JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

ANCAMAN PERANG SIBER DI ERA DIGITAL DAN SOLUSI KEAMANAN NASIONAL INDONESIA

Salomon A.M. Babys

Abstract

This article aims to explain the meaning, forms, and threats of cyberwar against the Indonesian nation and State as well as the solutions offered to be implemented by the Indonesian people in anticipating the possibility of cyberwar by other countries against the Indonesian nation. This study uses a descriptive analysis methodology by taking information from journal articles that discuss cyber warfare. Cyberwar can be said as war through the penetration of computer systems, networks, information, and communications of other countries with the aim of damaging or creating disturbances so that the country being fought can be controlled either directly or by direct action. Cyberwarfare is identical to hybrid warfare, namely war that is complex in nature, because it can start from cybercrime, but will continue to develop towards cyberwar. The various forms of cyber warfare include Hacking, Cyber sabotage/sabotage, espionage, Cyberattack, Garding, Spyware, Vandalism, and attacks on electricity networks or vital elements of a country. Indonesia has experienced crimes or cyber wars with other countries, and Indonesia has responded by taking several anticipatory efforts including encouraging cyber security cooperation, forming regional and international agreements or norms, and building institutions. non-military national cyber to anticipate it. All anticipatory efforts by the Indonesian state are basically very positive and ideal, but there are weaknesses in the development of cyber military strength, the development of the national satellite itself, and the formation of legislation that is still not perfect to minimize the realization of cyberwar.

Abstract

Artikel ini bertujuan untuk menjelaskan terkait makna, bentuk dan ancaman dari pada perang siber terhadap bangsa dan Negara Indonesia serta solusi yang ditawarkan untuk dilaksanakan oleh bangsa Indonesia dalam mengantisipasi kemungkinan perang siber yang dilakukan negara lain terhadap bangsa Indonesia. Penelitian ini menggunakan metodologi analisis deskriftif dengan mengambil informasi dari tulisan jurnal yang membahas terkait perang siber. Perang siber dapat dikatakan sebagai sebuah perang melalui penetrasi terhadap system computer, jaringan, informasi dan komunikasi negara lain dengan tujuan untuk merusak atau menciptakan gangguan hingga negara yang diperangi dapat dikendalikan baik secara langsung maupun tindak langsung. Perang siber identik sebagai perang hibrida/*hybrid warfare* yakni peperangan yang bersifat kompleks, karena bisa bermula dari kejahatan dunia maya (*cyber crime*), tetapi akan terus berkembang menuju kepada perang siber. Bentuk dari perang siber bermacam macam meliputi *Hacking, Cyber sabotase/sabotase, Cyber spionase, Cyber attack*, *Garding, Spyware, Vandalisme*, dan *S*erangan pada jaringan listrik atau elemen vital dari suatu Negara. Telah beberapa kali Indonesia mengalami kejahatan atau perang siber, dan Indonesia telah merespon dengan melakukan beberapa upaya meliputi mendorong kerjasama keamanan siber, membentuk kesepakatan atau norma regional dan internasional, serta membangun lembaga siber nasional non militer. Segala upaya antisipasi oleh Negara Indonesia pada dasarnya sudah sangat positip dan ideal namun terdapat kelemahan meliputi belum adanya pembentukan perundang-undangan terkait perang siber yang memadai, pembangunan kekuatan militer siber nasional, pembangunan satelit nasional sendiri.

Kata kunci : ancaman perang siber, dan Solusi keamanan nasional Indonesia

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

Latar Belakang

Era digital adalah satu kondisi dimana kehidupan manusia dilaksanakan dengan teknologi digital. sebagai perkembangan dari revolusi teknologi komunikasi, sedangkan perang siber adalah suatu kondisi konflik dengan menggunakan perkembangan teknologi informasi dan komunikasi. Perang siber adalah sebuah venomena sosial dalam relasi internasional yang menjadi problem serius bagi bangsa-bangsa di dunia dalam membangun stabilitas internasional, oleh karena itu maka perang siber menjadi isu yang penting untuk dibahas karena perang siber adalah sebuah fakta, kenyatan atau realitas yang telah terjadi, sedang terjadi dan bahkan akan menjadi tren dari perang moderen di masa depan.

Perang siber (*cyber war/cyber warfare)* sangat fariatif bentuknya, sehingga untuk menghadapi perang siber, dibutuhkan adanya proses pembangunan nasional berbasis keamanan siber/*cyber security* sebagaimana telah dilakukan oleh beberapa bangsa-bangsa di dunia seperti dijelaskan oleh Letkol. Chb. Ir. Bagus Artiadi Soewardi, M.,Si; (2013;31-33), bahwa Amerika Serikat telah mengantisipasi ancaman perang siber sejak tahun 2009 dengan membangun sebuah lembaga militer siber yakni *United States cyber Command* (USCYBECOM) dengan berkedudukan dibawah *United States Strategic Command* (US-STRATCOM) bahkan, kementerian pertahanan keamanan Amerika Serikat (U.S. DoD) juga telah membangun matra tempur internet dan dunia maya sebagai matra tempur ke empat, sama dengan matra darat, laut, dan udara.

Selain Amerika Serikat (Bagus Artiadi (2013;33) dalam tulisannya menyatakan bahwa Israel juga telah membangun sebuah unit khusus untuk perang siber dengan nama Unit 8200 di bawah *Israel Difense force* (IDF). Unit ini pernah menunjukan kemampuan untuk menghentikan operasi radar senjata anti pesawat Suria dan mengirim *Worm Stuxnet* (semacam virus) terhadap sistem komputer fasilitas nuklir Iran dengan tujuan merusakan system pertahanan Suria pada tahun 2011.

Menurut Bagus Artiadi (2013;34), Australiapun sebagai negara terdekat dengan Indonesia telah membuat *Cyber security Operational Center* (CSOC) dibawah koordinasi Depertemen Pertahanan Australia yang bertugas untuk mendeteksi dan menangkal ancaman kejahatan siber terhadap pemerintahan dan kepentingan Australia. Sebelum Australia membangun CSOC, Inggris sesungguhnya telah membangun pertahanan siber dengan nama yang sama yakni "*cyber security operations center* (CSOC). Aliansi NATO pun sesungguhnya sejak tahun 2008 telah membangun pertahanan siber yang disebut juga dengan NATO CCD COE yang berpusat di Estonia. Tidak hanya negara Eropa Barat yang telah membangun kekuatan siber sebagai langkah antisipasi terhadap ancaman perang siber, Rusia dan Cina juga telah membangun kekuatan siber. Cina sendiri telah membentuk pasukan dunia maya yang disebut dengan "*blue Army*" yang bertugas untuk melindungi negara dari serangan siber dengan berpusat di Guangzhou Cina Selatan.

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

M. Badri, dalam bukunya berjudul "Perang cyber dalam dinamika komunikasi Internasional." (2012) mengatakan bahwa perang siber sesungguhnya sudah dilakukan pertamakalinya sejak tahun 2007 oleh Rusia terhadap Estonia. Bentuk serangan siber ini berhasil melumpuhkan jaringan keuangan, situs presiden, perdana menteri, parlemen, partai politik, perusahaan dan hingga situs berita. Perang siber juga pernah dilaksanakan pada tanggal 9 Juni 2009 antara korea Utara terhadap Korea Selatan dimana Korea utara melakukan perang siber dengan melakukan penyebaran virus sehingga sekitar 30.000-60.000 komputer korsel terinfeksi firus, juga sekitar 166 000 komputer bot berasal dari 74 negara diarahkan membombardir situs web pemerintah Korsel termasuk bank-bank.

