Jurnal Kewarganegaraan
Vol. 6 No. 1 Juni 2022
P-ISSN: 1978-0184 E-ISSN: 2723-2328

ANCAMAN SERANGAN SIBER PADA KEAMANAN NASIONAL INDONESIA

Tamarell Vimy[1], Surya Wiranto[2], Rudiyanto[3], Pujo Widodo[4], Panji Suwarno[5]
Program Studi Keamanan Maritim, Fakultas Keamanan Nasional, Universitas Pertahanan Republik Indonesia[1,2,3,4,5]
Email: tamarell.vimy@gmail.com[1] suryawiranto1@gmail.com[2] mazz.rudiyanto@gmail.com[3] suwarnopanji30@gmail.com[5]

Abstrak

Keamanan atas kepentingan nasional menjadi 'nyawa' dari suatu negara, menjadi hal yang dilindungi dan dipertahankan bagi setiap pihak. Ancaman, gangguan dan hambatan akan terasa apabila hal-hal tersebut diproyeksikan dapat mengganggu kepentingan nasional, yang kemudian negara dapat mempersepsikan bentuk-bentuk ancaman yang mengganggu keamanan nasional. Berangkat dari meningkatkan keamanan nasional, sebagai konsekuensinya setiap negara menggunakan deterrence dan balance of power untuk melindungi kepentingan nasional mereka. Dari beberapa ancaman yang dihadapi di Indonesia, ancaman serangan siber dianggap memiliki prioritas ancaman yang tinggi. Dalam analisi ini kami mencoba menggunakan pendekatan melalui teori lykke dengan membagi elemen-elemen dalam suatu formulasi strategi yaitu end, mean, dan ways, yang kemudian dirubah kedalam bentuk 4T mitigasi resiko untuk mengetahui prioritasnya. Kemudian akhirnya ditentukan strategi untuk meningkatkan keamanan nasional atas ancaman serangan siber.
Kata Kunci : Ancaman Siber, Keamanan Nasional, Kepentingan Nasional, *Cyber War*

Abstract

Security over the national interest becomes the 'life' of a country, it is something that is protected and maintained for each party. Threats, disturbances and obstacles will be felt if these things are projected to interfere with national interests, which then the state can perceive the forms of threats that interfere with national security. Departing from increasing national security, as a consequence each country uses deterrence and balance of power to protect their national interests. Of the several threats faced in Indonesia, the threat of cyber attacks or Cyber War is considered to have a high threat priority. In this analysis, we try to use an approach through Lykke's theory by dividing the elements in a strategy formulation, namely end, mean, and ways, which are then converted into the 4T form of risk mitigation to determine the priorities. Then finally a strategy was determined to improve national security against the threat of cyber attacks.
Keywords: *Cyber Threat, National Security, National Interest, Cyber War.*

PENDAHULUAN

Kemajuan zaman dimana orang-orang menggunakan teknologi dalam kehidupan sehari-hari dimulai dari komunikasi, transaksi online, berbelanja, edukasi, ekonomi, layanan kesehatan hingga semua keperluan lain kini dapat dengan mudah dikerjakan melalui internet. Perubahan yang signifikan dimulai dari cara-cara konvensional kini berubah menjadi serba menggunakan teknologi. Tahun 2017 penggunaan internet di seluruh dunia mencapai 50 persen dengan penduduk mencapai 7,4 miliar diikuti oleh pemakai internet lebih dari 3,7 miliar orang. Kebanyakan orang menggunakan internet karena kemudahan yang diberikan dan membuat mereka menghabiskan waktu untuk berselancar di dunia maya (*cyberspace*).

Dalam dunia internet, demi keamanan diperlukan untuk memasukan data privasi kita di internet namun bersamaan dengan hal tersebut terdapat ancaman yang merugikan kita jika

data kita kemudian digunakan atau dimanfaatkan untuk hal negatif oleh pihak tertentu yaitu digunakan untuk serangan siber.

Indonesia adalah negara yang termasuk target serangan siber dimana menurut Kominfo setiap tahunnya data yang dicuri mencapai jutaan identitas, selain itu Indonesia juga termasuk negara yang dijadikan target dalam serangan siber, Badan Siber dan Sandi Negara (BSSN) mempublikasikan laporan tahunan monitoring keamanan siber tahun 2021. Laporan ini dipublikasikan pada situs resmi milik Direktorat Operasi Keamanan Siber BSSN tepatnya pada Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center), dari laporan tersebut dapat terlihat bahwa lebih dari 1,6 miliar atau tepatnya adalah 1.637.973.022 anomali trafik atau serangan siber (*cyber attack*) yang terjadi di seluruh wilayah Indonesia pada tahun 2021.

