Journal of Education, Humaniora and Social Sciences (JEHSS) *ISSN 2622-3740 (Online)*
Vol 5, No. 1, Agustus 2022: 264-274, DOI: 10.34007/jehss.v5i1.1192

Perlunya Tentara Nasional Indonesia Memiliki Angkatan Siber Guna Menghadapi Era *Cyber warfare*

The Need for the Indonesian National Army to Form a Cyber Force to Face Modern Warfare and Cyber Warfare

Krida Eva Setiawan Hasan
Sekolah Staf dan Komando Angkatan Laut, Indonesia

Diterima: 23 Maret 2022; Direview: 23 Maret 2022; Disetujui: 15 Mei 2022
Coresponding email: kridaeva.setyawan@tnial.mil.id

Abstrak

Artikel ini bertujuan untuk mengetahui serta menjelaskan mengenai perlunya Tentara Negara Indonesia (TNI) untuk membentuk angkatan siber, mengingat perkembangan teknologi yang semakin cepat. Masalah dalam artikel ini difokuskan pada ancaman kejahatan siber terutama bagi kedaulatan negara serta penekanan bahwa pada saat ini Indonesia membutuhkan adanya TNI angkatan siber guna melindungi serta memberantas kejahatan siber di Indonesia. Artikel ini menggunakan metode studi literatur dengan mengambil referensi dari berbagai sumber terpercaya dan artikel terkait. Hasil penelitian menunjukkan bahwa saat ini perang siber sudah berada di depan mata, dalam artian setiap negara tentu harus bersiap untuk hal ini. Seperti contohnya spionase yang dilakukan oleh negara lain terhadap Indonesia tentu sangat mengancam keamanan Indonesia. Oleh karena itu diperlukan adanya pembentukan matra keempat yaitu tentara *cyber* atau TNI Angkatan Siber demi terciptanya pertahanan dan keamanan nasional secara maksimal dan merata. Seperti halnya berbagai negara yang sudah memiliki angkatan perang khusus untuk siber, Indonesia juga harus segera merealisasikannya.
Kata Kunci: Perang; Ancaman; Siber; Angkatan Siber

Abstract

This article aims to identify and explain the need for the Indonesian National Armed Forces (TNI) to form a cyber force, given the increasingly rapid development of technology. The problem in this article is focused on the threat of cyber crime, especially for state sovereignty and the emphasis that at this time Indonesia needs the Indonesian National Armed Forces (TNI) for cyber forces to protect and eradicate cyber crime in Indonesia. This article uses the literature study method by taking references from various trusted sources and related articles. The results of the study show that currently cyber war is in sight, in the sense that every country must be prepared for this. For example, espionage carried out by other countries against Indonesia certainly threatens Indonesia's security. Therefore, it is necessary to establish a fourth dimension, namely the cyber army or the Cyber Force TNI for the creation of maximum and equitable national defense and security. As with various countries that already have a special military force for cyber, Indonesia must also immediately realize it.
Keywords*: War; Threat; Cyber; Cyber Army*

How to Cite*:* Hasan, K.E.S., (2022). Perlunya TNI Memiliki TNI Angkatan Siber Guna Menghadapi Era *Cyber warfare. Journal of Education, Humaniora and Social Sciences (JEHSS). 5(1): 264-274.*

PENDAHULUAN

Ketika membicarakan keamanan nasional, saat ini semakin bertambah lagi aspek di dalamnya selaras dengan perkembangan zaman. Dalam satu faktor utama yang menjadi perhatian baru pada sektor keamanan nasional adalah faktor meningkatnya pengetahuan dan teknologi (Hidayati, 2019). Aspek tambahan yang disebabkan karena faktor perkembangan teknologi adalah bagaimana saat ini ancaman pada pertahanan negara tidak hanya sebatas pada ancaman fisik namun juga secara siber. Ancaman siber sendiri hadir karena konteks dari kehidupan manusia masa sekarang yang bergantung pada teknologi terutama internet. Kebergantungan kehidupan manusia dengan teknologi terutama internet membuat sebuah celah baru akan potensi ancaman yang dapat terjadi pada keamanan negara. Celah ini ada karena penggunaan internet saat ini semakin masif dari level individu sampai level negara, semua aktivitasnya sangat bergantung pada penggunaan internet. Hal inilah mengapa keamanan sektor siber menjadi salah satu hal yang harus diperhatikan.

Ketika membicarakan pertahanan nasional, tentu saja kita ketahui pemerintah memiliki lembaga-lembaga pertahanan untuk menjaga keamanan dari potensi-potensi serangan. Salah satu lembaga yang dibentuk pemerintah perihal urusan pertahanan adalah TNI (Tentara Nasional Indonesia). Namun TNI sendiri dibentuk sebagai lembaga pemerintah yang bergerak pada sektor pertahanan yang salam ini berfokus pada potensi serangan-serangan fisik. Secara general, ketika membicarakan keamanan negara sangatlah identik dengan keamanan dari potensi-potensi ancaman secara fisik. Oleh karenanya sektor pertahanan di Indonesia dan lembaga-lembaga khusus untuk mengurusi pertahanan hanya berfokus pada persiapan menghadapi ancaman secara fisik. Dalam hal ini tentu saja dapat dilihat dari secara *skill* atau keterampilan dari Sumber Daya Manusia yang ada di dalamnya hanya difokuskan untuk memiliki kemampuan-kemampuan untuk peperangan/ancaman secara fisik. Dari segi lain seperti sarana dan prasarana dalam bentuk persenjataan yang dimiliki adalah untuk kepentingan serangan secara fisik. Hal ini kemudian perlu diperhatikan secara lebih lagi mengingat sektor ancaman yang saat ini meluas pada sektor siber karena kemajuan teknologi maka konsep pertahanan juga mau tidak mau mengikuti perkembangan teknologi yang ada.