Richard A. Clarke and Robert K. Knake dalam tulisan berjudul "*Cyber War The Next Threat to National Security and What to Do About It*," menjabarkan bahwa perang siber sesungguhnya merupakan bentuk dari perang dunia ketiga yang sudah terjadi. Indonesia sendiri pernah mengalami perang siber, berdasarkan catatan sejarah, sejak tahun 1998 Indonesia mengalami perang siber dengan Cina, dan Taiwan, kemudian di tahun 1999 dengan Portugal. Menurut Bagus Artiadi Soewardi, M.,Si, (2013;34) Indonesia pernah mengalami serangan siber berupa *worm stuxnet*, dengan pelaku di duga oleh Amerika Serikat dan Israel akibat sikap Indonesia dalam kasus nuklir Iran. Tidak hanya itu, Indonesia juga pernah mengalami perang siber dengan Malaysia.

Nur Khalimatus Sa'diyah dan Ria Tri Vinata (2016 h. 169), dalam tulisannya menyatakan bahwa Indonesia pernah terlibat perang siber dengan metode saling susup antara hacker Indonesia dengan Malaysia terkait isu agama, selanjutnya antara Indonesia dan Australia sebagaimana dilansir oleh Sydney Morning Herald 31 Oktober 2013 bahwa adanya penggunaan fasilitas gedung kedutaan negara Australia untuk melakukan penyadapan terhadap pemerintahan Indonesia. Perang siber jika dilihat berdasarkan metode berpikir dialektis Marx adalah kondisi anti tesis terhadap globalisasi didukung oleh era digitalisasi yang sedang berlangsung dalam panggung politik internasional saat ini, oleh karenanya perang siber akan menjadi tren dalam peperangan di era moderen, sehingga perang siber merupakan ancaman baru dalam dunia keamanan internasional, regional bahkan nasional Indonesia itu sendiri, maka menjadi pertanyaan adalah bagaimana Indonesia memahami ancaman perang siber? dan bagaimana Indonesia merespon tantangan tersebut?

Asumsi penulis adalah bahwa Indonesia masih lambat dan menunjukan tidak serius menyikapi ancaman ataupun tantangan siber, dan hal ini tentu sangat dipengaruhi oleh faktor pemahaman atau persepsi pemerintah akan perang siber itu sendiri. Disini pemerintah terkesan galau dalam menyikapi tantangan perang siber, maka menyadari bahaya laten dari perang siber serta tren perang siber sebagai strategi perang di era moderen maka penulis merasa perlu untuk melakukan penelitian terkait makna, dan sejauhana perang siber menjadi ancaman, tantangan, halangan ataupun rintangan bagi bangsa Indonesia serta sejauhmana bangsa Indonesia

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

mengkonstruksi sistem pertahanan siber nya dalam rangka menjawab ancaman perang siber itu sendiri.

Metode Penelitian

Penelitian ini menggunakan metodologi penelitian kualitatif dengan objek penelitian terfokus pada tulisan-tulisan yang telah di publikasi *(publish*) pada jurnal nasional maupun internasional. Penelitian ini juga bersifat deskriptif untuk menjelaskan makna dan subtansi perang siber itu sendiri serta solusi bagi bangsa Indonesia dalam menyikapi perang siber. Penelitian ini merupakan penelitian awal terkait isu perang siber sehingga penelitian ini adalah penelitian konseptual. Hal yang dikaji dari penelitian ini adalah seputar makna, dan bentuk dari perang siber serta solusi yang bisa dilakukan oleh Negara Indonesia dalam menghadapi ancaman perang siber. Diharapkan penelitian ini dapat menghancurkan kegalauan kita dalam mengartikan perang siber, juga membantu semua pihak untuk lebih memahami secara mendalam bentuk ancaman ataupun tantangan dari perang siber serta pemikiran alternative yang dapat dijadikan sebagai jawaban solus khusunyai bagi bangsa Indonesia dalam menghadapi ancaman ataupun tantangan perang siber itu sendiri.

PEMBAHASAN

1. Makna Perang Siber

Pembangunan teknologi informasi dan komunikasi yang berjalan sangat cepat oleh karena revolusi industry telah mendorong terjadinya perubahan pola kehidupan masyarakat dunia pada sebuah era baru yang dikenal dengan era digital/*digital era* atau *era cyber physical system.* Pada era *cyber physical system* ini muncul venomena baru pada dimensi keamanan nasional maupun internasional yakni perang siber yang dianggap sebagai tantangan ataupun ancaman baru abad ini. Perang siber berarti perang melalui media ruang siber/*cyber space*, dan karena ruang siber/C*yber space* itu sendiri bersifat *borderless*, *spaceless*, dan bahkan *timeless,* oleh karena itu perang siber sangat mudah dilaksanakan dari mana saja, dimana saja dan bisa pada momen mana saja. Tidak hanya itu, perang siber juga sangat mudah untuk dilakukan baik oleh negara (*state actor*), maupun actor non negara *(non state actor).* Perang siber dilaksanakan pada ruang siber (*syber space*) dengan menggunakan media *cyber phisycal system*. Perang siber disebut sebagai perang modern atau perang dalam bentuk modern karena dilakukan dengan menggunakan teknologi informasi, jaringan internet, dan computer sebagai alat perang. Perang siber (*cyberwarfare*/*cyber war)* cenderung menggunakan teknologi computer dan internet, oleh karena itu sering terjadi saling bersaing untuk menguasai dan memanfaatkan sumberdaya teknologi dan informasi yang ada. Menurut Richard A. Clarke and Robert K. Knake (2010. h.11) perang siber dapat diartikan sebagai suatu aksi yang dilakukan oleh sebuah negara dengan cara melakukan penetrasi terhadap komputer dan jaringan negara lain dengan tujuan untuk merusak atau menciptakan ganguan"*cyber war it*

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

refers to action by a nation-state to penetrate another nation's computer or networks for the purposes of causing damage or disruption."

Terdapat dua (2) tujuan dari perang siber yakni tujuan perantara dan tujuan utama. Tujuan perantara perang siber adalah merusak sistem tatanan, sedangkan tujuan utamanya adalah menghancurkan suatu bangsa. Secara khusus serangan siber dapat dikategorikan sebagai sebuah upaya ofensif yang dilakukan oleh-aktor-aktor negara maupun non negara dengan target penghancuran sistem informasi computer, infrastruktur, jaringan computer dan atau perangkat computer negara lain dengan menggunakan metode seperti meretas sistem computer yang rentan terhadap proses peretasan. Ciri utama dari perang siber adalah kemampuan melakukan kontrol terhadap sistem kekuatan dari suatu negara, meliputi di dalamnya adalah dapat mematikan sistem SCADA, sistem SCADA adalah *softwere* yang mengontrol jaringan kekuatan elektrik. Salah satu bentuk perang siber yang dianggab paling berbahaya adalah serangan siber dengan menggunakan *worm stuxnet* atau diistilahkan dengan "cacing computer" yang dapat merusak peranti lunak yang berjalan di atas sistem operasi *Microsoft windows*.