Selain itu pula terjadi peretasan data yang kemudian data pribadi tersebut dijual di website tertentu, tentu hal ini sangat merugikan bagi kita. Pakar keamanan siber dari Cissrec, Pratama Persadha, mengatakan bahwa serangan siber dan ancaman peretasan ini terjadi berkali-kali dalam satu bulan, hal ini yang menyebabkan keamanan siber di Indonesia dalam tahap Red Alert atau tahap berbahaya.

Dapat dilihat bahwa serangan siber menjadi salah satu ancaman yang mengancam keamanan nasional, Keamanan nasional sendiri merupakan keamanan suatu negara sebagai satu kesatuan serta keamanan bagi manusia untuk menjalani kehidupan dalam suatu negara. Ancaman terhadap keamanan nasional yang terjadi saat ini bisa ada karena perubahan lingkungan yang dihadapi oleh seluruh negara pada sistem internasional.

Perubahan ini yang menjadikan isu keamanan menjadi semakin kompleks. Pada awalnya isu keamanan hanya berfokus terhadap perimbangan kekuasaan negara dalam segi kekuatan militer. Tetapi seiring berjalannya waktu aspek-aspek non militer juga dapat dikategorikan sebagai agenda khusus isu keamanan. Mulai terjadi perubahan ancaman yang awalnya bersifat tradisional (dengan kekuatan militer) lama kelamaan menjadi non-tradisional (meluas terhadap ekonomi, politik, sosial dan budaya). Perubahan ini didukung dengan perkembangan global yang pesat, sehingga memunculkan perubahan dalam bentuk ancaman dan peperangan.

Berdasarkan perubahan yang terjadi, pada ahli seringkali membagi ancaman menjadi dua, tradisional dan non tradisional. Tapi nyatanya, perkembangan dunia ini lagi-lagi memunculkan bentuk ancaman yang baru, salah satunya adalah hybrid. Dalam konteks ini, ancaman mulai memiliki sifat yang fluid atau multibentuk. Ada ancaman yang dikategorikan sebagai ancaman non-tradisional, tetapi dalam prakteknya berimplikasi terhadap ancaman militer. Sehingga, semakin berkembangnya zaman, semakin berkembangnya ancaman, semakin sulit juga menganalisis musuh dan ancaman. Sulitnya memetakan ancaman ini menjadi salah satu hambatan bagi aktor negara dalam menghadapi ancaman-ancaman yang bermunculan.

Ancaman baru seperti *Cyber War* atau perang Siber, saat ini telah menjadi ancaman nyata bagi suatu negara dimana ancaman modern ini tidak dapat dikategorisasi hanya sebatas militer dan non-militer saja. Perang saat ini tidak hanya dapat terjadi di dunia nyata saja melainkan dapat pula terjadi di dunia maya. Beberapa contoh perang atau serangan siber yang terjadi adalah Internet social engineering attacks, Network sniffers, Packet spoofing, Hijacking sessions, Automated probes and scans, GUI (Graphical User Interface) intruder tools, Automated widespread attacks, Widespread denialof- service attacks, Executable code attacks (against browsers), Techniques to analyse code with Vulnerabilities without source, Widespread attacks on DNS infrastructure, Widespread attacks using NNTP to distribute attack, “Stealth” and other advanced scanning techniques, Windows-based remote

controllable Trojans (Back Orifice), Email propagation of malicious code, Wide-scale Trojan distribution, Distributed attack tools, Distributed Denial of service (DDoS) attacks, Targeting of specific users, Antiforensic techniques, Wide-scale use of worms, dan Sophisticated command and control attacks. Serangan siber yang terjadi ini bahkan akan terus berkembang sesuai dengan kemajuan teknologi informasi yang semakin canggih.

Telah dilakukan penelitian sebelumnya berjudul Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional, yang dilakukan oleh Kolonel Inf Sugeng Santoso, S.I.P., yang berisi tentang cara memperkuat pertahanan siber Indonesia agar dapat meningkatkan ketahanan nasional, selain itu pada penelitian yang dilakukan oleh Diny Luthfah dalam penelitiannya yang berjudul Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia, menjelaskan bahwa pentingnya hukum internasional untuk mendapatkan pertanggung jawaban dari negara asal serangan siber, sehingga dengan aturan hukum yang ketat dapat berpengaruh pada keamanan nasional.

