampuan perlindungan elektronik dan pertahanan psikologis untuk mengatasi ancaman keamanan yang terus berkembang. Joint Intelligence Command bertugas untuk memberikan intelijen yang akurat, relevan, dan tepat waktu untuk peringatan dini dan pengambilan keputusan untuk operasi SAF. Digital Ops-Tech Centre tugasnya adalah untuk meningkatkan tenaga kerja digital yang menerapkan praktik teknik yang kuat dan mengembangkan solusi digital bagi SAF untuk memenuhi kebutuhan operasional yang terus berubah, dan bermitra dengan digital (Choucri & Clark, 2019).

Penggunaan ruang siber yang tidak terbatas oleh batasan wilayah negara telah memungkinkan berbagai pihak untuk melakukan tindakan yang merugikan orang lain, yang dapat dilakukan baik oleh aktor negara maupun aktor bukan negara. Aktor Negara sebagai aktor hubungan internasional yang menjadi subyek interaksi antar Negara-negara yang berdaulat. Merujuk pada sejarah yang ada, Negara-negara di dunia memiliki potensial konflik yang berujungpada perang, misalnya saja Perang Dunia I dan Perang Dunia II (Soeprapto, 1997).

Selain aktor Negara, aktor-aktor non Negara yang mempunyai pengaruh terhadap kehidupan suatu Negara misalnya individu hacker, kelompok hacker, kegiatan para hacker, non-government organization (NGO), terorisme, kelompok kejahatan terorganisir (organized criminal groups) dan sektor swasta (seperti internet companies and carries, security companies) dapat mengancam pertahanan dan kedaulatan Negara. Saat ini di Indonesia, kewenangan dalam melaksanakan tugas dan fungsi keamanan siber diberikan kepada Badan Siber dan Sandi Negara (BSSN).

Kedudukan BSSN hanya diatur melalui Peraturan Presiden, hal ini tentu kurang kuat dibandingkan dengan suatu lembaga/entitas yang dibentuk melalui Undang-Undang. Sebaran berbagai fungsi siber di berbagai lembaga pemerintah menuntut keberadaan suatu lembaga/entitas yang memiliki kemampuan untuk mengkoordinasikan semua fungsi tersebut. Selain itu, dalam konteks konsep baru dalam dunia internasional, ditegaskan bahwa kerja sama antara negara sebagai koordinator dan pengawas, serta pihak lain yang berkontribusi pada keamanan siber infrastruktur mereka, menjadi suatu kebutuhan penting. Pada hal ini, pembentukan matra ke-4 yakni Angkatan Siber dan Digital dalam organisasi TNI demi menjaga kedaulatan NKRI perlu diperhitungkan.

Dalam penulisan ini penulis merumuskan pokok permasalahan berdasarkan dengan apa yang telah diuraikan pada latar belakang di atas, dengan rumusan sebagai berikut: 1) Bagaimana tindakan Indonesia yang tepat untuk memitigasi ancaman akibat adanya transformasi digital yang sedang dan/atau akan datang? 2) Bagaimana kondisi hukum dan faktor penunjang lainnya terkait dunia siber dan digital di Indonesia saat ini?

Metode Penelitian

Penelitian secara ilmiah, dilakukan oleh manusia untuk menyalurkan hasrat ingin tahu yang telah mencapai taraf ilmiah, yang disertai dengan suatu keyakinan bahwa setiap

gejala akan dapat ditelaah dan dicari hubungan sebab akibatnya, atau kecendrungan-kecendrungan yang timbul. Dalam hal ini, penelitian merupakan suatu sarana untuk mengembangkan ilmu pengetahuan, baik dari segi teoritis maupun praktis (Soerjono, 1986). Tujuan adanya metode penelitian ini adalah untuk, memahami tata cara melakukan penelitian dan mampu melakukan penelitian kepustakaan serta menyusun skripsi secara metodologis dan sistematis (Sugiyono, 2017).