Perang siber dilakukan dengan beberapa motifasi; pertama sebagai bentuk dari persaian. Kedua upaya untuk menguasai, ketiga hanya untuk mengganggu, keempat untuk menyesatkan, kelima bertujuan mempengaruhi, keenam menyandera, ketujuh mengurangi informasi, kedelapan menghilangkan informasi, kesembilan mengalihkan perhatian, kesepuluh sebagai bentuk aksi seaksi saling menyerang, kesebelas menghancurkan, keduabelas menghentikan komunikasi, ketigabelas upaya menghentikan arus informasi, isi, serta berbagai bentuk lainnya yang menyebabkan negaral lain rugi, atau bahkan hancur.

Perang siber secara harafiah diartikan sebagai perang yang dilakukan di dunia maya *(cyber space)* dengan menggunakan teknologi canggih dan jaringan nirkabel/*wify*. Agus Subagyo (2015) dalam tulisannya tentang "Sinergi dalam menghadapi ancaman cyber warfare", menyatakan bahwa perang siber adalah dampak dari era digital (*digital era of world*). Era digital dapat diasosiasikan sebagai era informasi, era computer, era internet, dan era media sosial yang menuntut dan mengarahkan aktifitas manusia dilakukan secara elektronik melalui website, situs komunikasi elektronik seperti *e-commerce*, *e procurement*, *e bisnis*, *e trade*, *e servis*, *e-life stile* dan lain-lain. Pada kondisi dimana semua sektor mengalami kemajuan teknologi digital ini, maka akan muncul kerentanan terhadap serangan ataupun perang siber. Perang siber bermula sebagai bagian dari kejahatan dunia maya (*cyber crime*), dan akan terus berkembang menuju kepada perang siber. Menurut Agus, kejahatan siber (*cyber crime)*, merupakan suatu jenis kejahatan transnasional yang melibatkan pelaku dari dua Negara atau lebih, dengan korbannya bisa lebih dari satu negara. Bentuk operasional dari perang siber pada tingkatan kejahatan siber adalah pertama melakukan *hacker* dan *cracker* di dunia maya melalui situs, blog, email, dan media sosial, dan kedua adalah peretasan, dan pengrusakan terhadap berbagai sistem *software*/perangkat lunak.

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

Kejahatan siber/*Cyber crime* memiliki dua makna, pertama *cyber crime* dalam arti luas disebut juga sebagai *computer related crime,* dimana pelaku secara illegal menggunakan sistem computer dan jaringan, dan kedua *cyber crime* dalam arti sempit adalah *computer crime* yakni pelaku secara illegal/melanggar menyerang sistem keamanan computer, dan data yang diproses oleh computer lain. Kejahatan siber (*cyber crime)* menurut Agus Subagyo (2015) sangatlah kompleks beliputi beberapa bentuk antara lain;

1. *Hacking*. H*aecking/*peretasan merupakan kegiatan menerobos masuk program-program computer milik pihak lain. *Hacking* terbagi atas 2 bentuk. Pertama; *Hacking* budiman yang sifatnya tidak merusak dan kedua *haecking* pencoleng yang masuk ke dalam computer untuk merusak dan atau mencuri data. Termasuk dalam *hacking* pencoleng biasa disebut juga sebagai *Cracking*. *Cracking* menurut Ineu Rahmawati (2017, h. 59-60) memiliki sasaran yang kompleks diantaranya data base, kartu kredit, data base *account bank*, data base informasi pelanggan, dan pembelian barang dengan kartu kredit palsu.
2. *Cyber sabotase/sabotase*; adalah kegiatan yang dilakukan dengan membuat gangguan, pengrusakan dan penghancuran terhadap suatu data, program computer atau sistem jaringan yang berhubungan dengan internet. Sabotase dilakukan menggunakan komputer dan satelit untuk mengetahui koordinat lokasi peralatan tempur musuh, juga dapat berupa penyadapan informasi, mengganggu peralatan komunikasi terkait sumber energi, air, bahan bakar, komunikasi, dan infrastruktur transportasi, sehingga semua menjadi rentan terhadap gangguan sabotase, dan itu dapat dilakukan pada perangkat *hardwere* maupun *softwere.* Mcdonnell dan Sayers, dalam pembahasan terkait sabotase melalui perangkat *hardwere* dan *softwere* menjelaskan tiga (3) jenis ancaman siber meliputi: **pertama**; Ancaman melalui perangkat keras (*hardwere threat*) ancaman ini merupakan ancaman yang disebabkan oleh pemasangan perangkat tertentu yang berfungsi untuk melakukan kegiatan tertentu di dalam suatu system sehingga peralatan tersebut merupakan elemen pengganggu system jaringan dan perangkat keras lainnya. **Kedua;** ancaman perangkat lunak/*softwere threat;* merupakan ancaman yang disebabkan masuknya perangkat lunak tententu yang berfungsi untuk melakukan kegiatan pencurian, pengrusakan dan manipulasi informasi. Pada ancaman melalui perangkat lunak ini menurut Amarmuazam Usmani Bin Othman (2001) terbagi dalam beberapa bentuk seperti propaganda media social, penyadapan, dan menggangu system pertahanan dan atministrasi dari sebuah Negara. **Ketiga;** adalah ancaman data/informasi/*information threat;* merupakan ancaman yang diakibatkan oleh penyebaran data/informasi tertentu yang bertujuan untuk kepentingan tertentu (Ineu Rahmawati (2007;55)).
3. *Cyber spionase* dan propaganda siber. Menurut Amarmuazam Usmani Bin Othman (2001) bentuk ancaman media siber terhadap suatu negara termasuk *cyber spionase* dan propaganda siber. *Spionase siber* sendiri adalah kejahatan yang menggunakan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain dengan memasuki

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

system jaringan computer (*computer network system*) pihak sasaran. Makna lain dari *cyber spionase* adalah Pengumpulan informasi rahasia dari individu pesaing/*rival*, kelompok pemerintah, dan musuh baik dari bidang militer, politik maupun ekonomi dengan cara eksploitasi secara illegal melalui internet, jaringan, perangkat lunak, ataupun perangkat keras. Sedangkan propaganda siber adalah sebuah upaya yang bertujuan mempengaruhi opini publik. Propaganda siber dapat mengancam kestabilan sebuah Negara.