Perbedaan penelitian yang dilakukan saat ini dibanding penelitian-penelitian sebelumnya adalah kedua penelitian sebelumnya tidak spesifik membahas strategi pertahanan yang tepat guna menjaga keamanan nasional dari serangan siber berdasarkan pengelompokkan intensitas & prioritas ancaman yang dianalisa menggunakan pendekatan teori lykke dengan membagi elemen dalam suatu formulasi strategi yaitu end, mean, dan ways, yang kemudian dirubah kedalam bentuk 4T mitigasi resiko untuk mengetahui prioritasnya.

Indonesia sebagai negara berdaulat, saat ini dihadapkan oleh ancaman ini. Untuk memetakan kebijakan dan strategi guna menjaga keamanan nasional. Suatu negara mampu menilai suatu ancaman dengan berlandaskan kepentingan nasional yang dimilikinya. Apabila ditemukan suatu isu, peristiwa atau fenomena yang dinilai mengganggu kepentingan nasional maka akan dikategorikan sebagai ancaman.

Penelitian ini penting untuk dibahas karena dengan melakukan pemetaan ancaman ini, Indonesia mampu membentuk suatu kebijakan atau strategi yang dapat digunakan dalam menghadapi ancaman yang membahayakan keamanan nasional. Rumusan penelitian ini adalah bagaimana menjaga keamanan nasional dari ancaman serangan siber dan strategi pertahanan yang dapat dibentuk. Penelitian ini dilakukan dengan tujuan untuk mengetahui bagaimana strategi pertahanan yang tepat guna menjaga keamanan nasional dari serangan siber.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif, yang mana menurut Sugiyono (2016) metode penelitian kualitatif adalah metode penelitian yang digunakan untuk meneliti pada kondisi obyek yang alamiah dimana peneliti adalah sebagai instrumen kunci. Selanjutnya desain penelitian yang digunakan adalah Literature Review atau tinjauan pustaka. Penelitian kepustakaan atau kajian literatur (literature review, literature research) merupakan penelitian yang mengkaji atau meninjau secara kritis pengetahuan, gagasan, atau temuan yang terdapat di dalam tubuh literatur berorientasi akademik (academic-oriented literature), serta merumuskan kontribusi teoritis dan metodologisnya untuk topik tertentu, (Cooper, 2010).

Teknik pengumpulan data pada penelitian ini menggunakan studi literatur. Studi literatur sendiri adalah suatu cara untuk mengumpilkan data dan sumber yang berkaitan dengan hal yang diteliti dalam suatu penelitian. Setelah data yang dibutuhkan telah terkumpul selanjutnya dilakukan analisis deskriptif, yaitu proses penguraian terhadap data yang telah didapatkan, kemudian dijelaskan agar penjelasan dapat dipahami oleh pembaca.

HASIL PENELITIAN DAN PEMBAHASAN

Hasil Penelitian

Keamanan nasional dapat sangat bermanfaat didefinisikan sebagai kemampuan dari suatu bangsa untuk melindungi nilai-nilai internalnya dari ancaman pihak luar. Keamanan nasional bisa menjadi sebuah konsep yang digunakan untuk pemerintahan yang berkuasa dalam rangka mengamankan posisi atau status quonya. Keamanan nasional dapat didefinisikan sebagai suatu kondisi protektif yang para negarawan berusaha capai, atau jaga, dalam rangka mengamankan berbagai macam komponen politik dari ancaman dalam dan luar. Keamanan disini berarti usaha untuk mengurangi dampak dari ancaman atau bahaya, ancaman sendiri adalah sesuatu yang berpotensi mengganggu, menghalangi atau merusak nilai-nilai yang dianut atau dipercaya. Upaya keamanan biasanya dilakukan dengan perlindungan dimana ini berarti kita terlepas dari penghalang, terbebas untuk dapat melakukan sesuatu yang bernilai bagi kita. Hal ini menjadikan Kepentingan nasional menjadi keamanan dengan mengacu pada hasil bernilai yang diinginkan oleh mereka yang berada dalam basis efektif politik dalam suatu bangsa, nilai seperti itu biasanya diasosiasikan dengan konsep kepentingan nasional.