Spesifikasi penelitian yang digunakan adalah preskriptif analisis yaitu metode ini diterapkan karena tidak hanya bermaksud mengungkapkan atau menggambarkan data sebagaimana adanya, namun juga untuk menggambarkan bagaimana sebaiknya atau idealnya terhadap pembaharuan hukum yang dilakukan dari hasil penelitian (Ishaq, 2017). Pendekatan penelitian dalam jurnal ini:

Pendekatan undang-undang (*statute approach*) dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkut-paut dengan isu hukum yang sedang ditangani. Pada penelitian ini, pendekatan undang-undang membuka kesempatan bagi penulis untuk mempelajari apakah Penemuan hukum baik itu konkretisasi, kristalisasi atau individualisasi peraturan hukum (das sollen) yang bersifat umum dengan mengingat peristiwa konkret (das sein) telah sejalan (Marzuki, 2013).

Pendekatan Konseptual (*Conceptual Approach*). Pendekatan ini dilakukan karena memang belum atau tidak ada aturan hukum untuk masalah yang dihadapi, pendekatan konseptual ini beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum sehingga melahirkan pengertian hukum dan asas-asas hukum yang relevan dengan permasalahan yang dihadapi (Ibrahim, 2006).

Pendekatan perbandingan (*comparative approach*), yakni pendekatan perbandingan makro (*macro comparative approach*) serta pendekatan perbandingan mikro (*microcomparative approach*). Pendekatan perbandingan makro (*macro comparative approach*) digunakan untuk membandingkan suatu kejadian atau peristiwa hukum yang terjadi diberbagai negara, sedangkan pendekatan perbandingan mikro (*microcomparative approach*) hanya membandingkan dalam suatu negara tertentu dalam periode waktu tertentu (Hartono, 1994).

Analisis data diartikan sebagai proses pengorganisasian dan mengurutkan data ke dalam pola, kategori, dan satuan uraian dasar sehingga dapat ditemukan tema dan dapat dirumuskan hipotesis kerja seperti yang disarankan oleh data. Metode analisa data dalam penelitian ini menggunakan metode analisa data dengan pendekatan Kualitatif (Salim & Nurbani, 2017).

Hasil dan Pembahasan

Setiap negara sejatinya akan melakukan tindakan yang diperlukan untuk melindungi dirinya dari ancaman negara lain atau lingkungannya, hal tersebut dapat dikatakan sebagai kepentingan nasional. Objektifnya, agar tidak terganggunya tujuan negara yang meliputi empat hal, pencarian keamanan nasional (*national security*), martabat atau citra negara (*prestige*), kesejahteraan ekonomi atau kemakmuran (*economic wealth or prosperity*), dan perlindungan danpenyebaran ideologi (*protection and*

promotion of ideology) Spanier (1978). Di Indonesia, adanya nilai-nilai Pancasila dalam pembukaan UUD 1945 menjadikanPancasila memiliki kedudukan tertinggi dalam norma positif di Indonesia (Eleanora, 2012).

Era yang ada sekarang ini mendorong potensi perang antar Negara tidak lagi menggunakan cara perang tradisional dan konvensional. Akibatnya, kekuatan negara tidak lagi dilihat pada kekuatan persenjataan, tetapi juga pada segi budaya, perekonomian, politik, dan teknologi. Bentuk dari peperangan pun berubah yang menimbulkan ancaman baru pada ruang siber (Rahmawati, 2017). Trend ancaman serangan siber akan berkembang terus sesuai perkembangan teknologi informasi, oleh karenanya perlu dilakukan riset secara terus-menerus untuk mampu mengatasi berbagai teknik, taktik dan, strategi pertahanan siber yang akan terus berkembang ke depan (Soewardi, 2013).

Saat ini, kewenangan dalam melaksanakan tugas dan fungsi keamanan siber diberikan kepada Badan Siber dan Sandi Negara (BSSN). BSSN yang sangat berkoordinasi dengan kementerian dan lembaga negara lainnya perihal: 1) Kementerian Komunikasi dan Informatika dalam hal penanganan konten negatif ataupun destruktif pada internet dengan mesin sensor. 2) Unit cyber crimes Mabes Polri dalam hal memburu kejahatan siber (cybercrime). 3) Kementerian Pertahanan divisi *Cyber Operation Center* (COC) dlaam hal pertahanan negara. 4) Kementerian Luar Negeri dalam hal penanganan insiden keamanan siber dan diplomasi siber. 5) Kementerian Perindustrian dan Kementerian Perdagangan dalam hal penanganan fraud e-commerce. 6) Badan Nasional Penanggulangan Terorisme (BNPT) dalam hal penanggulangan terorisme. 7) Badan Intelejen Negara (BIN) dalam hal operasi intelijen pada ruang siber. 8) Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) dan Komisi Pemberantasan Korupsi (KPK) dalam hal kejahatan keuangan dan ekonomi digital.