4. *Cyber attack* adalah semua tindakan yang sengaja dilakukan untuk mengganggu kerahasiaan informasi, integritas dan ketersediaaan informasi. Rika Isnarti (2016) dalam tulisannya *A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War* menjelaskan perbedaan antara *cyber attac* dan *siber espionage*, bahwa *cyber attack* dapat diasosiasikan juga sebagai *syber war. C*iri dari *cyber attack* adalah yang diserang adalah musuh, sebaliknya jika yang menyerang adalah bukan musuh maka itu disebut Siber mata mata/*cyber espionage*. *Cyber espionage* adalah sikap mencuri informasi secara khusus dari hasil penelitian perusahaan atau universitas kemudian mengirimkannya pada lembaga lain dengan berorientasi mengambil keuntungan, atau mendapat informasi tanpa mengeluarkan banyak uang untuk melakukan pelitian.
5. *Garding. Garding* adalah berbelanja menggunakan nomor dan identitas kartu kredit orang lain yang diperoleh secara illegal misalnya mencuri data internet.
6. *Spyware*. *Spyware* adalah program merekam secara rahasia segala aktifitas online user, kemudian dijual kepada pihal lain.
7. *Vandalisme*. Vandalisme merupakan suatu bentuk perang siber dengan merusak halaman web (*deface*) atau menggunakan serangan *denial of service* yaitu merusak sumber daya dari computer lain. *Deface* biasa dilakukan dalam bentuk propaganda. melalui situs, email, instant massage/pesan teks.
8. *S*erangan pada jaringan listrik. Bentuk serangan ini dapat berupa pemadaman jaringan listrik sehingga bisa mengganggu perekonomian, mengalihkan perhatian terhadap serangan militer lawan yang berlangsung secara simultan, yang mengakibatkan trauma nasional.

Nur Khalimatus Sa'diyah dan Ria Tri Vinata pada tulisannya menekankan perang siber merupakan perang gaya baru, identik sebagai perang hibrida/*hybrid warfare*. perang hibrida/*hybrid warfare* adalah peperangan yang bersifat kompleks, karena dilakukan secara kompleks baik pada metode, cara, teknik dan taktik berperang. Perang siber sendiri adalah perang yang menggunakan fasilitas *world wide web* dan jaringan komputer, atau teknologi system informasi untuk mendukung kepentingan komunikasi oleh satuan-satuan komando kendali militer modern.

Richard A. Clarke and Robert K. Knake (22) menjelaskan bahwa perang siber tidak hanya merupakan perang psikologi yang menggunakan misi propaganda, atau melakukan spionase elektronik dengan melakukan penetrasi untuk mengumpulkan data atau memutuskan jaringan, tetapi Perang siber memiliki orientasi yang kompleks. Menurut Richard A. Clarke and Robert K. Knake (39) terdapat tiga pemikiran di dalam ruang siber

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

yang membuat perang siber itu dapat terjadi; pertama adalah kelemahan dalam mendesain internet, (yang meliputi jaringan ISPs dan IT and T/ biasa disebut juga dengan BGP/*border Getway Protocol*) sehingga mudah di hacker, kedua adalah adanya kerentanan dari computer itu sendiri dan kecacatan dalam *softwere*/perangkat lunak dan *hardwere/* perangkat keras, (senjata dari para haeker adalah marware) dan ketiga adalah penempatan sistem dan langkah yang semakin penting secara online.

2. Aktor perang siber

M. Badri (2012) Dalam tulisanya, menjabarkan bahwa ruang maya/*cyber space* adalah ranah pertempuran modern. Actor dari perang siber dikategorikan dalam dua jenis yakni pertama actor Negara/ *state actor* dan kedu aktor non Negara/*non state actor*. Kedua actor ini kemudian dibagi lagi dalam dua kategori yakni actor dari kalangan para ahli, dan kemudia actor amatiran yang melakukan untuk memenuhi keinginan untuk belajar melakukan kegiatan destruktif, meski demikian aktor dari perang siber rata rata memiliki ketrampilan di bidang strategi keamanan dan pengamanan serta serangan informasi (*information security and warfare*), seperti ahli meretas/hacking, spionase/espionage, forensic digital/digital forensic dan, analis keamanan jaringan/*network security analysist.*
Ineu Rahmawati (201. H. 56), dalam analisisnya menyatakan bahwa actor kejahatan siber didominasi oleh actor non Negara seperti individu *hacker*, kelompok *hacker*, non *governmental organization* (NGO), terorisme, kelompok kejahatan terorganisir serta sektor swasta seperti *interent companies* and *carries*, dan *security companies.* Mengutip hasil penelitian Dr. Frederick Wamala Ineu Rahmawati (2017. H. 56) menambahkan bahwa elemen dari aktor kejahatan siber bisa dari Inteligen asing/*foreign intelligence*, bisa dari pekerja yang mengalami Kekecewaan/*disaffected employees*, juga bisa dari Investigasi jurnalis/*investigative journalist*, Organisasi ekstimis/*extremist organization*, Aktivitas para haecker/*hacktivist* dan Group criminal yang terorganisasi.

Kerawanan Terhadap Perang Siber

Revolusi di bidang teknologi informasi dan komunikasi telah memberikan kemafaatan atau kearifan yang berarti bagi masyarakat dunia untuk berinteraksi, namun hal tersebut juga menyisihkan persoalan baru berupa ancaman perang siber. Jan Kalberg mengatakan bahwa terdapat empat hal yang perlu diantisipasi dari perang siber Pertama; musuhnya anonim, kedua; objeknya tetap, ketiga; hasilnya terukur, dan keempat; eksekusinya cepat.
Dalam tulisannya, M. Badri (2012. H. 104) menjelaskan bahwa perang siber rentan pada negara dan masyarakat yang melakukan pengembangan teknologi elektromagnetik dan teknologi informasi dan komunikasi. Menurutnya perang siber bukan hanya perang di dunia maya untuk menyerang personil, fasilitas atau peralatan informasi dan computer, tetapi menjadi bagian dari *Information operations* (IO) yang meliputi di dalamnya adalah

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

operasi psikologis, penipuan militer, operasi keamanan, peperangan elektronik dan *computer network operations* (CNO) yang diduga sebagai suatu tindakan penggunaan jaringan computer untuk menyerang sistem dan jaringan informasi masyarakat.

Teori yang digunakan dalam strategi perang siber berdasarkan Dr. J. Kallberg (2016;13) adalah menciptakan instabilitas pada negara sasaran, sehingga perang siber dapat dikatakan berhasil jika mampu menghilangkan kapasitas militer atau menciptakan destabilisasi sosial pada negara sasaran. Dalam hal ini maka orientasi perang siber adalah memperlemah institusi sehingga masyarakat menjadi tidak stabil, dan pada akhirnya kondisi negara menjadi lemah, dan ketika negara menjadi lemah, maka negara tersebut akan cenderung tunduk pada kekuatan asing. Dalam pandangan strategis, perang siber hanya digunakan dalam mensuport operasi militer dan geopolitik, oleh karena itu dikatakan oleh Martin Libicki bahwa perang dunia maya bukan mekanisme yang berdiri sendiri dalam peperangan, tetapi ada korelasi yang intim antara perang siber dan kekuatan lainnya (Jan Kallberg (2016 h.119).