Ketika membicarakan potensi serangan pada sektor siber saat ini kasusnya baik di seluruh dunia maupun di Indonesia sendiri saat ini sudah semakin masif keberadaannya. Serangan siber sendiri sangat beragam jenisnya jika dilihat dari pelaku dan juga tujuannya. Serangan siber bisa saja dilakukan oleh individu atau bahkan dalam level organisasi atau perusahaan bahkan mungkin pada level negara. Sedangkan untuk tujuannya juga sangat beragam dari tujuan yang bersifat remeh seperti rasa penasaran dari individu atau bahkan sampai tujuan yang sangat serius seperti misalkan spionase atau sabotase dalam ruang lingkup yang lebih makro seperti informasi kenegaraan. Ketika membicarakan kasus siber di Indonesia sendiri pada Januari sampai November 2020 terjadi serangan dengan jumlah total 1,3 miliar serangan. Selain itu menurut data yang dihimpun oleh kominfo pada tahun 2021 jumlah serangan siber yang menyerang Indonesia adalah sebanyak 888.711.736 serangan (Liputan6.com, 2021).

Serangan siber secara kuantitas saat ini sudah sangat masif diikuti dengan potensi kerugian yang cukup besar jika tujuan yang juga beragam dari yang tidak berbahaya sampai sangat berbahaya pada sektor pertahanan negara. Serangan siber yang angkanya sudah semakin masif di Indonesia saat ini ketika dilihat dari perspektif makro yakni pertahanan negara, tentu saja serangan siber adalah ancaman yang cukup serius. Penggunaan teknologi terutama internet saat ini sudah merambah pada semua sektor kehidupan manusia, tidak terkecuali pada sektor pemerintahan. Dalam menyelenggarakan aktivitas administrasi negara ataupun segala urusan yang berhubungan dengan informasi-informasi strategis negara tentu saja tidak lepas dari penggunaan internet. Aset-aset dalam bentuk informasi digital adalah salah satu hal yang berpotensi untuk di ambil dan dipersalahgunakan oleh pihak-pihak lain. Oleh karenanya sangat krusial sekali untuk negara memiliki kemampuan dan sistem pencegahan serangan siber dalam usaha pertahanan negara. TNI sebagai lembaga garda depan dan dalam struktur kenegaraan memiliki wewenang dan tugas dalam pertahanan negara, idealnya juga memiliki kemampuan untuk bisa memperluas jangkauan fokus persiapan dalam usaha pertahanan negara pada sektor

siber. Namun sayangnya kondisi pertahanan dan lembaga pertahanan di Indonesia masih tidak berfokus pada pertahanan secara siber. Hal ini berakibat pada ketidaksiapan sistem pertahanan negara pada serangan siber.

Saat ini dalam membicarakan politik negara dan korelasinya dengan pertahanan negara, potensi konflik antar negara tentu saja tidak hanya pada serangan fisik atau perang secara fisik. Dengan cepatnya kemajuan serangan siber, hal ini secara praktis dapat dimanfaatkan oleh negara-negara yang sedang berkonflik untuk melakukan *cyber warfare* atau medan perang secara siber. *Cyber warfare* sendiri memiliki arti perang yang dilakukan pada dunia maya atau *cyber space* dengan menggunakan teknologi canggih dan jaringan nirkabel/wifi (Subagyo, 2015). Melihat potensi konflik dalam *cyber space* atau ruang siber ini menjadi salah satu poin penting dimana strategi pertahanan siber haruslah ada pada sistem pertahanan Indonesia. TNI sendiri merupakan komponen utama dalam sistem pertahanan negara dalam menghadapi ancaman militer (Putra, 2018). TNI sebagai komponen utama dalam sistem pertahanan Indonesia, idealnya harus mengikuti perkambangan pada sektor pertahanan secara siber. Dalam hal ini sangat penting bagi TNI untuk membentuk pasukan khusus untuk menangani urusan pertahanan siber. Dalam hal ini pasukan khusus yang dimaksud adalah kumpulan dari sumberdaya manusia yang secara aktif dibekali oleh set kemampuan untuk menggunakan aset digital dan dapat melindungi negara dari serangan siber dan kemungkinan terjadinya perang siber (*cyber warfare).*

Untuk mendukung tulisan ini, terdapat beberapa penelitian terdahulu yang digunakan sebagai rujukan dalam penelitian. Penelitian-penelitian yang diambil sebagai rujukan adalah penelitian dengan *scope* atau ruang lingkup yang serupa berkaitan dengan *cyber warfare* dan pertahanan negara. Penelitian pertama adalah penelitian dari (Chotimah, 2019) dalam penelitian ini menyoroti tentang peran lembaga negara dalam sektor pertahanan yakni BSSN dalam mengatur tata kelola keamanan siber di Indonesia. Selain itu penelitian ini juga menyoroti pelaksanaan serta diplomasi siber yang ada di Indonesia baik dalam kerjasama negara secara bilateral ataupun secara multilateral. Penelitian yang kedua adalah penelitian dari (Putra, 2018) yang berfokus pada ancaman siber pada pertahanan negara di Indonesia. Dalam tulisn ini juga disinggung peran TNI dan bagaimana kondisi strategi pertahanan siber yang dimiliki oleh TNI saat ini dalam menghadapi *cyber threat.*

Dari permasalahan diatas maka sangatlah penting untuk TNI sebagai komponen utama sistem pertahanan nasional untuk memiliki angkatan siber. Menghadapi tren perkembangan serangan siber yang sangat pesat dan juga potensi konfil politik antar negara yang bisa terjadi pada ruang siber (*cyber space).* Berdasarkan latar belakang serta penelitian-penelitian terhadahulu tersebut maka tulisan ini berusaha untuk menyoroti secara khusus urgensi dari TNI dalam membentuk angkatan siber sebagai usaha menghadapi potensi *cyber warfare.* Tulisan ini diharapkan dapat memberikan gambaran tentang urgensi dari TNI untuk membentuk angkatan siber yang diharapkan dapat menjadi literatur untuk menjadi pertimbangan pada sektor pertahanan terutama pertahanan siber.

METODE PENELITIAN

Pada tulisan ini metode yang digunakan adalah metode kualitatif dengan teknik studi literatur. Metode kualitatif digunakan untuk bisa mendeskripsikan topik penelitian secara lebih eksploratif. Dengan topik *cyber warfare* dan peran TNI dalam angkatan *cyber* ini studi secara kualitatif dapat melakukan eksplorasi lebih dan analisis yang lebih spesifik pada permasalahan peran TNI dalam menghadapi *cyberware.* Pada pengambilan data pada tulisan ini data yang dipakai adalah data sekunder yang diambil dengan menggunakan teknik penelitian studi literatur. Studi literatur sendiri memiliki pengertian sebuah penelitian yang pengumpulan informasinya dan juga masalah penelitian dilakukan dengan mengumpulkan sejumlah buku atau majalah (Danial & Warsiah, 2009).