Sinergi antara pertahanan dan keamanan Negara serta kesejahteraan nasional sangat diharapkan untuk memperkuat ketahanan nasional. Jika sinergi ini berhasil direalisasikan dan dipertahankan, maka aspirasi Negara dan pemerintah untuk menjaga keamanan dan pertahanan Negara sekaligus meningkatkan kesejahteraan masyarakat dengan tujuan mencapai keadilan sosial dapat tercapai.

Kedudukan BSSN hanya diatur melalui Peraturan Presiden, hal ini tentu kurang kuat dibandingkan dengan suatu lembaga/entitas yang dibentuk melalui Undang-Undang yang memiliki kapabilitas untuk menjalankan fungsi penyelenggara pertahanan siber. Penulis berpendapat bahwa Indonesia perlu mengambil tindakan berdasarkan fakta-fakta yang telah dikemukakan di atas, dengan inisiasi konstruksi pembentukan matra ke-4 yakni Angkatan Siber dan Digital dalam organisasi TNI demi menjaga kedaulatan NKRI.

Lebih lanjut, Penulis merumuskan 4 (empat) poin yakni pertama terkait peraturan terkait siber dan digital di Indonesia, kedua terkait infrastruktur digital di Indonesia, ketiga terkait literasi digital di Indonesia, dan keempat terkait sumber daya manusia di Indonesia sebagai kondisi hukum dan faktor penunjang lainnya terkait dunia siber dan digital di Indonesia saat ini, berikut penjelasannya:

Peraturan Terkait Siber dan Digital di Indonesia

Pasal 30 ayat (1) UUD 1945. menyatakan: "tiap-tiap warga negara berhak dan wajib ikut serta dalam usaha pertahanan dan keamanan negara." Maka dari itu keamanan siber merupakan bagian dari pertahanan dan keamanan Negara yang tidak hanya menjadi hak dan kewajiban aparat Negara saja, namun bagi seluruh warga Negara. Saat ini, pengaturan keamanan siber masih belum terorganisir dengan baik dan terdapat dalam beberapa peraturan perundangan-undangan yang bersifat sektoral dan terpecah-pecah.

Materi yang berkaitan dengan pengaturan keamanan siber tersebar di beberapa peraturan perundangan-undangan, yakni: 1) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. 2) Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia. 3) Undang-Undang Nomor 3 Tahun 2002 tentang Pertahan Negara. 4) Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia. 5) Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara. 6) Undang-Undang Nomor 3 Tahun 2014 tentang Perindustrian. 7) Undang-Undang Nomor Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.

Dengan demikian, guna mewujudkan pembentukan matra ke-4 yakni Angkatan Siber dan Digital dalam organisasi TNI maka perlu dilakukan revisi baik dalam bentuk usulan pasal baru dan/atau reviu pada Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia. Angkatan Siber dan Digital yang baru ini perlu mengintegrasikan komponen-komponen pertahanan siber yang sudah ada. Dalam konteks ini, Kementerian Pertahanan dan Badan Siber dan Sandi Negara (BSSN) harus bersedia untuk mengkonsolidasikan unit-unit siber yang dimiliki. Hal ini sangat penting karena tanpa hal tersebut akan menyebabkan terjadi tumpang tindih dalam kewenangan dan tugas antar lembaga.

Angkatan Siber juga harus dipisahkan dari fungsi keamanan. Dengan kata lain, kewenangan Direktorat Tindak Pidana Siber di bawah Reserse Kriminal Polri tidak boleh diotak-atik oleh keberadaan matra baru ini meskipun masih akan diperdebatkan bagaimana jika Angkatan Siber ini diperbantukan ke Polri. Sebab, kita telah telanjur menerima jargon "Sinergitas TNI-Polri" yang merupakan implementasi tugas perbantuan TNI menurut Tap MPR Nomor VI/MPR/2000 Tahun 2000 tentang Pemisahan TNI dan Polri. Pemisahan fungsi pertahanan dan keamanan ini harus tetap diprioritaskan.

