Utilization of The Semesta Defense Concept in Facing Siber Attacks During The Covid-19 Pandemic in Indonesia

Aththaariq Rizki
Program Studi Peperangan Asimetris, Fakultas Strategi Perang, Universitas Pertahanan Republik Indonesia, Kawasan IPSC Sentul, Bogor, Indonesia
erikatorik@gmail.com

Abstract

This study argues that currently the threat of cyber attacks has become a real threat that has the potential to grow during the Covid-19 pandemic. The concept of a universal defense system can be used as strategy to deal with cyber threats. This research using a qualitative method with a literature review approach that focuses on the threat of cyber attacks in Indonesia during the Covid-19 pandemic. The purpose of this study is to find out how the threat of cyber attacks in Indonesia during the Covid-19 pandemic is, and how the concept of a universal defense system can handle it. The theory used is concept of threats, cyber attacks, and universal defense systems as a literature review. This study, was found that the threat of cyber attacks during the Covid-19 pandemic has increased and is growing, besides that the use of the universal defense concept is considered capable of dealing with the escalation of existing cyber threats. So it can be concluded from this study that the threat of cyber attacks in Indonesia during the Covid-19 pandemic is increasing and the use of the concept of a universal defense system is considered capable of tackling these cyber threats.
Keywords: *Defense, Universe, Cyber, Attack, Covid-19*

Abstrak

Penelitian ini mengajukan argumen bahwa saat ini ancaman serangan siber telah menjadi ancaman nyata yang berpotensi untuk semakin berkembang selama masa pandemi Covid-19. Dengan hadirnya kebijakan Pembatasan Sosial Berskala Besar dan sistem kerja Work From Home. Kondisi inilah yang dimanfaatkan oleh aktor non pemerintah untuk melakukan aksi penyerangan melalui cyberspace. Untuk menangani permasalahan tersebut, konsep sistem pertahanan semesta bisa dijadikan sebagai alternatif strategi untuk menghadapi ancaman siber yang ada. Riset ini dilakukan dengan menggunakan metode kualitatif dengan pendekatan literatur review yang berfokus pada ancaman serangan siber di Indonesia selama masa pandemi Covid-19. Tujuan dari penelitian ini adalah untuk mengetahui bagaimana ancaman serangan siber di Indonesia selama masa pandemi Covid-19, serta bagaimana konsep sistem pertahanan semesta dapat menanganinya. Adapun teori yang digunakan adalah konsep ancaman, serangan siber, dan sistem pertahanan semesta sebagai tinjauan pustaka. Di dalam penelitian ini didapatkan hasil bahwa ancaman serangan siber selama masa pandemi Covid-19 mengalami peningkatan dan semakin berkembang, selain itu pemanfaatan konsep pertahanan semesta dinilai mampu untuk menghadapi eskalasi ancaman siber yang ada. Sehingga bisa diambil kesimpulan dari penelitian ini bahwa ancaman serangan siber di Indonesia selama masa pandemi Covid-19 semakin meningkat dan penggunaan konsep sistem pertahanan semesta dinilai mampu untuk menanggulangi ancaman siber tersebut.
Kata kunci: Pertahanan, Semesta, Siber, Serangan, Covid-19

PENDAHULUAN

Perkembangan teknologi di dunia saat ini berkembang sangat pesat. Mulai dari kegiatan sehari-hari sampai dengan kegiatan profesional memanfaatkan teknologi dalam aktivitasnya. Namun selain memberikan keuntungan, adanya perkembangan teknologi juga bisa memberikan dampak negatif terhadap manusia. Salah satu ancaman berbasis teknologi yang sedang marak dilakukan adalah ancaman siber (*cyber threat*). Ancaman siber menjadi suatu tantangan serta permasalahan baru yang harus di hadapi oleh pemerintah. Terlebih saat ini

dunia dan Indonesia tengah menghadapi wabah pandemi Covid-19.