Buku Putih Pertahanan Indonesia Tahun 2015 (BPPI 2015) mendefinisikan ancaman nyata sebagai ancaman yang sering terjadi dan dihadapi setiap saat, dapat berasal dari dalam negeri maupun luar negeri yang dinilai membahayakan kedaulatan negara, keutuhan wilayah,dan keselamatan segenap bangsa. Ancamannya merupakan bentuk ancaman yang menjadi prioritas dalam penanganannya, yang diantaranya termasuk wabah penyakit. Ancaman besar atau nyata meliputi ancaman teroris, *Cyber War*, penyakit menular, bencana alam, wabah penyakit, pelanggaran wilayah, pencurian sumber daya alam, pemberontakan separatis dan narkoba. Konsep tersebut diungkapkan Menhan Ryamizard Ryacudu dihadapan wartawan media cetak dan elektronik dalam forum silaturahmi antara Menhan dengan wartawan, Selasa (26/5), di kantor Kemhan Jakarta.

Terdapat hubungan yang saling terkait antara ancaman dengan kepentingan nasional. Menurut Samuel Huntington, kepentingan nasional suatu negara dapat terbentuk karena ada pihak lain yang mengancam nilai-nilai kehidupan suatu bangsa. Pada hakikatnya, manusia akan membentuk suatu batas antara 'us and the others' (kami dan mereka) secara alamiah. Hakikat individu ini lama kelamaan dapat membentuk identitas suatu bangsa, termasuk menentukan nilai-nilai apa yang bertentangan dengan mereka. Pihak yang berbeda dengan mereka ini dikategorikan sebagai musuh atau ancaman. Dalam hal ini ditemukan bahwa terbentuknya kepentingan nasional berdasar pada ancaman yang dihadapi. Berdasarkan dari sejarah yang dialami oleh Amerika Serikat, hal ini dijadikan kesimpulan oleh Huntington, bahwa kepentingan nasional dapat digunakan sebagai standar bagi negara untuk menentukan ancaman.

Indonesia memiliki kepentingan nasional yang menjadi landasan terbentuknya kebijakan dan strategi. Dengan itu, Indonesia menjadikan Pembukaan Undang-Undang Dasar 1945 alinea IV yang didalamnya terkandung kepentingan nasional Indonesia, yang pertama meliputi "Melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia.", kedua "Memajukan kesejahteraan umum". Ketiga "Mencerdaskan kehidupan bangsa". Dan keempat ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial Keempat butir ini mampu dijadikan landasan setiap kebijakan serta strategi yang dibentuk oleh pemerintah. Perlindungan atas segenap bangsa menjadi kepentingan nasional yang sangat penting. Menurut Morgenthau, setiap negara harus melindungi teritorial bersamaan dengan politik untuk berhadapan dengan negara lain.

Pembahasan

Di dunia yang terdiri dari banyak negara yang bersaing dan menentang untuk mendapatkan kekuasaan, kelangsungan hidup mereka adalah syarat mutlak dan minimum mereka. Dengan demikian semua negara melakukan apa yang tidak bisa tidak mereka lakukan: melindungi identitas fisik, politik, dan budaya mereka dari perambahan oleh negara lain, kepentingan nasional dasar dapat digambarkan sebagai berikut:

- Kepentingan pertahanan: perlindungan negara-bangsa dan warganya terhadap ancaman kekerasan fisik yang diarahkan dari negara lain, dan / atau ancaman yang diilhami secara eksternal terhadap sistem pemerintahannya.
- Kepentingan ekonomi: peningkatan kesejahteraan ekonomi negara-bangsa dalam hubungannya dengan negara-negara lain.
- Kepentingan Tatanan Dunia: pemeliharaan sistem politik dan ekonomi internasional di mana negara-bangsa dapat merasa aman, dan di mana warga dan perdagangannya dapat beroperasi secara damai di luar perbatasannya.
- Kepentingan ideologis: perlindungan dan kelanjutan dari seperangkat nilai yang dimiliki dan dipercayai oleh orang-orang dari negara-bangsa secara universal.