Skema pengambilan data melalui literatur pada tulisan ini dilakukan dengan mengambil beberapa sumber relevan terkait topik penelitian. Sumber-sumber relevan yang digunakan pada penelitian ini diantaranya adalah sumber-sumber buku, penelitian seperti skripsi, tesis dan

disertasi, selanjutnya sumber artikel ilmiah yang dipublikasi secara online, dan juga dokumen-dokumen dari internet pada lembaga-lembaga terkait yang relevan dengan diskusi mengenai pertahanan negara.

HASIL DAN PEMBAHASAN

Ancaman *Cyber warfare* Bagi Pertahanan Indonesia

Dalam era digital, perkembangan teknologi semakin cepat. Semakin cepatnya perkembangan teknologi maka semakin cepat pula penyebaran informasi dan komunikasi. Perkembangan teknologi ini tidak lepas dari internet sebagai pemeran utamanya. Internet tidak hanya menyumbang sisi positif bagi perkembangan teknologi dan kemudahan bagi seluruh penggunanya, namun juga turut menyumbang sisi negatif. Kemunculan dan perkembangan internet mengundang juga munculnya jenis kejahatan baru. Salah satunya mengganggu dimensi keamanan nasional hingga internasional yaitu perang siber atau *cyber warfare* dimana fenomena baru ini telah dianggap sebagai ancaman jenis baru pada zaman ini (Babys, 2021). *Cyber warfare* didefinisikan sebagai salah satu jenis perang yang dilakukan dilingkungan *cyber*space dan penyerangannya berbeda dengan perang konvensional yang lain (Tampubolon, 2019). Selain itu *cyber warfare* juga dimaknai dengan aktivitas perang yang dilakukan dengan menggunakan peralatan elektronik dan komputer dengan tujuan merusak dan mengganggu peralatan elektronik dan jalur komunikasi target lawan (Saputera, 2015). Menurut Permenhan No.82 Tahun 2014 *cyber warfare* diartikan sebagai segala tindakan yang secara sengaja dilakukan dan bergerak secara teratur dan terkoordinasi yang bertujuan untuk menganggu kedaulatan sebuah negara (Kementerian Pertahanan Republik Indonesia, 2014).

Terdapat beberapa kriteria khusus *cyber warfare* menurut Thomas Rid (dalam Candra et al., 2021) yaitu harus berpotensi mematikan, harus instrumental dan harus bersifat politis. Namun, menurut Libicki *cyber warfare* dianggap sebagai serangan yang dilakukan dengan sengaja yang menargetkan jaringan lawan dengan tujuan menonaktifkan (Candra et al., 2021). *Cyber warfare* dapat dibedakan menjadi 2 yaitu *cyber warfare* strategis dan operasional, dikatakan strategis apabila serangannya berasal dari suatu kelompok tertentu yang menyasar suatu negara beserta rakyatnya tidak secara eksklusif namun bertujuan untuk mempengaruhi perilaku, sedangkan operasional dilakukan melalui jaringan internet maupun komputer sasaran untuk membantu operasi militer (Candra dkk, 2021). Banyak negara-negara di dunia menjadikan ancaman *cyber warfare* merupakan ancaman strategis dengan level bahaya yang cukup tinggi untuk keamanan, pertahanan dan kepentingan nasional negara (Setiyawan, 2018).

Penyerangan dalam bentuk aktivitas *cyber* merupakan bentuk kejahatan yang berada dalam wilayah keamanan nasional (kewenangan penegak hukum) menurut hukum Indonesia (Pratama, 2021). *Cyber warfare* di Indonesia sendiri disebut perang sibernetika (Pratama, 2021). *Cyber warfare* dilakukan dengan tujuan untuk masuk tanpa akses kemudian melakukan pengendalian, modifikasi, pencurian, menghancurkan hingga melumpuhkan sistem informasi atau aset negara (Pratama, 2021). Ancaman *cyber warfare* di negara Indonesia tentunya sangat berbahaya bagi keamanan data nasional. Menurut Permenhan No.28 Tahun 2014 *cyber warfare* sendiri dapat berupa serangan terorisme (*cyber terrorism*) hingga spionase (*cyber espionage*) yang memiliki dampak yang sangat berbahaya dan menganggu keamanan nasional, pada dasarnya karateristik dari *cyber warfare* ini adalah sebagai berikut: disengaja (*intentional*), kegiatan aktif, serta berskala besar (Kementerian Pertahanan Republik Indonesia, 2014).

Salah satu ancaman *cyber warfare* yang pernah dialami oleh negara Indonesia adalah kasus penyadapan kepala negara ke-6 yaitu Susilo Bambang Yudhoyono, beserta ibu negara dan jajarannya oleh negara Australia dan Selandia baru (Subagyo, 2015). Tidak hanya itu Indonesia sendiri juga pernah melakukan aktivitas *cyber warfare* dengan negara Portugal pada tahun 1999 hingga menyebabkan penghapusan semua data, sedangkan pada tahun 2010 Indonesia terdaftar di urutan ke-2 dari 10 negara sebagai negara yang mengalami serangan *worm stunxnet* (Soewardi, 2013). Serta pada tahun 2014, Indonesia dan Malaysia juga terlibat dalam aktivitas *cyber warfare* dimana Malaysia telah menyerang siber pertahanan basis militer yang penting bagi Indonesia

(Schell, 2014). Dilansir dari laman antaranews.com (10 Juni 2020) pada tahun 2017 lalu telah terdeteksi sebanyak 2015.502.219 kali penyerangan siber dilakukan ke pertahanan digital negara Indonesia yang dilakukan dengan serangan hoaks, peretasan website KPU, peretasan website resmi pemerintah dan BUMN dan serangan ransomware yang diikuti dengan permintaan tebusan kepada masyarakat Indonesia. Menurut data dari Badan Siber dan Sandi Negara atau BSSN (dalam Candra et al., 2021) menyatakan bahwa telah terjadi 290,3 juta aktivitas penyerangan *cyber* dimana Indonesia adalah targetnya pada tahun 2019 serta terjadi peningkatan yang signifikan pada tahun 2020 sebesar 495,3 juta serangan yang teridentifikasi. Peningkatan serangan *cyber* di Indonesia juga terjadi pada masa pandemi, hal ini tentu saja menempatkan negara Indonesia menjadi negara yang sering dijadikan sebagai sasaran serangan *cyber* (Candra, 2021).