Menurut BSSN (2020), selama masa pandemi Covid-19 ini, banyak cyber threat actor yang memanfaatkan kelengahan berbagai pihak untuk mencari keuntungan. Saat ini banyak threat actor yang sengaja memanfaatkan rasa penasaran dan antusiasme masyarakat dalam memenuhi kebutuhan informasi mengenai Covid-19. Threat actor memanfaatkan isu Covid-19 sebagai pembuka jalan untuk melakukan penyerangan terhadap infrastruktur TI melalui penyebaran malware, virus, ransomware serta spam email. Sehingga hal tersebut menyebabkan peluang ancaman pencurian data sensitif atau insiden siber lainnya menjadi lebih besar. Terlebih banyak masyarakat yang saat ini mengalihkan pekerjaanya kedalam sistem digital atau work from home.

Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) (2020), juga mencatat bahwa terdapat 88.414.296 serangan siber telah terjadi sejak 1 Januari hingga 12 April 2020 selama masa pandemi Covid-19. Menurut BSSN Mekanisme work from home bisa memperbesar potensi risiko terjadinya serangan siber.

Untuk menghadapi ancaman siber tersebut, Pemerintah Indoneisa dapat memanfaatkan konsep sistem pertahanan semesta kedalam sistem pertahan siber Indonesia. Dalam pasal 30 UUD 1945 dijelaskan bahwa sishankamrata adalah sebuah doktrin dan sekaligus strategi pertahanan negara Republik Indonesia yang menggunakan segenap kekuatan dan kemampuan komponen militer dan non militer secara menyeluruh dan terpadu.

Berdasarkan Lampiran Keputusan Panglima TNI Nomor Kep/666/VI/2018 tentang Doktrin TNI Tri Dharma Eka Karma, konsepsi mengenai pertahanan negara pada hakekatnya merupakan segala upaya pertahanan negara yang bersifat semesta, yang mana penyelenggaraanya didasarkan pada kesadaran akan hak dan kewajiban seluruh warga negara, serta keyakinan akan kekuatan sendiri untuk mempertahankan kelangsungan hidup bangsa dan negara Indonesia yang bersatu berdaulat dan merdeka.

Menurut Kementerian Pertahanan (2015), didalam sistem pertahanan nirmiliter Indonesia, postur pertahanan negara Indonesia terdiri atas unsur utama terkait yang berasal dari Kementerian atau Lembaga diluar bidang pertahanan. Selain itu, unsur utama akan didukung oleh unsur lain penguat bangsa yang berasal dari Kementerian, Lembaga atau Pemerintah Daerah lain.

Disi lain, Oona (2012), serangan siber adalah serangan dalam dunia maya, baik yang ditujukan untuk menyerang ataupun bertahan yang diharapkan dapat sebagai penyebab kematian seseorang atau kerusakan suatu objek yang dituju. Sedangkan Subagyo (2015), menjelaskan serangan siber dapat di bagi dan dieskalasikan menjadi ancaman siber, kejahatan siber, dan perang siber.

Untuk mewujudkan pertahanan semesta di bidang nirmiliter terutama bidang pertahanan siber, Pemerintah melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN), Pemerintah membentuk BSSN yang bertugas sebagai unsur kekuatan utama pertahanan negara dibidang siber yang memiliki tugas untuk

melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan ikut serta mengkosolidasikan semua unsur yang terkait dengan keamanan siber nasional. BSSN sebagai unsur utama pertahanan siber dalam melaksanakan tugasnya tidak bergerak sendirian. Sesuai dengan konsep perang semesta ada berapa instansi dan lembaga yang saling beririsan dan bersinergi dalam melakukan kewajibannya sebagai unsur lain penguat bangsa sesuai dengan prinsip perang semesta.

Sehingga berdasarkan ulasan latar belakang diatas, didapatkan dua rumusan masalah yakni:

(1) Bagaimana ancaman siber selama masa pandemi Covid-19 di Indonesia?