Pola untuk menguasai suatu negara tidak lagi dilakukan secara frontal atau melalui perang konvensional militer dengan senjata, karena adanya hukum-hukum dan organisasi dunia, sehingga dilakukan dengan cara-cara nonlinier, tidak langsung, dan bersifat proxy war. Ancaman pertahanan dan keamanan negara saat ini cenderung mengarah pada sifat-sifat perang tanpa menggunakan senjata atau nir-militer. Perang dilakukan secara semu (pseudo) sehingga siapapun yang mempunyai kepentingan strategis dalam perang tersebut tetap tidak terlibat secara langsung, atau bahkan tidak diketahui sama sekali. Paradigma keamanan nasional telah bergeser kepada aspek yang lebih luas yaitu termasuk jaminan keamanan pribadi warga negara. Kewajiban pokok dari suatu negara adalah memberikan keamanan terhadap warganyanya tersebut termasuk keamanan dari berbagai kejahatan siber.

Memahami tipikal ancaman seperti ini dibutuhkan pendekatan strategi yang berbeda. Tren menguasai suatu negara dengan menggunakan ‘senjata’ asimetris yang dibangun secara sistematis. Penciptaan kondisi lewat propaganda dilakukan dengan memanfaatkan kemajuan teknologi informasi dan ruang siber seperti media sosial, perang siber telah menjadi strategi untuk menimbulkan kerugian yang berdampak strategis terhadap suatu negara. Pola devide et impera atau memecahbelah komponen-komponen bangsa dalam negeri merupakan cara yang efektif untuk menghancurkan suatu negara, konflik yang dapat memicu gerakan separatis karena kepentingan politik dan wilayah, termasuk konflik sosial yang terjadi di beberapa negara dengan dilatarbelakangi dinamika sosial, budaya, primordialisme, suku, ras, dan agama.

Cyber War atau serangan siber sendiri menjadi ancaman nyata yang dihadapi Indonesia seiring berjalannya zaman serta globalisasi yang membuat informasi lebih mudah didapat, dan jika tidak diproteksi akan mengancam keamanan, dengan penggunaan teknologi juga membuat adanya tindakan illegal seperti hacking, pencurian data, penjualan data pribadi yang rahasia, pembajakan akun, penyebaran virus atau malware yang dimasukkan ke dalam suatu file dan website yang berbahaya bila di klik, data-data penting/rahasia yang diambil alih untuk disalahgunakan, upaya fitnah, penistaan maupun pencemaran nama baik, selain itu juga adanya penyerangan jaringan komputer dari negara lain. Serangan siber ini juga rawan ancaman terorisme, yang melakukan peretasan sistem pemerintah, penghancuran data, dan pencurian informasi.

Cyber crime dan *Cyber War* tidak hanya menjadi ancaman yang menyerang individu saja melainkan juga ancaman terhadap bidang bisnis dan industri serta objek vital pemerintahan. Pembuatan opini publik dan dunia internasional terhadap suatu maksud seperti untuk kampanye hingga propaganda. Dengan adanya teknologi informasi dan internet para pelaku ini dapat melakukannya dengan cara mudah, menggunakan biaya dan sumber daya yang lebih efisien. Kejadian terkait serangan siber adalah upaya spionase pada bidang industri dan objek vital pemerintah seperti penyanderaan dan perusakan informasi rahasia yang penting dapat menimbulkan rasa khawatir dan tidak aman karena kehilangan batas-batas pribadi dan ancaman kehilangan aset serta kekayaan. Tidak hanya itu jika upaya serangan siber ini terjadi maka dapat dimanfaatkan untuk kepentingan politik dunia siber juga dapat digunakan sebagai alat politik seperti penyebaran berita hoax dengan tujuan provokasi politis hingga rekayasa pada sektor perekonomian. Interkoneksi internet juga memungkinkan terjadinya serangan yang bertujuan melumpuhkan dan menghancurkan sumber daya negara lawan tanpa perlu mendekati objek tersebut.

Era globalisasi dimana keterkaitan dan ketergantungan antar bangsa dan antar manusia di seluruh dunia melalui perdagangan, investasi, perjalanan, budaya populer, dan bentuk-bentuk interaksi yang lain sehingga batas-batas suatu negara menjadi semakin sempit. Semua orang di dunia sudah dapat saling terhubung, orang-orang di dunia dapat saling berbicara, mengobrol, saling terhubung satu dengan yang lain karena adanya kemajuan teknologi. Ohmae (1990) menyatakan ini sebagai the bordeless world atau yang dikenal sebagai dunia tanpa batas. Hal ini memungkinkan dunia nyata yang terbatas karena terpisah negara-negara yang berbeda, dapat menjadi satu tempat, satu dunia yang sama karena pengaruh teknologi dan globalisasi, tentu akan membuat ideologi-ideologi berbahaya, budaya-budaya asing yang bukan budaya Indonesia, ajaran-ajaran menyesatkan, dan berbagai ancaman terhadap ideologi bangsa sehingga kesatuan dan persatuan Indonesia dapat menjadi taruhannya.