Dari fenomena dan peristiwa penyerangan hingga berada pada tingkat perang *cyber* yang telah menyerang negara Indonesia, maka terdapat 3 jenis ancaman perang *cyber* yang dapat terjadi yaitu sabotase, spionase dan subversi (Rid, 2012). Ketiga jenis perang *cyber* ini banyak dilakukan oleh negara-negara di dunia saat menyerang negara sasaran. Subversi dilakukan dengan cara propaganda melalui penyebaran pamflet, sastra, link atau tautan dan film dengan tujuan untuk melemahkan suatu kekuasaan, integritas dan sebuah konstitusi. Sedangkan spionase dilakukan dengan peretasan jaringan dan sistem teknologi perangkat lunak dengan tujuan mengakses secara sembunyi sistem target kemudian mengeksploitasi informasi rahasia maupun informasi yang dilindungi pihak sasaran. Kemudian sabotase dilakukan dengan menyusupkan suatu virus atau *logic* yang terhubung dengan jaringan internet (Fitiani & Pakpahan, 2020) kepada negara sasaran dengan berbagai macam cara yang bertujuan untuk menghancurkan serta melemahkan suatu sistem militer atau ekonomi suatu negara. Perang *cyber* dengan jenis spionase pernah dialami oleh negara Indonesia dimana waktu itu Negara Australia yang melakukannya dengan menargetkan Presiden Indonesia ke-6 beserta ibu negara dan beberapa petinggi penting pada tahun 2013. Sedangkan *cyber* sabotase juga pernah terjadi di Indonesia saat pemilihan umum tahun 2009 dimana jaringan internet pada pusat tabulasi nasional KPU mengalami gangguan dan dinyatakan bahwa terdapat 20 kali serangan saat penghitungan dimulai. Serta subversi di Indonesia dilakukan dengan ujaran-ujaran kebencian yang berhubungan dengan ideologi serta pemerintahan negara Indonesia yang dilakukan di media sosial.

Atas dasar ketiga jenis perang *cyber* yang pernah dialami oleh Indonesia menjadikan alasan yang kuat bahwa ancaman perang *cyber* atau warfare dapat terjadi dan menyerang Indonesia kembali. Dilansir dari laman databoks.katadata.co.id (14 Oktober 2021) hal ini juga ditambah dengan jumlah pengguna internet di Indonesia yang mencapai 212,35 juta per Maret 2021 dan Indonesia berada pada urutan ketiga di Asia sebagai pengguna internet terbanyak. Dilansir dari laman katadata.co.id (2 Oktober 2020) menyatakan bahwa Indonesia merupakan salah satu negara yang menempati urutan tertinggi sebagai negara yang ditargetkan sebagai sebagai target penyerangan *cyber* dengan menggunakan malware pada tahun 2019 se Asia Pasifik. Maka dari itu banyak jenis dari *cyber*crime yang kerap ditemui dan menyerang Indonesia salah satunya yaitu *cyber warfare*.

Dilain sisi, pandemi juga mengakibatkan kemungkinan ancaman *cyber warfare* menjadi meningkat. Hal ini dikarenakan penggunaan internet di Indonesia semakin bertambah dan aktivitas sehari-hari seperti bekerja bahkan sekolah dilakukan menggunakan jaringan internet. Menurut Badan Siber dan Sandi Negara (dalam Yanuar, 2021) menyatakan bahwa saat pandemi covid-19 terjadi antara Januari hingga April 2020 terjadi 88.414.296 penyerangan *cyber* di Negara Indonesia, dimana di bulan Januari sejumlah 25.224.811 penyerangan *cyber* terdeteksi, bulan Februari sebanyak 29.188.645 serangan terdeteksi, bulan Maret terdeteksi 26.423.989 serangan *cyber* dan mengalami puncak pada tanggal 12 Maret dengan jumlah 3.344.470 serangan, serta pada tanggal 12 April terdeteksi 7.576.851 serangan. Tidak hanya itu dilansir dari laman kompas.tv (29 Juni 2021) menyatakan bahwa pada bulan Januari hingga Mei 2021 telah terdeteksi 448.491.256 aktivitas serangan siber.

Serangan *cyber* yang terjadi di Indonesia saat pandemi menggunakan beberapa jenis software antara lain trojan, malware, spyware, malicious zoom hingga tracker (BSSN, 2020).

Anomali ini juga didukung oleh pernyataan Kepala BSSN Letjen TNI (Purn) Hinsa Siburian yang dilansir dari laman kompas.tv (29 Juni 2021) yang menyatakan bahwa kategori penyerangan siber terbanyak yaitu menggunakan *malware, trojan activity, information leak*. Tidak hanya itu, penyerangan ini juga dilakukan melalui web defacement serta email phising Peristiwa ini tentu saja mengganggu aktivitas elektronik masyarakat Indonesia pasalnya penyerangan ini menggunakan virus yang ditanam di komputer ataupun alat elektronik lain, selain itu terdapat aktivitas pencurian sebuah data baik pribadi atau personal hingga pencurian file rahasia negara atau HKI sebuah perusahaan. Sehingga serangan *cyber* dapat dikategorikan sebagai serangan yang cukup sulit untuk ditaklukan, sebab aktivitas ini dilakukan secara sembunyi dan memanfaatkan teknologi canggih dengan sangat baik.