(2) Bagaimana pemanfaatan konsep sistem pertahanan semesta dalam menghadapi ancaman serangan siber selama pandemi covid-19?

Berdasarkan rumusan tersebut, dapat ditentukan tujuan penelitian ini adalah untuk mengetahui bagaimana ancaman siber selama masa pandemi Covid-19 di Indonesia, serta mengetahui bagaimana pemanfaatan konsep sistem pertahanan semesta dalam menghadapi ancaman serangan siber selama pandemi covid-19.

METODE PENELITIAN

Dalam penulisan tulisan ilmiah ini, penulis menggunakan metode penelitian kualitatif dengan pendekatan tinjauan kepustakaan (*literature review).* Menurut Creswell (2013), tinjauan kepustakaan adalah pendekatan penelitian yang didasarkan pada *non-numeric* data yaitu dapat berupa tulisan dan gambar, dan penyaringan terhadap data dilakukan untuk membuat interpretasi dari tinjauan pustaka (*literature review).* Kajian penelitian ini dilakukan melalui sumber literatur seperti jurnal, buku, tesis, *research report*, maupun artikel ilmiah dengan sumber yang valid dan *realible*.

HASIL DAN PEMBAHASAN

Ancaman serangan siber selama masa pandemi covid-19 di Indonesia

Berdasarkan hasil pemberitaan Zakia dalam Kompas (2020), diketahui bahwa selama pandemi covid-19, kejahatan siber di Indonesia naik empat kali lipat. Angka terbanyak untuk kasus serangan siber terjadi pada Agustus 2020, di mana tercatat ada 63 juta serangan siber di Indonesia, angka ini jauh lebih tinggi dibandingkan Agustus 2019 yang hanya di kisaran 5 juta.

Menurut Kepala Badan Siber dan Sandi Negara (BSSN), Letjen TNI (Purn) Hinsa Siburian dalam Beritasatu (2021), Peningkatan aktivitas digital saat pandemi Covid-19 berbanding lurus dengan bertambahnya serangan siber hampir seluruh dunia, termasuk Indonesia. Ancaman dan risiko serangan siber naik seiring banyaknya pengguna internet dan aktivitas digital masyarakat. Pada beberapa kasus di era pandemi, *threat actor* terus meningkatkan serangan, termasuk memanfaatkan isu Covid-19.

Selain itu, dikutip dalam Tirto.id (2020), saat ini di Indonesia, disinformasi terkait Covid-19 menjadi kasus yang diperhatikan khusus oleh Kementrian Komunikasi dan Informatika (Kemkominfo). Hingga 5 Mei 2020, Tim AIS Direktorat Jendral Aplikasi Informatika (Aptika) mengklaim telah berhasil mengidentifikasi 1.401 konten hoaks dan disinformasi terkait COVID-19. Lebih lanjut dalam siaran persnya, Kemkominfo menjelaskan mayoritas konten hoaks

merajalela di Facebook yang berjumlah 999, disusul Twitter dengan 375 unggahan hoaks.

Berdasar data dari *ASEAN Cyberthreat Assessment* 2020 dalam Tirto.Id (2020), Indonesia menjadi target serangan phishing tertinggi di ASEAN pada 2019. Indonesia dilaporkan memiliki PDB gabungan lebih dari 2,7 triliun dolar AS dan diperkirakan akan mencapai 4 triliun dolar AS pada 2022.

Perusahaan teknologi IBM dalam Prasetya (2020), menjelaskan bahwa serangan siber secara global meningkat pada tiga bulan terakhir sejak pandemi virus Covid-19 di berbagai negara. Catatan internal IBM menunjukkan secara global terdapat kenaikan serangan siber hingga 6.000 persen dalam tiga bulan terakhir, adapun peningkatan kasus serangan siber di Indonesia antara lain terjadi pada situs dagang *online*.

Sehingga berdasarkan data diatas, dapat disimpulkan bahwa disaat masa pandemi Covid-19, serangan siber di Indonesia mengalami peningkatan yang cukup signifikan.