Jangan sampai, matra baru ini ikut memperkeruh gesekan antara sipil dan militer. Mengingat, Indonesia belum tegas mengatur penindakan terhadap anggota TNI yang melanggar prinsip-prinsip pidana sipil. Jangan sampai, operasi keamanan yang diembankan kepada Angkatan Siber ini kelak menjadi imun dan mutlak, bahkan mampu merepresi ruang demokrasi masyarakat.

Infrastruktur Digital di Indonesia

Saat ini, belum meratanya infrastruktur digital di Indonesia yang disebabkan oleh kesenjangan digital antara masyarakat perkotaan dan pedesaan. Infrastruktur teknologi informasi, seperti akses telekomunikasi dan internet, saat ini hanya menjangkau wilayah perkotaan. Oleh karena itu, ada beberapa permasalahan yang harus segera diselesaikan,

termasuk distribusi broadband kawasan, percepatan analog untuk dimatikan, serta pemersatu visi infrastruktur digital pembangunan antara pemerintah pusat dan pemerintah daerah. Pemerataan cakupan nasional layanan broadband juga terkendala oleh perizinan, penggalian, dan penempatan jangka panjang dan kabel rumit untuk tujuan penempatan dan pemeliharaan. Pemeliharaan infrastruktur menghadapi tantangannya tantangan tersendiri karena pencurian dan vandalisme masih sering terjadi pada infrastruktur dan jaringan telekomunikasi.

Salah satu faktor penting dalam pembentukan matra ke-4 Angkatan Siber dan Digital dalam organisasi TNI adalah infrastruktur digital yang memadai, Pemerintah harus cepat tanggap dalam mengadopsi dan/atau mengolah:

a. Teknologi terbarukan dan kecerdasan buatan (AI) yang diharapkan dapat mengubah semua sektor masyarakat, termasuk sifat perang. Kegagalan untuk mengadopsi dan mengintegrasikan teknologi AI secara efektif dapat menghambat pertahanan nasional.
b. Pengelolaan Big Data dengan benar, yang menjadi "sumber daya strategis yang mendasar" dan berupaya melindungi aset strategis Indonesia dengan mewajibkan lokalisasi data di dalam negeri.
c. Jaringan seluler 5G yang akan meningkatkan kecepatan transmisi dan mengurangi latensi secara signifikan. Jaringan 5G akan menawarkan kecepatan pengunduhan video yang lebih cepat. Namun, fitur berkapasitas tinggi dan latensi sangat rendah adalah fitur yang lebih penting. Kedua fitur ini akan memungkinkan penerapan kendaraan otonom, otomatisasi pabrik, Internet of Things (IoT), dan banyak lagi. 5G jaringan memiliki tiga bagian jaringan utama dengan fungsi utama yang berbeda.

   Pertama, peningkatan seluler broadband (eMBB), yang memungkinkan kecepatan pengunduhan jauh lebih tinggi untuk ponsel cerdas dan perangkat lainnya; kedua, komunikasi latensi rendah yang sangat andal (uRLLC), dirancang untuk aplikasi seperti kendaraan otonom yang memerlukan celah sesedikit mungkin untuk aplikasi penting seperti penginderaan hambatan jalan dan komando dan kendali; dan ketiga, mesin-ke-mesin secara besar-besaran komunikasi (mMTC) yang dirancang untuk menangani miliaran sensor dan perangkat lain yang berkomunikasi antara mereka sendiri dan bagian lain dari jaringan (Triolo, Allison, & Brown, 2018). Fitur ini sangat penting untuk mengembangkan aplikasi di sekitar jaringan, seperti Internet Of Things (IoT),dan smart cities.
d. Keberdikarian dalam memiliki Satelit yang digunakan untuk sistem pertahanan di NKRI, mengingat Indonesia adalah negara Non-Blok. Pada tahun 2020, Sistem Satelit Navigasi Beidou Tiongkok memiliki 35 satelit yang beroperasi dan bersaing dengan Global Amerika Positioning System (GPS) dan Galileo Eropa. Sistem Beidou dianggap lebih maju dan menawarkan presisi lebih tinggi daripada GPS. Dukungan Amerika Serikat dalam bidang sarana dan prasarana berdasarkan pada geostrategi yang menyangkut keunggulan komperatif Singapura, sebagai hub bagi negara-negara Asia Tenggara turut membantu Singapura dalam akselerasi pendirian DIS.
e. Penerapan potensial komputasi kuantum di bidang militer. Salah satu contoh adalah penginderaan kuantum. Sensor kuantum dapat digunakan untuk mendeteksi kapal

selam dan pesawat siluman. Dia juga dapat digunakan sebagai sistem navigasi inersia yang andal. Perangkat tersebut, yang dikenal sebagai perangkat Posisi, Navigasi, dan Waktu kuantum (PNT), memungkinkan navigasi tanpa memerlukan referensi eksternal seperti GPS.