Dari aspek pertahanan, ruang siber telah menjadi domain kelima yang dapat dijadikan sebagai medan peperangan, selain medan perang darat, laut, udara dan ruang angkasa, karena penggunaan sistem, peralatan, dan platform berbasis internet cenderung semakin meluas yang berpotensi menjadi kerawanan. PBB (Perserikatan Bangsa-Bangsa) pun sudah mengeluarkan keputusan Nomor 55/63, yang berisi bahwa telah disepakati bahwa semua negara harus bekerja sama untuk mengantisipasi dan memerangi kejahatan yang menyalahgunakan teknologi informasi. Poin yang penting dalam keputusan ini adalah setiap negara harus memiliki undang-undang atau peraturan hukum yang mampu untuk mengeliminasi kejahatan siber tersebut. Berkembangnya dunia ini sangat cepat dan dinamis diperlukan kesiapan dan strategi pertahanan negara untuk mengantisipasinya sehingga dapat tercipta keamanan dalam menghadapi ancaman dalam kehidupan berbangsa dan bernegara.

Dalam analisa ini peneliti mencoba menggunakan pendekatan melalui teori lykke dengan membagi elemen-elemen dalam suatu formulasi strategi yaitu end, mean, dan ways, yang kemudian dirubah kedalam bentuk 4T mitigasi resiko untuk mengetahui prioritasnya. 4T yaitu:

1. Tolerate (Accept/retain): bahaya mungkin dapat ditoleransi tanpa ada tindakan lebih lanjut yang diambil. Sekalipun tidak dapat ditoleransi, kemampuan untuk melakukan sesuatu terhadap beberapa risiko mungkin terbatas, atau biaya untuk mengambil tindakan apa pun mungkin tidak sebanding dengan potensi manfaat yang diperoleh. Saya beri nilai 4, karena tingkat resiko masih bisa ditoleransi.
2. Treat (Control/reduce): Sejauh ini, semakin banyak risiko yang akan ditangani dengan cara ini. Tujuan perlakuan adalah bahwa, sementara terus dalam organisasi dengan aktivitas yang menimbulkan risiko, tindakan (pengendalian) diambil untuk membatasi risiko ke

tingkat yang dapat diterima.Saya beri nilai 3 karena resiko masih dalam tahap pengendalian.

3. Transfer (Insurance/contract): Untuk beberapa risiko, respons terbaik mungkin adalah mentransfernya. Ini mungkin dilakukan dengan asuransi konvensional, atau mungkin dilakukan dengan membayar pihak ketiga untuk mengambil risiko dengan cara lain. Opsi ini sangat baik untuk mengurangi risiko terhadap aset. Saya beri nilai 2 karena membutuhkan kewenangan tingkat atas.
4. Terminate (Avoid/eliminate): Beberapa risiko hanya akan dapat diobati, atau dapat ditahan hingga tingkat yang dapat diterima, dengan menghentikan aktivitas. Saya beri nilai 1 karena beresiko tinggi.

Untuk *Cyber War* atau serangan siber ini sendiri dapat diuraikan sebagai berikut:

Tabel 1. Bentuk *Cyber War*

BENTUK	MEAN	WAYS	END	BOBOT	PRIOR
*Cyber Ware*fare	-Banyak hacker dan cracker Indonesia -Militer dengan pengetahuan IT masih terbatas	- Tim cyber Polri Tim Cyber TNI	-Mencegah pencurian data objek vital negara -Mencegah pelumpuhan fasilitas publik	Treat	3

Dari analisis yang telah dilakukan diatas maka, strategi yang dapat diambil diantaranya adalah melakukan kerjasama dengan negara lain dalam rangka membangun keamanan global. Pemerintah harus mulai membentuk kesadaran akan ancaman dari perang siber ini dan mulai memperbanyak ahli yang memahami soal keamanan dan pertahanan di sektor siber ini sehingga dapat dibentuk sistem keamanan yang terbaik oleh orang-orang yang kompeten. Dengan adanya ahli siber, pemahaman pemerintah ditambah kerjasama dengan negara lain kemudian dapat diimplementasikan kedalam bentuk regulasi, kebijakan dan aturan mengenai keamanan siber (cyber law) yang lebih kuat dan memberikan pengaruh secara global. Diperlukan kesadaran pihak-pihak untuk mengkaji lebih jauh tentang topik siber ini ke diskusi politis hingga kemudian dibuat undang-undang spesifik yang mengatur tentang ancaman siber. Selain itu para komponen utama seperti TNI dan Polri harus diperbanyak jajaran yang memahami dan ahli di bidang IT untuk mencegah potensi *Cyber War*efare yang dapat menyerang keamanan nasional Indonesia.