Unsur utama dan unsur lain penguat pertahanan siber di Indonesia

Berdasarkan Buku Putih Pertahanan Indonesia (2015), didalam menghadapi ancaman nirmiliter, sistem pertahanan semesta Indonesia menggunakan kekuatan unsur utama dan unsur lain pendukung pertahanan dari K/L yang terlibat dengan ancaman militer yang ada. Adapun unsur utama dan unsur lain penguat pertahanan di bidang siber antara lain:

Unsur Utama

Menurut Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN), saat ini BSSN adalah unsur utama yang menjadi leading sector dibidang pertahanan siber negara Indonesia. BSSN adalah salah satu badan pemerintahan non kementerian yang memiliki tujuan utama untuk melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan ikut serta mengonsolidasikan semua unsur yang terkait dengan keamanan siber nasional. BSSN memiliki wewenang untuk menyusun Strategi Keamanan Siber Indonesia sebagai acuan bersama seluruh pemangku kepentingan keamanan siber nasional.

Unsur Lain Penguat Pertahanan

Menurut Siagian (2018) unsur lain penguat pertahanan siber di Indonesia tersusun atas tiga instansi pemerintah yakni KOMINFO, Puskom KEMHAN, dan Pusinfolahta Mabes TNI. Sedangkan menurut Subagyo (2015), instansi siber POLRI juga menjadi salah satu unsur lain penguat sistem pertahanan siber Indonesia. Oleh karena peneliti simpulkan bahwa terdapat empat institusi negara yang memiliki peran sebagai unsur lain penguat pertahanan siber di Indonesia. Adapun penjelasan unsur lain pendukung sistem pertahanan siber di Indonesia antara lain:

Kementerian Komunikasi dan Informatika RI

Dikutip dari website resmi Kominfo (2021), sesuai Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara, Kementerian Kominfo adalah instansi dan perangkat Pemerintah Republik Indonesia yang membidangi urusan dengan wilayah ruang lingkup sesuai dengan yang disebutkan dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yaitu informasi dan komunikasi.

Kementerian Komunikasi dan Informatika memiliki tugas utama untuk menyelenggarakan urusan-urusan

pemerintahan di bidang komunikasi dan informatika dalam rangka membantu Presiden dalam menyelenggarakan pemerintahan negara. Didalam sistem pertahanan siber, Indonesia, Kominfo memliki peran membuat kebijakan, melakukan pemblokiran situs, serta melakukan sosialisasi digital terhadap masyarakat Indonesia.

Puskom Kemhan

Dikutip dari halaman resmi Puskom Kemhan (2021), Puskom Kemhan adalah salah satu fungsi pendukung dalam kementerian pertahanan di bidang komunikasi dan informasi. Berdasarkan Peraturan Menteri Pertahanan Republik Indonesia Nomor 58 Tahun 2014 Puskom Kemhan RI atau Pusat Komunikasi Publik adalah sebuah unsur pendukung pelaksana tugas dan fungsi pertahanan berada dibawah dan bertanggung jawab kepada Menteri. Puskom Kemhan dapat berperan untuk membantu BSSN menyusun strategi pertahanan siber negara, maupun membantu dalam mengatasi ancaman perang siber.

Pusinfolahta Mabes TNI

Berdasarkan halaman resmi Pusinfolahta (2021), dijelaskan bahwa Pusat Informasi dan Pengolahan Data TNI (Pusinfolahta TNI) dibentuk berdasarkan Keputusan Panglima TNI Nomor Kep/7/XII/2006 tanggal 5 Desember 2006 sebagai Badan Pelaksana Pusat di tingkat Mabes TNI yang berkedudukan langsung di bawah Panglima TNI. Adapun tugas pokok Pusinfolahta TNI adalah menyiapkan informasi dan pengolahan data pembinaan dan penggunaan kekuatan TNI, menyelenggarakan fungsi pembinaan sistem informasi TNI bagi Pimpinan dan Staf di lingkungan Mabes TNI, serta melakukan pembinaan sistem komputer dan komunikasi data dalam rangka pelaksanaan tugas pokok TNI. Pusinfolahta TNI dapat berperan mendukung BSSN dalam aspek ancaman perang siber ataupun pelatihan dan penyusunan strategi pertahanan siber Indonesia.