Sasaran dari perang siber sangat variatif, namun salah satu bentuk dari sasaran utama dilakukanya perang siber adalah menciptakan ketidakstabilan. Upaya menciptakan ketidakstabilan itu dimulai dari mencari kelemahan institusional, melahirkan gelombang sentiment rakyat serta adanya oposisi terhadap pemerintah yang dapat menciptakan dampak lanjutan. Disinilah target dari perang siber adalah menciptakan rasa kurang percaya masyarakat pada pemerintahan karena dianggab pemerintah tidak mampu mengatur struktur sosial. Colin S. Gray dalam DR. Jan Kallberg (2016.119-121) menjabarkan lima (5) factor berdasarkan theory Waldo yang dijadikan rujukan sasaran oleh negara aggressor dalam melakukan perang siber;

Pertama; factor legitimasi (yang terpenting dari faktor ini adalah adanya legitimasi masyarakat terhadap pemerintah yang sah dan adanya penerimaan oleh elemen masyarakat). Serangan siber dalam dimensi ini berusaha untuk menghancurkan legitimasi negara, dengan cara menghancurkan harapan dari masyarakat terhadap pemerintahan negara dan menciptakan opini masyarakat bahwa pemerintah (yang sedang memerintah) tidak mampu memerintah negara. Target lain dari perang siber pada dimensi pertama ini adalah; pada lembaga legislatif, dinama diupayakan untuk mengungkapkan informasi yang dirahasiakan, pembocoran terhadap lalu lintas Email dan komunikasi dari eselon tertinggi negara.

Kedua; adalah factor otoritas (meliputi internal dan eksternal) yakni kemampuan untuk menjalankan kebijakan secara rasional yang sesuai dengan harapan untuk kepentingan umum, bersifat etis, dan sesuai institusional. Dalam dimensi ini, otoritas memiliki hubungan yang erat dengan hirarki, tanpa hirarki tidak ada kepemimpinan yang dapat bertanggungjawab, dan jika tidak ada tanggungjawab secara kelembagaan maka sebuah organisasi akan menjadi anarki. Pada dimensi ini, sasaran dari serangan siber adalah pada

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

sistem informasi penegakan hukum, berupaya memperoleh data pribadi informan loyalis, menyuntikkan materi terlarang pada computer dan jaringan loyalis.

Ketiga; adalah pengetahuan manajemen (pengetahuan dalam arti ini adalah segala yang dihasilkan dari sektor pelayanan publik sebagai informasi baik itu berupa dokumen, sikap, tuntutan-tuntutan, publikasi maupun kebijakan. Sedangkan manajemen artinya kemampuan untuk mengatur/ mengkoordinasikan, oleh birokrasi). Salah satu tantangan bagi sebuah pemerintahan moderen adalah terkait dengan pengetahuan manajemen. Jika administrator public, tidak mampu mengatur pengetahuan dan informasi, maka rakyat akan menilai bahwa pemerintahan tidak kompeten. Serangan siber pada dimensi manajemen pengetahuan institusional ini akan melumpuhkan birokrasi dan memancing kemarahan publik. Serangan siber pada dimensi ini terfokus pada data real negara, merusak informasi dasar data kepemilikan.

Keempat; adalah kontrol birokrasi (adalah kemampuan untuk mendominasi dan mengendalikan birokrasi). Ketika pemerintah tidak memiliki kemampuan untuk melakukan kontrol tersebut, maka kewenangan itu hilang, dan jika kontrol itu hilang, maka korupsi, sikap pilih kasih, pencurian akan turut terjadi. Serangan siber dalam dimensi ini terfokus pada penghancuran perangkat keras latihan, sistem informasi unit keamanan, mendestabilisasi sistem keuangan oleh pembayaran besar-besaran dana public.

Kelima; adalah kepercayaan (yang dimaksud dari kepercayaan di sini adalah kepercayaan masyarakat terhadap pemerintah yang sanggup membawa masyarakat mencapai impian mereka dan mampu melindungi masyarakat di masa depan). Ketika masyarakat merasa aman, maka mereka masih memiliki kepercayaan, dan optimisme terhadap masa depan, dan mereka percaya bahwa pemerintah dapat memenuhi kebutuhan kebutuhan yang mereka butuhkan, namun kegagalan yang dilakukan secara sistematik, akan mengurangi kepercayaan masyarakat terhadap pemerintah. Sasaran siber dari dimensi ini antara lain; pada sistem gaji pemerintah, transfer dukungan keuangan publik, data real korupsi, dan data informasi kepemilikan.

Target utama dari perang siber sesungguhnya adalah pemerintahan sebuah negara yang lemah, tujuan utamanya adalah untuk menimbulkan rasa ketidakpercayaan masyarakat terhadap pemerintahan yang sah, karena negara dianggap gagal dalam menjaga struktur masyarakat sehingga menimbulkan destabilitasi sosial. Jan Kalberg mengartikan Perang Siber adalah sebuah sarana dalam mencapai tujuan geopolitik dari suatu negara melalui mengacaukan negara musuh dengan strategi mengeksploitasi kelemahan negara yang dimusuhi. Untuk melaksanakan perang siber beberapa strategi yang digunakan adalah pertama memprediksi kelemahan pemerintah yang ditarget, kedua membantu melakukan perubahan rezim yang ditarget dengan rezim yang diprakarsai dan ketiga membuat negara yang ditarget tunduk pada kekuatan asing, jadi strategi perang siber sesungguhnya bertujuan mengubah teori Waldo terkait stabilitas sebuah masyarakat menjadi masyarakat yang tidak stabil, maka jika menurut Waldo factor stabilitas sebuah masyarakat itu bergantung pada factor legitimasi/*legitimacy*, otoritas/*authority*, pengetahuan

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

manajemen*/knowleg management,* kontrol birokrasi/*bureaucratic control* dan kepercayaan/*confidenc,* maka siber war berorientasi melumpuhkan 5 faktor yang menjadi bagian dari pilar penting stabilitas masyarkat ini.

Ineu Rahmawati (2017) menyatakan bahwa kejahatan siber dapat berdampak pada ganguan siber (*cyber violence*), bahkan perang siber (*cyber warfare*) karena pada hakekatnya setiap kejahatan siber merupakan ancaman siber yang potensial dalam kehancuran sebuah Negara. Dalam konteks tersebut, maka ancaman siber tidak hanya ditujukan kepada instansi dan lembaga pemerintah secara khusus ke elemen TNI dan polri tetapi juga mengancam aspek lain seperti ekonomi, politik dan budaya.

Amarmuazam Usmani Bin Othman (2001), pada tulisannya berjudu "Analisis penggunaan media siber terhadap keamanan nasional suatu studi di Malaysia" menyatakan bahwa kerawanan siber dari suatu negara dapat terjadi karena beberapa hal Pertama adalah peralatan system pertahanan siber yang belum memadai, (harus selalu mengikuti tren perkembangan teknologi siber terbaru), kedua adalah faktor politik nasional yang tidak harmonis, ketiga ketidakhati-hatian terhadap penyebaran virus yang dapat menciptakan kekacauan dalam system jaringan, dan keempat adalah budaya masyarakat yang tidak baik dan benar dalam bekerja atau bermedia social atau bercomputer.

Hidayat Chusnul Chotimah (2019) dalam tulisan tentang "Tata kelolah kemanaan siber Indonesia di bawah kelembagaan Badan Siber dan sandi Negara" menyatakan bahwa Dari kerawanan siber, dapat menuju kepada ancaman siber. Kerawanan siber dipengaruhi oleh beberapa faktor seperti ketergantungan pada kesediaan (*availability*), keutuhan (*integrity*) dan kerahasiaan (*confidentially*) informasi melalui jaringan internet, sedangkan ancaman siber meliputi beberapa bentuk diantaranya; *siber crime, cyber terrorism*, *cyber hacktivism* maupun *cyber warefare.* Berdasarkan konsepsi teoretis terkait tingkat kerawanan sebuah Negara terhadap ancaman siber ini, maka dapat dikatakan bahwa Indonesia memiliki kelemahan yang sangat kompleks dalam mengantisipasi perang siber oleh karenanya Indonesia sangat rentan atau rawan terhadap perang siber.