Literasi Digital di Indonesia

Aksesibilitas infrastruktur digital yang semakin mudah dan murah serta literasi digital yang kuat. Penduduk Indonesia juga telah mempercepat digitalisasi di Indonesia. Meski begitu, literasi digital penduduk Indonesia belum mencapai tingkat "baik". Dalam skala 1 sampai 5, Indonesia digital indeks melek huruf sedikit di atas 3,47 (Katadata 2020). Dari empat sub-indeks yang diperhitungkan membentuk indeks literasi digital yaitu: 1) Literasi Informasi dan Data, 2) Komunikasi dan Kolaborasi, 3) Keamanan, 4) Kapabilitas Teknologi, didapatkan subindeks literasi informasi dan data mempunyai skor paling rendah. Dengan kata lain, kemampuan masyarakat Indonesia masih cukup terbatas mencari, memfilter, dan menyimpan data, serta mengarahkan pencarian data.

Indeks literasi digital Indonesia dianalisis berdasarkan beberapa faktor yang berhubungan dengan responden, karakteristik dan profil. Laki-laki cenderung memiliki indeks literasi digital di atas perempuan. Orang yang lebih muda cenderung memiliki indeks literasi digital di atas kelompok usia tua. Orang yang dengan sosial ekonomi yang lebih tinggi mempunyai indeks literasi digital lebih cenderung memiliki indeks literasi digital di atas rata-rata nasional dibandingkan mereka yang memiliki indeks literasi digital di bawah rata-rata nasional bagi status sosial-ekonomi yang rendah. Mereka yang memiliki tingkat pendidikan lebih tinggi cenderung memiliki literasi digital indeks di atas rata-rata nasional dibandingkan mereka yang berpendidikan rendah. Terakhir, kawasan perkotaan cenderung memiliki indeks literasi digital lebih tinggi dibandingkan wilayah perdesaan.

Sumber Daya Manusia di Indonesia

Transformasi Digital memberikan banyak peluang namun juga menimbulkan risiko-risiko baru bagi pertahanan negara, sehingga memerlukan Upaya penerapan kebijakan yang memadai. Meskipun tingkat penetrasi telepon seluler tinggi, namun kendala cakupan layanan internet yang rendah tingkat keamanannya, rendahnya mitigasi Masyarakat dan Pemerintah dalam melawan informasi yang hoaks dan simulakra, kurangnya infrastruktur, inovasi, dan deregulasi untuk memanfaatkan potensi penuh lingkungan digital di Indonesia.

Kabar baiknya, sebagian besar masyarakat Indonesia siap untuk mengadopsi layanan digital karena banyak masyarakat yang memiliki smartphone dan akses internet. Kemudian, Kementerian PPN/Bappenas dan BPS merilis Proyeksi penduduk 2020-2050. Indonesia harus cermat dalam memanfaatkan bonus demografi, kondisi yang sejatinya menguntungkan bagi Pembangunan karena melimpahnya penduduk di usia produktif.

Periode 2030 hingga 2040 Indonesia diproyeksi berada di puncak bonus demografi, dengan penduduk usia produktif mencapai 180 juta orang, sedangkan jumlah usia tidak produktif hanya sepertiga, yakni 60 juta jiwa. Jika direncanakan dengan baik, optimalisasi bonus demografi dapat berkontribusi pada berlipatnya produk domestic

bruto atau PDB per kapita. Sebaliknya, tanpa perencanaan yang matang, bonus demografi dapat berujung pada tingginya angka pengangguran karena kurangnya lapangan kerja, diiringi dengan meningkatnya jumlah lanjut usia.