Dittipidsiber Polri

Berdasar informasi melalui website resmi Dittipidsiber Polri (2021), didapatkan hasil bahwa Direktorat Tindak Pidana Siber (Dittipidsiber) adalah satuan kerja yang berada di bawah Bareskrim Polri dan bertugas untuk melakukan penegakan hukum terhadap kejahatan siber. Secara umum, Dittipidsiber menangani dua kelompok kejahatan, yaitu computer crime dan computer-related crime.

Computer crime adalah kelompok kejahatan siber yang menggunakan komputer sebagai alat utama. Bentuk kejahatannya adalah peretasan sistem elektronik (hacking), intersepsi ilegal (illegal interception), pengubahan tampilan situs web (web defacement), gangguan sistem (system interference), manipulasi data (data manipulation).

Sedangkan jenis computer-related crime adalah kejahatan siber yang menggunakan komputer sebagai alat bantu, seperti pornografi dalam jaringan (online pornography), perjudian dalam jaringan (online gamble), pencemaran nama baik (online defamation), pemerasan dalam jaringan (online extortion), penipuan dalam jaringan (online fraud), ujaran kebencian (hate speech), pengancaman dalam jaringan (online threat), akses ilegal (illegal access) dan pencurian data (data theft).

Pemanfaatan konsep sistem pertahanan semesta dalam menghadapi ancaman serangan siber selama pandemi covid-19 di Indonesia.

Dalam menghadapi serangan siber diperlukan peran dari banyak pihak yang terkait. Oleh karena itu diperlukan pemanfaatan konsep pertahanan semesta, dengan pengunaan kekuatan dari unsur utama dan unsur lain penguat pertahanan siber dari berbagai pihak yang terkait untuk saling bersinergi, berkomunikasi dan saling koordinasi.

Serangan siber merupakan ancaman serius di era pandemi Covid-19 sekarang ini, sehingga diperlukan kesatuan pandangan dan satu persepsi untuk mensinergikan satu tindakan, satu kebijakan dan satu rencana aksi yang utuh. Ancaman siber memerlukan partisipasi aktif baik dari unsur utama, maupun unusr lain penguat pertahanan siber dari berbagai pihak. Karena untuk menghadapi serangan siber tidak mungkin hanya bisa dihadapi oleh satu instansi semata. Ancaman serangan cyber tidak bisa dilakukan secara parsial semata, melainkan memerlukan langkah penanganan yang dilakukan secara komprehensif, integral dan terpadu.

Dalam menghadapi serangan siber, diperlukan analisis terhadap eskalasi ancaman dan gradasi dalam menghadapi serangan siber. Berikut penulis uraikan tentang eskalasi ancaman siber, dihadapkan dengan unsur utama dan unsur lain pendukung yang berperan sebagai pihak yang menanganinya :

Tabel 1. Eskalasi Serangan Siber

No	Jenis Serangan	Unsur Utama & Unsur Lain Penguat Pertahanan Siber
1	Ancaman Siber	BSSN, Puskom Kemhan, Kominfo
2	Kejahatan Siber	BSSN, Dittipidsiber Polri, Kominfo
3	Perang Siber	BSSN, Puskom Kemhan, Pusinfolahta Mabes TNI, Kominfo

Sumber: Olahan Peneliti 2021

Berdasarkan tabel eskalasi serangan siber diatas, dapat di analisa bahwa pada saat ini BSSN unsur utama pertahanan siber yang ada di Indonesia. Berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN), BSSN memiliki tujuan utama untuk melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan ikut serta mengonsolidasikan semua unsur yang terkait dengan keamanan siber nasional. Oleh karena itu BSSN sebagai unsur utama mengatur semua sinergi dan unsur lain penguat pertahanan siber yang ada di Indonesia. Adapun pemanfaatan unsur utama dan unsur penguat dalam menghadapi setiap serangan siber antara lain:

1. Ancaman Siber

Untuk menghadapi ancaman siber, unsur utama BSSN akan didukung oleh unsur lain penguat pertahanan yang terdiri atas Puskom Kemhan dan Kominfo. Puskom Kemhan bersama BSSN memiliki fungsi untuk merancang sistem pertahanan dan keamanan siber di Indonesia. Sedangkan Kominfo memiliki peran untuk membuat kebijakan, melakukan pemblokiran terhadap situs atau akun yang dinilai salah dan mendukung sosialisasi dari program pengamanan dan pertahanan yang sedang dijalankan.

2. Kejahatan Siber

Dalam menghadapi serangan dalam jenis kejahatan siber, BSSN akan didukung oleh Dittipidsiber Polri terkait penanganan terhadap computer crime dan computer-related crime. Polri memilki wewenang untuk menjalan tindakan penangkapan terhadap pelaku kejahatan. Selain itu, pihak Kominfo juga bisa membantu untuk menyusun kebijakan, serta memberikan sosialisasi dan

literasi terhadap masyarakat terkait bahaya kejahatan siber.

3. Perang Siber

Untuk menghadapi potensi adanya perang siber di Indonesia, BSSN dibantu dengan Puskom Kemhan dan Pusinfolahta Mabes TNI dapat menyusun strategi pertahanan dan pedoman pertahanan siber Indonesia dalam menghadapi peperang siber. Kominfo juga bisa memberikan bantuan dengan memberikan informasi dan sosialisasi kepada masyarakat terkait perang siber yang berpotensi akan terjadi.

Akan tetapi ketika turun dilapangan tidak menutup kemungkinan setiap penyelenggara juga bisa saling beririsan dalam hal penanganan suatu kasus serangan siber. Luasnya spektrum dunia siber, mengharuskan setiap penyelenggara untuk selalu bekerjasama. Disinilah peran BSSN agar bisa menjadi penghubungan dan memantau bagaimana jalannya serangan siber yang mengancam di Indonesia. Adapun langkah yang harus dilakukan BSSN untuk menjaga keamanan siber Indonesia antara lain:

BSSN dalam hal membuat kebijakan yang berfungsi menangkis, menangkal, dan mencegah ancaman siber yang dapat membahayakan jaringan komunikasi, instansi pemerintah, maupun lembaga swasta yang terkait dengan komunikasi dan informatika dengan menjalin koordinasi dan kerjasama dengan Kominfo

BSSN juga harus berkomunikasi dengan Puskom Kemhan terkait situasi pertahanan siber Indonesia dalam hal perang siber, baik dengan pihak dalam negeri maupun luar negeri. BSSN bersama Kemhan harus menyusun strategi pertahanan siber yang dapat digunakan untuk melindungi cyber space Indonesia, dalam rangka mewujudkan keamanan nasional dalam bidang siber.

Terkait peperangan siber, BSSN juga harus berkoordinasi dengan Pusinfolahta Mabes TNI terkait pengolahan informasi ketahanan TNI dalam rangka menjaga keamanan siber nasional. Pada saat terjadi perang siber, BSSN, Pusinfolahta Mabes TNI, dan Puskom Kemhan adalah penyelenggara terdepan yang melakukan pertahanan dan perlawan.

Sedangkan dalam hal menangani kejahatan siber. BSSN bisa melakukan koordinasi dengan Dittipidsiber Polri terkait pelacakan tindak kejahatan, penanganan kejahatan siber, antisipasi kejahatan siber, dan penanggulangan kejahatan siber. Polri juga bisa meminta bantuan BSSN dalam rangka operasi pengamanan aset, atau pencarian informasi terduga pelaku kejahatan siber.