Tingginya pengguna internet dan maraknya serangan *cyber* yang ditujukan kepada negara Indonesia, memposisikan negara Indonesia berada pada status waspada. Pasalnya serangan siber tidak akan berhenti dan melemah begitu saja. Bahkan dilansir dari laman kompas.tv (29 Juni 2021) saat ini Indonesia tengah memasuki era *cyber warfare*. Dilain sisi setelah banyak ditemukannya dan diadukannya serangan *cyber* pada ruang lingkup perbankan di Negara Indonesia, hal ini juga mengantar Indonesia pada situasi darurat *cyber*. Dilansir dari laman kontan.co.id (10 November 2021) menginformasikan bahwa Kementerian Komunikasi dan Informasi telah mengantongi sebanyak hampir 200.000 aduan mengenai serangan siber pada ruang lingkup perbankan dimana penyerangan ini menggunakan media aplikasi Whatsapp serta Instagram. Dari penjelasan dan faktor yang menempatkan Negara Indonesia berada pada darurat *cyber* dan *cyber warfare*, maka dari itu dibutuhkan SDM yang professional atau ahli, memiliki pengetahuan, keterampilan yang baik dalam dunia *cyber* serta regulasi negara yang kuat dan tegas untuk mengatasi dan mengantisipasi serangan *cyber* dan *cyber warfare* yang ditujukan kepada Negara Indonesia.

Penguasaan teknologi menjadi salah satu kualifikasi yang harus dimiliki oleh Negara Indonesia saat ini. Sehingga perlu adanya kesiapan baik secara ketrampilan maupun fasilitas atau infrastruktur khusus untuk teknologi dengan tujuan untuk menjaga, menstabilkan dan mengamankan negara Indonesia dari serangan siber yang semakin massif dan berbagai macam jenis. Disisi lain, perkembangan Negara Indonesia juga akan sejajar dengan cepatnya perkembangan teknologi yang ada. Maka dari itu, apabila penguasaan teknologi melemah serta regulasi yang kurang ketat mengenai pertahanan *cyber* dapat menempatkan Negara Indonesia dalam posisi yang berbahaya (Nainggolan, 2015). Dilansir dari laman viva.com (14 Februari 2022) Tentara Nasional Indonesia (TNI) telah menyadari bahwa *cyber warfare* merupakan ancaman yang berbahaya bagi militer tanah air, sehingga TNI dituntut untuk melakukan improvement dengan gerak cepat dengan melatih dan menyiapkan para prajurit untuk menghadapi fenomena ini.

Pentingnya Tentara Nasional Indonesia Memiliki Angkatan *Cyber*

Ramainya isu mengenai perang *cyber* dalam hampir satu dekade ini menimbulkan berbagai kekhawatiran bagi berbagai negara. Soewardi (2013) menjelaskan bahwa perang *cyber* dapat menimbulkan keresahan dalam masyarakat apabila eskalasinya meluas dengan cepat karena berpotensi mencuri informasi rahasia negara yang tentunya berisi informasi mengenai keseluruhan warga negara. Apalagi di era perkembangan teknologi ini, keseluruhan aktivitas manusia memiliki ketergantungan terhadap internet, baik dalam aspek sosial, ekonomi, pertahanan, dan lain sebagainya. Oleh karena itu diperlukan pencegahan secara maksimal dari bidang pertahanan Indonesia untuk menghadapi serangan-serangan yang berpotensi menimbulkan perang *cyber* ini. Salah satu upaya yang dapat dilakukan adalah dengan membentuk TNI Angkatan *Cyber*. Saat ini TNI telah memiliki unit-unit kecil dalam penanganan ancaman siber seperti organisasi Satuan Siber TNI, Pussansiad TNI AD, Labpamsisjar TNI AL, dan Satsiber TNI AU. Namun organisasi-organisasi tersebut masih bersifat sektoral dan internal serta dinilai masih belum optimal untuk mendukung pertahanan dan keamanan negara.

Unit khusus untuk pasukan siber sudah dibentuk di berbagai negara utamanya dalam bidang pertahanan dan keamanan karena perang siber bukanlah ancaman yang dapat disepelekan. Oleh karena itu, tidak menutup kemungkinan bahwa perang siber dapat menimbulkan perang secara

militer. Al Jazeera (2021, dalam Soewardi, 2013) menyebutkan bahwa perang siber telah menjadi garis pertempuran yang paling depan dalam bidang pertahanan sehingga dapat disebut sebagai matra perang kelima. Seperti contohnya, saat ini Amerika Serikat telah memiliki unit khusus angkatan siber yang diberi nama *United States Cyber Command* (US*CYBER*COM) yang berdiri di bawah kendali *United States Strategic Command* (US STRATCOM) yang telah berjalan selama kurang lebih 8 tahun, berdiri pada tahun 2009 (Soewardi, 2013). Kementerian Pertahanan Amerika Serikat bahkan telah mendeklarasikan bahwa serangan *cyber* ini telah menjadi matra tempur baru yang sejajar dengan darat, udara, dan laut di tahun 2011.

Negara lain yang diketahui memiliki unit khusus angkatan *cyber* adalah Israel. Unit khusus dari Israel diberi nama Unit 8200 dengan spesialis *cyber warfare*. Unit ini berdiri di bawah naungan Israel *Defense Forces* (IDF) yang telah berhasil menghentikan operasi radar senjata anti pesawat udara Suriah. Namun unit ini diduga merupakan aktor dari serangan *worm stuxnet* yang menyerang sistem komputer dari fasilitas nuklir milik Iran pada awal tahun 2011. Selain itu, Australia juga diketahui telah memiliki pasukan khusus dalam keamanan *cyber* yang bernama *Cyber Security Operations Centre* (CSOC) dimana pasukan ini memiliki tanggung jawab dalam keamanan *cyber*, meliputi mencegah, mendeteksi, serta menangkal segala ancaman maupun serangan *cyber*. Selain itu, China dan Inggris juga diketahui telah memiliki pasukan khusus untuk *cyber*. "Blue Army" merupakan pasukan khusus dari China yang berpusat di Guangzhou, sedangkan *Cyber Security Operations Centre* (CSOC) merupakan sistem pertahanan *cyber* yang dimiliki oleh Inggris dan berpusat di Cheltenham. (Soewardi, 2013).