Dengan demikian, Generasi muda Indonesia perlu dibekali dengan keterampilan digital yang memadai untuk merespons pesatnya perkembangan teknologi kemajuan teknologi yang mengubah lanskap sistem pertahanan negara. Pemerintah perlu untuk meningkatkan kemampuan beradaptasi tenaga kerja dengan menyediakan tenaga kerja berkualitas tinggi dan fokus secara digital. Selain itu, kolaborasi yang lebih intensif antara pemerintah dengan institusi Pendidikan formal dan nonformal untuk akselerasi pembentukan SDM Keamanan Siber.

Kesimpulan

Dalam era transformasi digital, setiap negara perlu mengadaptasi perubahan sebagai strategi untuk memperkuat pertahanan. Tiongkok dan Amerika Serikat telah meluncurkan inisiatif besar terkait kecerdasan buatan (AI), sedangkan Singapura merespons transformasi digital dengan mendirikan *Digital Intelligence Service* (DIS). Pada tahun 2017, Tiongkok meluncurkan "Rencana Pengembangan Kecerdasan Buatan Generasi Berikutnya" untuk menjadi pemimpin global dalam bidang AI pada tahun 2030. Di AS, Pemerintahan Biden-Harris pada tahun 2023 meluncurkan kompetisi "AI *Cyber Challenge*" (AIxCC) yang dipimpin oleh DARPA, dengan kolaborasi perusahaan AI terkemuka. Sejalan dengan itu, Indonesia perlu mengambil tindakan dengan membentuk matra ke-4 Angkatan Siber dan Digital dalam TNI untuk menjaga kedaulatan NKRI. Empat poin kunci termasuk keselarasan regulasi terkait siber dan digital, pembangunan infrastruktur digital, pembinaan literasi digital, dan strategi penggalangan personil sesuai dengan kondisi sumber daya manusia di Indonesia.

BIBLIOGRAFI

Choucri, Nazli, & Clark, David D. (2019). *International relations in the cyber age: The co-evolution dilemma*. MIT Press.

Eleanora, Fransiska Novita. (2012). Pancasila Sebagai Norma Dasar Dalam Sistem Hukum Indonesia. *ADIL: Jurnal Hukum*, *3*(1), 141–165.

Elisabeth, Duma Megaria. (2019). Kajian terhadap peranan teknologi informasi dalam perkembangan audit komputerisasi (studi kajian teoritis). *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, *3*(1), 40–53.

Hartono, C. F. G. (1994). *Penelitian hukum di Indonesia pada akhir abad ke-20*.

Ibrahim, Johnny. (2006). Teori dan metodologi penelitian hukum normatif. *Malang: Bayumedia Publishing*, *57*, 295.

Ishaq, Ishaq. (2017). *Metode Penelitian Hukum Dan Penulisan Skripsi, Tesis, Serta Disertasi*. Alfabeta.

John, Vivian. (2008). Teori Komunikasi Massa. *Jakarta: Prenada Media Group*.

Lovina, Ronaldy. (2022). Kajian Konektifitas Antar Pulau Di Wilayah Kepulauan Riau. *Jurnal Potensi*, *2*(2).

Marzuki, Peter Mahmud. (2013). Penelitian Hukum, Jakarta: Kencana. *Mertokusumo, Sudikno*.

Rahmawati, Ineu. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense. *Jurnal Pertahanan Dan Bela Negara*, *7*(2), 35–50.

Salim, H. S., & Nurbani, Erlies Septiana. (2017). *Penerapan teori hukum pada penelitian tesis dan disertasi/Salim HS*.

Sanusi, M. Arsyad. (2005). Hukum Teknologi dan Informasi. *Bandung: Tim Kemas Buku*.

Soeprapto, R. (1997). Hubungan Internasional Sistem Interaksi dan Perilaku. *Jakarta: Raja Grafindo Persada*.

Soerjono, Soekanto. (1986). Pengantar penelitian hukum. *Universitas Indonesia, Jakarta*.

Soewardi, Bagus Artiadi. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. *Media Informasi Ditjen Pothan Menhan*, 31–35.

Spanier, John, & Play, Gaines Nations. (1978). *Analyzing International Politics*. New York: Praeger.

Sugiyono. (2017). *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif dan R & D*. Bandung: Alfabeta.

Triolo, Paul, Allison, Kevin, & Brown, Clarise. (2018). Eurasia Group White Paper: The Geopolitics of 5G. *Eurasia Group*, 1811–1814.