KESIMPULAN

Sehingga berdasarkan uraian diatas dapat disimpulkan bahwa saat masa pandemi Covid-19, serangan siber di Indonesia mengalami peningkatan. Diketahui bahwa selama pandemi covid-19, serangan siber di Indonesia naik empat kali lipat. Angka terbanyak untuk kasus serangan siber terjadi pada Agustus 2020, di mana tercatat ada 63 juta serangan siber di Indonesia. Banyak aktor penyerang menggunakan isu Covid-19 sebagai jebakan untuk melakukan serangan.

Adapun untuk menghadapi ancaman siber yang semakin meningkat, Pemerintah bisa menerapkan konsep pertahanan semesta dengan mengerahkan unsur utama dan unsur lain penguat pertahanan siber di Indonesia. BSSN sebagi unsur utama memiliki tujuan utama untuk melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan ikut

serta mengonsolidasikan semua unsur yang terkait dengan keamanan siber nasional. Sedangkan untuk menangani ancaman siber, BSSN dibantu oleh Puskom Kemhan dan Kominfo. Untuk menghadapi kejahatan siber, BSSN akan dibantu oleh unsur lain penguat pertahanan siber dari Dittipidsiber Polri, Kominfo. Sedangkan unsur lain penguat pertahanan siber yang membangtu dalam menangani ancaman peperangan siber adalah Puskom Kemhan, Pusinfolahta Mabes TNI, Kominfo.

DAFTAR PUSTAKA

Agung, A. (2022). *Pencegahan Cybercrime Di Wilayah Hukum Polda Jambi* (Doctoral dissertation, Ilmu Hukum).

Beritasatu. (2021). "Serangan Siber Meningkat Seiring Aktivitas Digital Saat Pandemi." Dalam https://www.beritasatu.com/digital/747215/serangan-siber-meningkat-seiring-aktivitas-digital-saat-pandemi, Diakses pada tanggal 20 - 04 - 2021. Tersedia pada:

BSSN. (2021). Tugas dan Fungsi BSSN, dalam https://bssn.go.id/tugas-dan-fungsi-bssn/, diakses pada 17 – 02 - 2021.

Kemhan. (2021). Rohumas, dalam https://www.kemhan.go.id/rohumas/category/berita/page/2, diakses pada 17 – 02 – 2021.

Kertopati, L. (2018). Dua Rumah Sakit di Jakarta Kena Serangan Ransomware WannaCry, dalam https://www.cnnindonesia.com/teknogi/20170513191519192214642/dua-rumah-sakit-di jakarta kena-serangan-ransomware-wannacry, diakses pada tanggal 17 – 02 – 2021.

Siagian, L., Budiarto, A., & Simatupang, S. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Jurnal Prodi Perang Asimetris | Desember 2018, Volume 4, Nomor 3.*

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Technologies (TELNECT)*, *1*(2), 85-92.

Patrolisiber. (2021). About, dalam https://patrolisiber.id/about, diakses pada 17 – 02 – 2021.

Prasetya, E. (2020). "Serangan Siber Meningkat Sejak Pandemi Covid-19, dalam https://www.merdeka.com/peristiwa/serangan-siber-meningkat-sejak-pandemi-covid-19.html, Diakses pada tanggal 20 - 04 - 2021.

Sa'diyah, N. K. dan Vinata, R. T.. (2016). Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. *Jurnal Perspektif Volume XXI No. 3 Tahun 2016 Edisi September.*

Zakia, S. P. (2020). Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi, dalam tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi, Diakses pada tanggal 20 - 04 - 2021.

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 157-178.

Utami, M. N. (2019). *Kejahatan Peretasan (Hacking) Dan Pemerasan 3000 Website Di 44 Negara Oleh Surabaya Black Hat Dihubungkan Dengan Uu No 19 Tahun 2016 Tentang Informasi Teknologi Dan Elektronik (Ite)* (Doctoral dissertation, Fakultas Hukum Unpas).

Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 *Jurnal IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi)*, *22*(2), 143-158.