Banyaknya negara yang telah *aware* terhadap keseriusan dalam *cyber warfare* ini juga harus dapat mendorong pemerintah utamanya kementerian pertahanan Indonesia untuk segera membentuk TNI Angkatan *Cyber*, seperti halnya TNI Angkatan Udara, TNI Angkatan Laut, dan TNI Angkatan Darat dengan keseluruhan tugasnya adalah bertanggung jawab dalam keamanan dan pertahanan negara. Sa'diyah & Vinata (2016) menjelaskan bahwa saat ini kebijakan mengenai pembangunan kekuatan telah ditetapkan oleh Kementerian Pertahanan Indonesia terhadap keseluruhan TNI. Hal ini tentu menjadi kabar baik bagi sistem pertahanan Indonesia yang lebih bersiap mengenai perubahan zaman yang sangat cepat ini. Di sisi lain, pertahanan Indonesia bagian *cyber* tentu masih memerlukan penanganan yang lebih serius. Mengingat berbagai negara sudah memberikan tanggapan serius mengenai perang siber ini, maka tidak menutup kemungkinan apabila Indonesia belum memiliki unit khusus untuk menangani siber maka Indonesia-lah yang akan menjadi sasaran empuk para penjahat siber dalam kancah internasional. Bahkan Ardiyanti (2014) menjelaskan bahwa Indonesia merupakan negara nomor satu dengan tingkat kerentanan tertinggi dalam ancaman kejahatan siber, utamanya *hacking*. Hal ini tentu berdasarkan temuan bahwa kejahatan siber di Indonesia telah meningkat dua kali lipat seiring dengan meningkatnya pengguna smartphone dan media sosial di Indonesia.

Dilansir oleh theconversation.com (2021) TNI semakin banyak merekrut tenaga ahli siber untuk masuk ke dalam tiga matra yakni TNI AL, TNI AU, dan TNI AD. Namun salah satu kelemahan pertahanan Indonesia saat ini adalah penempatan keamanan siber di posisi kedua karena budaya strategis Indonesia mengedepankan pertahanan fisik, khususnya darat sebagai ancaman terdepan dalam bidang pertahanan dan keamanan negara. Nasional.tempo.co (2021) melansir Komandan Pussansiad Brigjen TNI Iroth Sonny Edhie menyatakan bahwa kebutuhan bagi keamanan siber yang dimiliki oleh kementerian pertahanan Indonesia masih belum memadai sehingga diperlukan penambahan personil. Oleh karena itu TNI AD merencanakan adanya Kompetisi Komunitas Siber (KKS) di setiap tahunnya yang bertujuan untuk memberikan kesempatan bagi warga sipil berkontribusi bagi pertahanan negara terutama dalam bidang IT, dan juga warga sipil yang memiliki kemampuan bidang IT dapat menunjukkan dan mengembangkan kemampuannya di tempat yang sesuai. Di sisi lain, seiring berjalannya waktu teknologi tentu mengalami perkembangan yang sangat pesat dan tidak menutup kemungkinan bahwa keamanan siber haruslah ditempatkan di posisi yang sejajar dengan keamanan dan pertahanan lainnya.

Permana, et al., (2022) menjelaskan bahwa kondisi TNI saat ini berdasarkan rencana makro dan berkelanjutan, anggota TNI memiliki keterampilan dan pengetahuan yang masih kurang

dalam pelaksanaannya. Namun hal ini juga disebabkan kurangnya anggaran yang berakibat kurang idealnya pertahanan dan keamanan Indonesia. Kementerian Pertahanan Indonesia menggunakan konsep *Minimum Essential Forces* (MEF) dalam membangun angkatan pertahanan, dimana konsep ini ditujukan untuk membangun kekuatan pertahanan dengan tidak mengesampingkan kemungkinan ancaman-ancaman yang berpeluang menerobos pertahanan Indonesia serta mempertimbangkan perkembangan lingkungan strategis. Permana, et al., (2022) juga menambahkan bahwa dalam membangun pertahanan ini, TNI harus menyesuaikan dengan perkembangan perang saat ini dan masa depan. Tidak menutup kemungkinan bahwa perang konvensional akan semakin ditinggalkan dan diganti menjadi perang siber dimana tentu akan semakin mengancam pertahanan suatu negara.

Konsep *Minimum Essential Force* (MEF) digunakan sebagai standar keamanan yang diterapkan oleh TNI, sesuai dengan kebijakan Kementerian Pertahanan. Hal ini ditujukan untuk membangun kekuatan militer dan terlaksananya tugas TNI yang efektif dalam menghadapi berbagai ancaman pertahanan (Rahman, et al., 2015). Dibentuknya MEF sebenarnya ditujukan untuk mengatasi berbagai kendala yang ada dalam pertahanan Indonesia dengan anggaran yang cukup terbatas, sehingga hal ini dilakukan secara bertahap yakni dari tahun 2010 sampai tahun 2024. MEF dalam hal ini terfokus untuk memenuhi kekuatan yang ada pada tiga matra TNI saat ini, dalam artian dengan adanya MEF maka dapat memenuhi peralatan perang secara konvensional. Oleh karena itu, tentu dibutuhkan pemenuhan senjata *cyber* secara maksimal dalam menghadapi ancaman perang *cyber* ini.

Serangan siber tentunya akan semakin berbahaya seiring berjalannya waktu, mengingat berbagai kasus *cyber crime* telah terjadi di berbagai negara. Subagyo (2015) berpendapat bahwa memang sudah saatnya Indonesia membentuk tentara *cyber* yang berfungsi menjaga pertahanan dan keamanan di bidang yang berfungsi menjaga pertahanan dan keamanan di bidang *cyber*. Oleh karena itu Kementerian Pertahanan harus segera melakukan koordinasi lebih lanjut dengan Mabes TNI untuk segera membentuk tentara *cyber* ini, sehingga hal ini tidak hanya menjadi wacana namun juga dapat segera direalisasikan. Subagyo (2015) juga menambahkan bahwa kualifikasi tentara kualifikasi tentara *cyber* haruslah mumpuni dan berkompeten dalam operasional komputer, internet, media sosial, penyadapan, serta perangkat lunak dan perangkat keras lainnya. Selain itu, tentara *cyber* juga harus memiliki kemampuan untuk melakukan serangan balik apabila mendapatkan serangan juga harus memiliki kemampuan untuk melakukan serangan balik apabila mendapatkan serangan *cyber* dari negara lain. Secara umum tentara *cyber* memiliki tugas dan tanggung jawab yang sama dengan tentara-tentara lainnya sesuai dengan bagian masing-masing.