Indonesia Menghadapi Ancaman Perang Siber

Indonesia termasuk dalam daftar negara yang sangat rawan terhadap serangan siber atau perang siber. Handrini Ardiyanti (2014) dalam tulisannya berjudul "Cyber-security dan tantangan pengembangan di Indonesia" mengatakan bahwa Negara yang paling rentan terhadap perang siber adalah negara pengguna jasa internet, dan Indonesia termasuk dalam daftar negara paling rentan terhadap serangan siber tersebut bahkan menjadi target utama para *hacker* karena Indonesia masuk dalam daftar Negara pengguna internet terbesar di dunia (dengan jumlah pengguna internet mencapai 82 juta orang) dn bahwa Indonesia sebagai negara yang lemah dalam manajemen keamanan siber.

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

Hidayat Chusnul Chotimah (2019) mengatakan bahwa dalam menghadapi ancaman siber yang terpenting adalah tatakelolah penanganan ancaman siber yang baik oleh Badan siber dan Sandi Negara, dengan kata lain lembaga ini harus benar-benar dapat berfungsi atau difungsikan untuk mengantisipasi ancaman siber, serta menjaga keamanan dan kedaulatan siber nasional. Nur Khalimatus Sa'diyah dan Ria Tri Vinata (2016) pada penelitian terkait rekonstruksi pembentukan *national cyber defence* menggambarkan mengenai solusi atau cara menghadapi perang hibrida (perang siber) secara nasional adalah;

Pertama; membuat/menyempurnakan doktrin TNI khusus terkait konsep menghadapi ancaman perang hibrida, juga perlu pembenahan pada dimensi hukum dan UU serta kebijakan dalam kaitan dengan *siber security,* termasuk perlu pembentukan unit perang siber seperti *national cyber defense/cyber army* atau *ciber warrior* yang memiliki kemampuan melakukan perang elektronik khususnya *cyber defense* dan *cyber attack*. **Kedua**; Peningkatan SDM melalui pelatihan dalam dan luar negeri sehingga mencapai SDM yang memiliki kemampuan dalam melaksanakan perang hibrida yang meliputi ahli piranti lunak, ahli anti haecker, pakar informasi, pakar telematika, ahli bahan peledak, ahli fisika atom, ahli biologi, dan pakar taktik militer. **Ketiga**; Pembangunan satelit bersama dalam menjalankan misi perang siber meliputi satelit teknologi system informasi NCW/*network Centric Warfare* infrastruktur *SIPRNet*, dan satelit mata-mata, termasuk satelit GPS. Tiga satelit ini kemudian diperinci pada 4 kebutuhan dalam perang hibrida meliputi, pertama; satelit untuk mempelajari ruang angkasa. Kedua; satelit telekomunikasi, ketiga; satelit militer yang dilengkapi dengan senjata laser dan keempat; satelit pemantau langit atau astronomi.

Nur Khalimatus Sa'diyah dan Ria Tri Vinata (2016) menambahkan bahwa dalam pembangunan badan siber dan tentara siber, beberapa prasyarat sederhana yang harus menjadi kualifikasi bagi para siber adalah; seperti memiliki kemampuan mengoperasionalkan computer, mengelolah internet, menyelidiki media social, melakukan penyadapan, mampu menggunakan perangkat lunak dan perangkat keras, mampu membangun system, jaringan, dan melakukan operasi dunia maya, mampu melakukan penyidikan dunia maya, dan menangkis berbagai virus dunia maya serta melindungi berbagai data dan informasi dalam system elektronik di Indonesia, termasuk memiliki kualifikasi untuk melakukan serangan balik terhadap serangan siber dari pihak lain sebagai bentuk menjaga kedaulatan nasional dari serangan siber.

Indonesia saat ini berada dalam giat pembangunan infrastruktur strategis dan layanan publik yang telah bergantung pada system informasi teknologi dan jaringan internet sehingga otomatis sangat rentan terhadap serangan siber. Melihat sisi kelemahan ini, maka diharapkan Indonesia dapat segera memperkuat infrastruktur militer berbasis siber, mengingat infrastruktur berbasis internet ini penting dan yang lebih penting adalah infrastruktur komando pasukan cyber, karena jika kebutuhan ini tidak dipenuhi maka Indonesia akan selalu berada pada posisi inferior dan mengalami kehilangan posisi tawar dalam percaturan politik global di masa depan.

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

Ineu Rahmawati (2017. H. 55) juga menyatakan bahwa untuk menghadapi kejahatan siber, maka pembentukan pasukan siber/*cyber army* merupakan bagian dari pertahanan siber/*cyber defense* yang sangat relevan dengan berfokus pada pertahanan system komunikasi dan informasi yang diperuntukan untuk menangkis segala serangan. Bahkan Ineu Rahmawati berharap agar pasukan siber yang dibangun harus memiliki kemampuan menyerang/*offensive* serta dapat mengimbangi kemajuan teknologi Negara lain.

Menghadapi tantangan baru ini, Handrini Ardiyanti. (2014 H. 98) menjelaskan bahwa Indonesia masih perlu mengkualifikasi beberapa hal penting dalam kaitan dengan keamanan siber/*cyber security* diantaranya; **Pertama**; kepastian hukum keamanan siber di Indonesia. Dikatakan bahwa saat ini acuan pertahanan siber hanya mengacu pada UU Informasi dan transaksi elektronik No. 11 tahun 2008 dan peraturan pemerintah tentang penyelenggaraan system dan traksaksi elektronik No. 82 tahun 2012, ditambah surat edaran dan peraturan menteri dan Perppres No.53 tahun 2017, dimana berdasarkan ketentuan perundang-undangan di atas, maka tata kelolah kemanan siber dibawah koordinasi dan kerjasama institusi di bawah BSSN dengan meliputi kepolisian *(cyber crime*), TNI (*cyber difense*) dan kementerian Luar negeri (*cyber diplomacy*), juga kementerian komunikasi dan informasi dan lembaga- lembaga lain sebagai upaya untuk saling berkalaborasi, berkoordinasi, sinergi, dan sharing informasi.

Kedua; Dalam persoalan teknis dan tindakan prosedural, Hasyim Gautama menjelaskan terkait adanya beberapa kelemahan yang mempengaruhi proses pembangunan *cyber security* di Indonesia adalah lemahnya kesadaran akan ancaman *cyber attack*, dan lemahnya kesadaran Negara terkait pentingnya *cyber security*. Menurutnya, hal ini nampak pada level kejahatan siber saja tidak adanya system penanganan kejahatan siber yang baku. Solusi yag ditawarkan dalam menyelesaikan hal ini menurut Hasyim adalah kita masih membutuhkan infranstruktur standar dalam menghadapi *cyber war*, termasuk di dalamnya adalah *perimeter defence* yang memadai, *network monitoring system*, *system information* dan *ivent managemen* yang berfungsi memonitoring berbagai masalah keamanan.