Banyaknya serangan ke sistem informasi Indonesia adalah karena kesadaran akan ancaman siber dan regulasi atau aturan belum kuat di Indonesia, hal ini karena para penentu kebijakan masih awam terhadap informasi terkait siber. Dimana tata kelola manajemen keamanan siber juga masih dibilang lemah, yang harusnya ketika timbul ancaman, tim IT langsung tanggap dan langsung melakukan upaya pertahanan pada situs-stu yang berisi data penting dengan cara pengecekan, menghubungi lembaga ahli seperti BSSN dan lebih jauh dengan melakukan takedown sementara sehingga tidak menimbulka kebocoran data ke internet.

Kurangnya pengetahuan tentang siber dan ancamannya dapat mulai dipelajari dan dipahami bersama-sama, mulai dari usia sekolah, dapat pula diadakan kunjungan ke sekolah sekolah untuk mengenalkan bidang siber dan ancaman serta menghadapinya, selain itu mengadakan seminar atau pameran terkait siber, juga diklat diklat kepada para pekerja tentang ancaman yang mungkin terjadi berhubungan dengan siber. Hal ini dilakukan dengan

tujuan menambah kesadaran serta ketertarikan publik akan ancaman siber dan kemungkinan *Cyber War*, sehingga dikemudian hari akan bertambah pula ahli-ahli yang berkecimpung di bidang siber dan memperkuat upaya pertahanan negara dan keamanan nasional.

KESIMPULAN

Indonesia tidak hanya menghadapi ancaman tradisional ataupun non-tradisional, isu pertahanan berada pada tahap yang semakin kompleks dengan kemunculan ancaman yang baru. Dapat disimpulkan bahwa medan pertempuran yang dimiliki Indonesia saat ini terdiri dari darat, laut, udara, luar angkasa dan cyber space. Indonesia saat ini tidak lepas dari ancaman terutama ancaman yang berbentuk *hybrid*. Kompleksitas ancaman yang terus berkombinasi dan bersinergi terutaman terkait ancaman serangan siber, tentunya mengharuskan Indonesia menguatkan pertahanan dalam bentuk pembuatan kebijakan dan undang-undang, sinergitas stakeholder terkait, serta menambah orang orang ahli yang kompeten di bidang siber, dan juga upaya pengenalan melalui seminar kepada masyarakat umum dan pengenalan pada anak-anak sekolah untuk menambah kesadaran akan pentingnya hal ini yang kemudian berimplikasi pada meningkatnya ketertarikan publik akan ancaman siber dan kemungkinan *Cyber War*.

Upaya Gap-gap yang muncul tentu harus ditutupi dengan membuat kelembagaan analisis dan juga memberikan saran masukan terkait objek vital negara. Kerjasama dalam bidang intelijen dan juga antar negara perlu di tingkatkan dengan menggalang masyarakat sebagai sumber informasi dan pelaksana kekuatan pertahanan semesta. Dan dengan upaya yang maksimal diharapkan dalam jangka panjang, Indonesia menjadi negara yang aman dari ancaman siber, memiliki sistem pertahanan siber yang kuat dan memiliki banyak ahli yang kompeten di sektor pertahanan siber.

DAFTAR PUSTAKA

Abdul Aziz. (2016). Memperkuat Kebijakan Negara Dalam Penanggulangan Radikalisme Di Lembaga Pendidikan. HIKMAH Journal of Islamic Studies XII, no. 1 (2016): 29– 56. Retrieved from http://journal.alhikmahjkt.ac.id/index.php/HIKMA H/article/view/55, hlm. 33.

Aitsi-Selmi, A., & Murray, V. (2015). The Sendai framework: Disaster risk reduction through a health lens. Bulletin of the World Health Organization, 93(6), 362. https://doi.org/10.2471/BLT.15.157362.

Amaritasari, Indah. (2015). Keamanan Nasional dalam Konsep dan Standar Internasional. Jurnal Keamanan Nasional Vol. I No. 2 2015.