Kementerian Pertahanan merupakan instansi yang memiliki wewenang penuh dalam pembentukan tentara *cyber*. Berbagai cara dapat dilakukan dalam merekrut tentara *cyber* seperti perekrutan TNI pada umumnya, ataupun mendata keseluruhan anggota TNI saat ini yang memiliki kemampuan serta keahlian lebih di bidang IT untuk dipindah tugaskan menjadi tentara *cyber* yang tentunya akan diberikan pelatihan khusus mengenai *cyber* maupun *cyber force* (Sa'diyah & Vinata, 2016). Oleh karena itu, sebelum dilakukan pembentukan tentara *cyber* memang perlu persiapan secara matang serta sistematis, seperti tersedianya anggaran, perangkat lunak, perangkat keras, sarana prasarana, serta regulasi yang terperinci dan lengkap. Sama halnya seperti matra lainnya, tentara *cyber* juga harus ditempatkan secara merata di berbagai wilayah dengan pusat komandonya tetap berada di Kementerian Pertahanan. Hal ini ditujukan supaya setiap wilayah dapat dipantau dan dilindungi secara maksimal oleh tentara *cyber*.

Saat ini, diketahui Indonesia membentuk Satuan Siber TNI yang memiliki tugas pokok berupa perlindungan terhadap infrastruktur siber milik TNI (Hidayati, 2019). Namun karena masih baru dibentuk, satsiber TNI ini masih berada dalam tahap penjagaan keamanan siber, belum sampai di tahap mampu melakukan serangan balik. Kementerian Pertahanan tentu telah memiliki rencana jangka panjang untuk mengembangkan pertahanan siber, salah satunya adalah pengembangan senjata siber. Tentunya hal ini memberikan kabar baik bagi dunia pertahanan Indonesia mengingat berbagai ancaman siber yang tiada henti saat ini. Oleh karena itu

pengembangan senjata siber juga harus diiringi dengan pengembangan SDM yang mumpuni dan berkompeten di bidang siber. Kedepannya, Kementerian Pertahanan tentu diharuskan semakin meningkatkan kualitas SDM terutama dalam bidang siber demi terciptanya keamanan dan pertahanan negara secara maksimal untuk menghadapi ancaman baik isu tradisional maupun isu non-tradisional.

SIMPULAN

Semakin canggihnya teknologi informasi dan komunikasi yang membutuhkan Internet sebagai kebutuhan utama, menjadikan segala kebutuhan terpenuhi dengan mudah serta mengakibatkan berubahnya pola kehidupan masyarakat. Namun tidak hanya itu, massifnya penggunaan internet juga menciptakan jenis kejahatan baru atau biasa dikenal dengan kejahatan *cyber*. Indonesia sendiri menempati posisi tertinggi sebagai negara yang mengalami serangan *cyber* terbanyak. Tidak hanya serangan *cyber* yang dialami oleh negara Indonesia namun telah mencapai level *cyber warfare*. *Cyber warfare* pernah dialami Indonesia dengan bentuk aksi spionase yang dilakukan oleh Negara Australia, sabotase yang dilakukan kepada KPU, penyerangan siber basis militer yang dilakukan oleh Negara Malaysia, serta aksi subversif yang meliputi ujaran kebencian dan teror. Selain *cyber warfare* masih banyak lagi serangan siber yang ditujukan kepada Negara Indonesia hingga saat ini. Sehingga menyebabkan ancaman *cyber warfare* masih menjadi momok bagi Negara Indonesia, ditambah lagi penguasaan dan sarana parasana terkait teknologi yang kurang maksimal menjadi masalah tersendiri dalam bidang Pertahanan Indonesia pada dunia *cyber*. Maka dari itu saat ini Indonesia berada pada situasi darurat *cyber* dan *cyber warfare*.

Ketika melihat tren pertahanan negara dalam sektor siber di dunia ternyata terdapat cukup banyak negara-negara yang sudah sangat *aware* dengan pentingnya keamanan siber negaranya. Hal ini dapat dilihat dari banyak negara yang bahkan telah memiliki unit khusus pada sistem pertahananya yang berfokus pada sektor siber seperti di negara israel. Namun sayangnya di Indonesia sendiri khususnya pada lembaga TNI menggunakan konsep MEF *Minimum Essential Forces* yang memiliki artian bahwa pemenuhan kebutuhan pertahanan masih berfokus pada pemenuhan secara konvensional. Ha ini menimbulkan peluang untuk perluasan pada kebutuhan pertahanan sektor siber sangat perlu untuk diperhatikan lebih lagi. Pada pelaksanaanya secara praktis TNI saat ini telah memiliki angkatan siber yang baru saja dibentuk. Satuan Siber TNI saat ini diketahui tugas pokok berupa perlindungan terhadap infrastruktur siber milik TNI. Namun dalam pelaksanaanya masih sangat perlu untuk banyak pembenahan baik secara Sumber Daya Manusia dan juga sarana serta prasana yang memadai mengingat pentingnya sektor siber dalam konsep pertahanan negara.

DAFTAR PUSTAKA

Amirullah. (2021). TNI AD Ingin Lebih Banyak Rekrut Ahli Siber Jadi Prajurit. Diunduh di https://www.nasional.tempo.co/tanggal 22 Maret 2022

Antara. (2020). "Pengamat: Waspada ancaman perang siber 2021. Diunduh di https://www.antaranews.com/berita/1544072/pengamat-waspada-ancaman-perang-siber-2021/ tanggal 21 Maret 2022

Ardiyanti, H. (2014). *Cyber*-Security dan Tantangan Pengembangannya di Indonesia. *Jurnal Politica*. 5 (1). 95-110

Babys, S.A.M. (2015). Ancaman Perang Siber Di Era Digital Dan Solusi Keamanan Nasional Indonesia. *Jurnal Oratio Directa* 3(1): 425-442

Badan Siber dan Sandi Negara (2020). Rekap Serangan Siber (Januari – April 2020). Diunduh di https://bssn.go.id/rekap-serangan-siber-januari-april-2020/ tanggal 21 Maret 2022

Candra, Ahmad dkk. (2021). Indonesia Menghadapi Ancaman *Cyber warfare*: Analisis Strategi. *Jurnal Pertahanan*. 7(3): 441-451

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [*Cyber* Security Governance and Indonesian *Cyber* Diplomacy by National *Cyber* and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 10(2), 113-128.