Ketiga; Terkait struktur organisasi. Dikatakan bahwa keamanan siber/C*yber security* yang dilaksanakan di Indonesia masih terbilang lemah karena dijalankan secara sektoral dan belum menyeluruh sehingga yang baru terlihat adalah pembentukan tim kerja pusat operasi dunia maya (*cyber difence operation center*) yang hanya bertujuan pada pengamanan keamanan internal Kemhan.

Keempat ; Terkait *capacity building*, dijabarkan bahwa *capacity building* yang dilakukan di Indonesia baru dalam koordinasi kemhan dengan membangun 3 program yang dilakukan dari tahun 2014-2017 seperti persiapan model *perang cyber*, membuat seminar *military cyber intelligence and cyber operation* dan kegiatan *cyber cam* atau pekan siber.

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

Kelima; Terkait kerjasama internasional, dikatakan bahwa sejauh ini Indonesia telah menjalin kerjasama internasional dan regional menangani *cyber crime* sebagai upaya membangun kerjasama dalam mengantisipasi pencegahan *cyber crime*. Prestasi yang telah di capai terkait hal ini seperti menjadi anggota *Asean network security council*, menjadi anggota *international telecommunication union* (ITU), menjadi *steering comitee Asia Pacific computer emergency Respons team* (APCERT), menjadi anggota dari *forum of incident Response and Security* (FIRST), melakukan kerjasama bilateral di bidang *cyber security* dengan Jepang, Inggris dan beberapa Negara, dan terakhir Indonesia juga terlibat dalam program *security agenda (*GSA) tahun 2007. Pada dimensi internasional, BSSN juga telah membangun beberapa kerjasama yang telah dilakukan antara lain; pertama kesepakatan bilateral dalam rana siber dengan Belanda pada tanggal 3 Juli 2018, dengan Australia dan Inggris pada Agustus 2018, dan dengan Amerika Serikat 28 September 2018, selain kerjasama bilateral, kerjasama dalam siber secara multilateral juga telah dilakukan Indonesia pada organisasi Asean Regional Forum (ARF) yang melibatkan beberapa Negara diluar ASEAN seperti Tiongkok, Rusia dll tetapi Indonesia juga tergabung dalam *ASEAN cyber Capacity program* (ACCP) yang diresmikan pada bulan April 2017. Dikatakan bahwa hingga saat ini belum ada kesepakatan internasional yang mengikat terkait dengan *cyber security* sehingga masih menjadi suatu pekerjaan rumah (PR) bagi Negara Indonesia dalam merumuskan sebuah kerjasama yang baik bagi keamanan siber dengan semua Negara di dunia.

Amarmuazam Usmani Bin Othman.(2017) pada tulisannya menawarkan solusi yang sangat rasional bagi negara Indonesia dalam menghadapi serangan siber melalui beberapa alternative strategi. Pertama; Penanganan pada skala global dan regional dimana Negara Indonesia perlu mendorong pembentukan mekanisme tanggap insiden internasional dan jaringan kerjasama ditingkat global dan regional untuk menjamin kemampuan pengelolaan kejadian dalam kasus ganguan global. Kedua; penanganan ancaman siber pada skala nasional. Hal ini dapat dilakukan dengan mengintegrasikan seluruh elemen yang terkait dengan keamanan siber, dan agar SOP diperjelas sehingga tidak terjadi tumpang tindih kewenangan dan tugas. Ketiga; penangananan ancaman siber pada skala masyarakat dan individu dengan cara melakukan kampanye terkait kesadaran siber masyarakat dan individu.

Rika Isnarti (2016) pada penelitiannya tentang *A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War* menawarkan tiga pendekatan untuk dapat menghadapi ancaman ataupun tantangan perang siber meliputi pendekatan Neorealism, Liberalism, and Constructivism. Berdasarkan pendekatan neorealis yang perlu adalah pertama negara mengontrol dan mengoperasikan jaringan internet pada seluruh wilayah dan pendekatan ini telah dipraktekan oleh Rusia dan Tiongkok dimana pada dua Negara tersebut Negara memfilter segala sesuatu yang yang masuk pada ruang siber. Kedua berdasarkan pendekatan liberalis, perang siber dilakukan oleh siapa saja entah itu actor negara maupun bukan Negara, baik oleh negara otoriter ataupun negara demokrasi, maka seluruh negara akan mengalami kesulitan untuk menanganinya, sehingga sesungguhnya tidak akan ada satupun negara yang dapat secara mandiri

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

mampu menjamin keamanan sibernya, oleh karena itu perlu kerjasama institusi supaya dapat mengontrol sikap para aktor dari dunia siber atau mencegah perang siber, dan ketiga berdasarkan paradigma konstruktifisme, menekankan bahwa karena realitas sosial adalah hasil dari konstruksi sosial, oleh karena itu jaminan terhadap keamanan siber sangat ditentukan dari sejauhmana suatu negara mengartikan dirinya sendiri, dan pola interaksi yang dilaksanakan sendiri, oleh karenanya solusi untuk dapat menghadapi perang siber adalah interaksi, mengingat banyak hal yang dapat diperoleh melalui intensitas berinteraksi atau komunikasi diantaranya, kita dapat memahami actor lain, dan kemudian mempermudah kita untuk menilainya sebagai teman atau lawan, dan dengan komunikasi akan terbangun kesadaran akan pentingnya norma dan standar sikap yang dikehendaki bersama sehingga akan mampu membangun sebuah budaya baru yang kaya akan nilai dan aturan yang berkeadaban.

Rika Isnarti (2016) menambahkan bahwa Perang siber sesungguhnya adalah perang informasi, karenanya perlu pembangunan kekuatan siber. Pembangunan kekuatan siber, tidaklah mahal karena terdapat perbedan mencolok antara *siber war* dengan *kinetic war* pertama; *siber war* lebih murah karena setiap orang yang dapat tersambung ke computer dan kemudian dapat melakukan siber war, oleh karena itu negara dengan ekonomi lemahpun dapat melakukan perang siber, karena itulah untuk dapat menentukan actor kekuatan siber itu sangat sulit untuk diprediksikan, dalam hal ini setiap Negara memiliki potensi untuk menjadi kekuatan siber. Kedua siber war tidak memakan banyak korban atau mererebut teritori dari negara lain. Ketiga actor perang siber tidak hanya menggunaan kekuatan militer, tetapi juga menggunakan masyarakat sipil yang paham/ sehingga setiap orang dapat menjadi prajurit siber *siber warrior*/penyerbu siber/*siber invader*.