Artiadi Soewardi, Bagus. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. Media Informasi Ditjen Pothan Kemhan.

Badan Siber dan Sandi Negara (BSSN). (2021). Laporan Tahunan Monitoring Keamanan Siber 2021 retrieved from https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw

Berkowitz, Morton, and Bock, P.G. (1965). eds. American National Security. New York: Free Press.

Buku Putih Pertahanan Indonesia 2015. (2015). Jakarta: Kementerian Pertahanan Republik Indonesia.

Cambridge University, Cambridge Advanced Learners Dictionary. (2008). Singapore: Cambridge University Press. hlm. 1170.

Cohen, Ira S., and Tuttle, Andrew C. (1972). National Security Affairs: A Syllabus.

Eufronius Marianus Suwarman, dkk. 2018. Rivalitas Geopolitik Amerika Serikat – Tiongkok Di Myanmar. Jurnal Asia Pacific Studies Volume 2 Number 2 http://dx.doi.org/10.33541/japs.v3i1.1071.

Fauzi, A., Hunainah, & Humedi. (2020). Menyimak Fenomena Tsunami Selat Sunda. Geografi Dan Pengajarannya, 18, 44. https://doi.org/10.26740/jggp.v18n1.p43-62.

Indrajit, R. E. (2020). Filsafat Ilmu Pertahanan dan Konstelasinya dalam Kehidupan Berbangsa dan Bernegara. Jurnal Kebangsaan, 1(1), 54–63.

Informasi Letusan. (2022). Magma Indonesia Retrieved from https://magma.esdm.go.id/v1/gunung-api/informasi-letusan?page=2

Kamus Besar Bahasa Indonesia. (2008). Pusat Bahasa Kementerian Pendidikan Nasional. Gramedia.

Kemhan. (2015). Konsep Pertahanan Indonesia Didasarkan pada Ancaman Nyata dan Tidak Nyata. https://www.kemhan.go.id/2015/05/27/konsep-pertahanan-indonesia-didasarkan-pada-ancaman-nyata-dan-tidak-nyata.html (Diakses tanggal 22 April 2022).

Luthfah, Diny. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (*Cyber attack*s as the Use of Force in the Perspective of Indonesia National Security Law). terAs Law Review : Jurnal Hukum Humaniter dan HAM. 3. 11. 10.25105/teras-lrev.v3i1.10742.

Marco V. (2012). Barahona Fuentes; A Threat to National Security. https://doi.org/10.21236/ada560682.

Nur Azizah. (2017). Empat Indikator Warga Terpapar Radikalisme. Medcom.Id, last modified 2017, accessed January 24, 2022, https://www.medcom.id/nasional/peristiwa/ybDRGJPK-empat-indikator-warga-terpaparradikalisme.

Nurhaidah, M. Insya Musa. (2015). Dampak Pengaruh Globalisasi Bagi Kehidupan Bangsa Indonesia. Jurnal Pesona Dasar Retrieved from http://jurnal.unsyiah.ac.id/PEAR/article/view/7506/6178#.

Ohmae, K. (1990). The Bordeless Word: Power and Strategy in Interlinked World Economy. New York: Harbet Business.

Priadi, R., Wijaya, A., Pasaribu, M. A., & Yulinda, R. (2019). Analysis of the Donggala-Palu Tsunami Characteristics based on Rupture Duration (Tdur) and Active Fault Orientation using the HC-plot Method. Jurnal Geofisika, 17(1), 16. https://doi.org/10.36435/jgf.v17i1.392.

Samuel Huntington, The Erosion of America Nat. Interest.

Santoso, Sugeng. (2018). Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional. Jurnal Kajian Lemhannas RI Edisi 34 retrieved from https://jurnal.lemhannas.go.id/index.php/jkl/article/download/120/42/.

Sefriani. (2003). Separatisme dalam Perspektif Hukum Internasional: Studi Kasus Organisasi Papua Merdeka. UNISIA NO. 47/XXVI/I/2003

Wardyaningrum, D. (2014). Perubahan Komunikasi Masyarakat Dalam Inovasi Mitigasi Bencana di Wilayah Rawan Bencana Gunung Merapi. Jurnal ASPIKOM, 2(3), 179. https://doi.org/10.24329/aspikom.v2i3.69

Wayan Partiana. (1990). Pengantar Hukum Internasional. Bandung: Mandar Maju.