Danial dan Wasriah. (2009). *Metode Penulisan Karya Ilmiah*. Bandung: Laboratorium Pendidikan Kewarganegaraan UPI.

Databoks. (2021). Pengguna Internet Indonesia Peringkat ke-3 Terbanyak di Asia. Diunduh di https://databoks.katadata.co.id/datapublish/2021/10/14/pengguna-internet-indonesia-peringkat-ke-3-terbanyak-di-asia/ tanggal 21 Maret 2022

Fitriani, Yuni&Pakpahan, Roida. 2020. Analisa Penyalahgunaan Media Sosial untuk Penyebaran *Cyber*crime di Dunia Maya atau *Cyber*space. *Cakrawala-Jurnal Humaniora*, 20(1): 21-27

Kata Data. (2020). Microsoft: Serangan Malware di Indonesia Tertinggi di Asia Pasifik. Diunduh di https://katadata.co.id/desysetyowati/digital/5f76e3df376e1/microsoft-serangan-malware-di-indonesia-tertinggi-di-asia-pasifik/ tanggal 21 Maret 2022

Kementerian Pertahanan Republik Indonesia. (2014). Pedoman Pertahanan Siber. Diunduh di https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf/ tanggal 21 Maret 2022

Kompas tv. (2021). Kepala BSSN: Indonesia Memasuki Era Perang Siber. Diunduh di https://www.kompas.tv/article/188013/kepala-bssn-indonesia-memasuki-era-perang-siber/ tanggal 22 Maret 2022

Kontan. (2021). "Indonesia sudah dalam situasi darurat kejahatan siber". Di unduh di https://newssetup.kontan.co.id/news/indonesia-sudah-dalam-situasi-darurat-kejahatan-siber?page=all/ tanggal 22 Maret 2022

Liputan6.com. (2021) Indonesia Diberondong 13 Miliar Serangan Siber Sepanjang 2021. Diunduh https://www.liputan6.com/bisnis/read/4706493/indonesia-diberondong-13-miliar-serangan-siber-sepanjang 2021#:~:text=Indonesia%20Diberondong%201%2C3%20Miliar%20Serangan%20Siber%20Sepanjang%202021.-Liputan6.com&text=Liputan6.com%2C%20Jakarta%20%2D%20Jumlah,2021%20mencapai%201%2C3%20miliar/ tanggal 21 April 2022

Nainggolan, D. R. M. (2015). National Defense System from the Perspective of *Cyber warfare*. *Information Science*, *30*, 192-204

Permana, Iman, dkk. (2022). Indonesian National Army: A Human Capital Strategy to Modernized National Army Power. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*. 5 (1): 2615-3076.

Pratama, B., & Bamatraf, M. (2021, April). Tallinn manual: *Cyber warfare* in Indonesian regulation. *In IOP Conference Series: Earth and Environmental Science.* 729(1): 012033

Putra, R. D., Supartono, S., & Deni, D. A. R. (2018). Ancaman Siber Dalam Persfektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta). *Peperangan Asimetris*, *4*(2)

Rahman, Alex Firmansyah, et al. (2015), Analisis Minimum Essential Force (MEF) dalam Rangka Pembangunan *Cyber*-Defense. *Jurnal Pertahanan*. 5 (5): 63-85.

Sa'diyah, Nur Khalimatus & Ria Tri Vinata. (2016). Rekonstruksi Pembentukan *National Cyber Defense* sebagai Upaya Mempertahankan Kedaulatan Negara. *Jurnal Perspektif*. 21 (3): 168-187.

Saputera, Moehammad Yuliansyah. (2015). Pengaruh *Cyber* Security Strategy Amerika Serikat Menghadapi Ancaman *Cyber warfare*. Jom Fisip Volume 2(2):1-14

Schell, Bernadette H. (2014). Sensor Internet: Buku Pegangan Referensi. ABC-CLIO

Setiyawan, Anang. (2018). Penguatan Kebijakan Dan Kelembagaan National *Cyber* Defense Dalam Menghadapi Ancaman *Cyber*warfare Di Indonesia. Thesis. Universitas Sebelas Maret. (Https://Digilib.Uns.Ac.Id/Dokumen/Detail/64295/Penguatan-Kebijakan-Dan-Kelembagaan-National-*Cyber*-Defense-Dalam-Menghadapi-Ancaman-*Cyber*warfare-Di-Indonesia)

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

Soewardi, Bagus Artiadi. 2013. Perlunya Pembangunan Sistem Pertahanan Siber (*Cyber* Defense) yang tangguh bagi Indonesia. *Potensi Pertahanan Media Informasi Kemhan.* 31-35.

Subagyo, Agus. (2015). Sinergi Dalam Menghadapi Ancaman *Cyber warfare* Synergy In Facing Of *Cyber warfare* Threat. *Jurnal Pertahanan.* 5(1): 89-108

Tampubolon, Kartini Elivia A. (2019). Perbedaan *Cyber* Attack, *Cyber*crime, Dan *Cyber warfare*. *Jurist-Diction.* 2(2): 539-554.

Theconversation.com. (2021). Pertahanan siber Indonesia jadi tugas penting panglima TNI yang baru. Diunduh di https://theconversation.com/pertahanan-siber-indonesia-jadi-tugas-penting-panglima-tni-yang-baru-171599/ tanggal 21 Maret 2022

Thomas Rid. (2012). *Cyber* War Will Not Take Place. *Journal of Strategic Studies*. 35(1): 5-32

Viva. (2022). "*Cyber warfare* Ancam Keamanan Dunia, Merpati Perang TNI Bergerak Cepat. Diunduh di https://www.viva.co.id/militer/militer-indonesia/1449196-*cyber*-warfare-ancam-keamanan-dunia-merpati-perang-tni-bergerak-cepat/ tanggal 21 Maret 2022

Yanuar, Adams Pratama. 2021. *Cyber* War : Ancaman Baru Keamanan Nasional dan Internasional. *Jurnal Keamanan Nasional.* 7(1): 23-35