Terkait dengan urgensi komunikasi yang menjadi solusi dalam mengantisipasi terjadi perang siber M. Badri (2012 H. 109) menyatakan bahwa perang siber dapat terjadi ketika komunikasi internasional gagal mencapai tujuan, atau ketika adanya ketidakharmonisasi/disharmonisasi dalam berkomunikasi antar Negara. Maka solusi yang dapat digunakan adalah membangun keharmonisan dalam kehidupan berbangsa dan bernegara. Memperkuat preposisi di atas Hidayat Chusnul Chotimah (2019) menawarkan satu-satunya solusi kongkrit dalam menghadapi serangan siber adalah dengan menjalankan diplomasi siber. Diplomasi siber yang diaksud adalah seperti yang diartikan oleh Berrinha dan Renard merupakan diplomasi yang dilakukan dalam ranah atau domain siber untuk mengamankan kepentingan nasional pada dunia maya yang dilakukan pada format bilateral maupun multilateral. Agenda diplomasi siber meliputi beberapa isu antara lain isu *cyber security, cyber crime, confidence building, internet freedom, internet governance.*

M. Badri. (2012) dalam tulisannya berjudul "Perang cyber dalam dinamika komunikasi Internasional" sedikit memperkaya makna diplomasi siber dengan istilah diplomasi virtual, dan menurutnya diplomasi virtual menurutnya lebih tepat sasar karena menurutnya diplomasi virtual memiliki dua makna. Pertama secara luas adalah suatu pengintegrasian dari teknologi komunikasi

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

dan informasi terutama media satelit seperti internet dalam rangka tercapainya kepentingan nasional, kedua secara sempit pemanfaatan teknologi informasi dan komunikasi terutama media satelit seperti internet untuk menjalankan fungsi dari diplomasi itu sendiri meliputi presentasi, informasi, negosiasi, dan komunikasi.

Kesimpulan

Perang siber pada tingkat umum dan general adalah bentuk ancaman baru terhadap keamanan, ketertiban dan keteraturan dunia, namun pada tingkatan spesifik merupakan ancaman baru dalam penguasaan dan pengendalian serta penghancurkan peradaban suatu bangsa. Perang siber diibaratkan sebagai sebuah perang melalui *remote control* dengan tujuan akhirnya adalah penguasaan atau pengendalian suatu negara baik secara langsung maupun tindak langsung. Perang siber sangat berbeda jauh dari perang konvensional yang selama ini terjadi, perbedaannya adalah bahwa perang siber dilaksanakan oleh aktor Negara maupun non Negara pada ruang siber (*syber space),* dengan karakter yang bersifat *borderless*, *spaceless*, dan bahkan *timeless.* Bentuk operasional dari perang siber dapat diklasifikasikan meliputi; *hackers*/meretas, menyadap *spy*/mata-mata, *alter*/mengubah, *sabotage*/sabotase, *disrupt*/mengganggu, *attack*/menyerang, *manipulate*/memanipulasi, *interfere*/menginterfensi, *expose*/mengungkap, *steal*/mencuri dan *destabilize*/destabilisasi.

Indonesia masih sangat rentan terhadap serangan siber. Hal mendasar adalah karena pertama Indonesia bukan negara maju dan kaya. Kedua; teknologis informasi dan telekomunikasi kita masih tergantung pada negara-negara maju/*be have* dengan hak paten pemilik teknologi. Ketiga Indonesia hanya konsumen atau pengguna jasa internet dengan prosentasi yang sangatlah tinggi. Keempat di Indonesia belum terbangun system pertahanan siber untuk dapat mengantisipasi segala kemungkinan bisa terjadinya perang siber. Perang siber adalah perang moderen yang perlu diantisipasi dengan segala analisis yang komprehensif, oleh karenanya berdasarkan kondisi, dan posisioning dari Indonesia sendiri, maka Indonesia perlu melakukan pembangunan keamanan siber*/siber security* dengan multi pendekatan dan dilaksanakan secara komprehensif dan professional. Indonesia juga perlu melakukan kerjasama pada level internasional, regional, tri dan biateral untuk menghadapi ancaman perang siber dari actor Negara maupun masyarakat trans internasional.

Menghadapi ancaman perang siber maka hal yang perlu dilakukan oleh Negara Indonesia meliputi tiga hal, pertama; pentingnya pembangunan Sumber Daya manusia Indonesia yang memahami terkait teknologi, meliputi pemahaman terkait pemanfaatan teknologi secara tepat guna, pemahaman operasional teknologi dalam menghadapi segala bentuk peran siber, termasuk qualitas sumber daya manusia dalam menjalankan diplomasi siber dan strategi manajemen informasi. Kedua adalah pentingnya pembangunan fasilitas media siber yang memadai meliputi fasilitas computer, penguasaan internet, pembuatan *soft were* anti firus, termasuk satelit, dan ketiga pentingnya pembangunan komando battalion pasukan siber dari seluruh unsur elemen bangsa dan

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

Negara Indonesia termasuk dari unsur masyarakat umum. Indonesia telah mengantisipasi terjadinya perang siber, namun terdapat beberapa kelemahan yang belum dilaksanakan Indonesia seperti pembanguanan satelit sendiri, pembangunan komando pasukan khusus siber dan aturan perundang-undangan yang belum memadai terkait perang siber. dengan kelemahan ini maka dapat di anjurkan bahwa Indonesia masih rentan terhadap perang siber dan perlu pembenahan secara comprehensive dalam memperkuat basis kekuatan vital siber nasional.

Daftar Pustaka

Dr. J. Kallberg. “strategic syber war theory-a foundation for designing decisive strategic cyber operations,” the cyber defense review, VOl.1, No. 1, Army Cyber institute(spring 2016)

Ineu Rahmawati. Analisis Manajemen Risiko ancaman kejahatan siber (cyber crime) dalam peningkatan cyber defense” Jurnal Pertahanan dan Bela Negara.Volume 7 Nomor 2.Agustus 2017,

M. Badri. “Perang cyber dalam dinamika komunikasi Internasional.” Komunikasi Militer. (Diterbitkan kerjasama Buku Litera, Prodi Ilmu komunikasi, Universitas Prof. Dr. Moestopo (beragama) Jakarta dan Asosiasi Pendidikan Tinggi Ilmu Komunikasi/ASPIKOM Cet. Pertama Mata Padi Pressindo Juli 2012).

Nur Khalimatus Sa’diyah dan Ria Tri Vinata. Rekonstruksi pembentukan national cyber defence sebagai upaya mempertahankan kedaulatan negara. Perspektif Volume XXI No.3 Edisi September,, Tahun 2016.

JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021
E-ISSN 2615-07435

Agus Subagyo. “Sinergi dalam menghadapi ancaman cyber warfare”, Jurnal Pertahanan April 2015, Volume 5, nomor 1.

Handrini Ardiyanti. “ Cyber-security dan tantangan pengembangan di Indonesia” Politica Vol. 5 No.1 Juni 2014.

Amarmuazam Usmani Bin Othman. “Analisis penggunaan media siber terhadao keamanan nasional suatu studi di Malaysia. Jurnal Prodi strategi pertahanan darat Desember 2001/Volume 3/Nomor 3.

Hidayat Chusnul Chotimah Tatakelolah kemanaan siber Indonesia di bawah kelembagaan Badan Siber dan sandi Negara Politica Vol. 10 No. 2 November 2019

Letkol Chb. Ir. Bagus Artiadi Soewardi, M.,Si; perlunya pembangunan system pertahanan siber (cyber defense) yang tangguh bagi Indonesia, media informasi Ditjen Pothan Kemhan (2013;31-33),

Rika Isnarti “A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War (Andalas Journal of International Studies) Andalas 2016 Vol 5 No 2 November.

Richard A. Clarke and Robert K. Knake dalam tulisan berjudul “*Cyber War The Next Threat to National Security and What to Do About It*,” HarperCollinse-book (2010 -1-138).

Surat kabar

Sydney Morning Herald 31 Oktober