

PEMBERDAYAAN KOMUNITAS SIBER OLEH PEMERINTAH REPUBLIK INDONESIA DARI PERSPEKTIF STRATEGI PERANG SEMESTA

THE EMPOWERMENT OF THE CYBER COMMUNITIES BY THE INDONESIAN GOVERNMENT FROM THE PERSPECTIVE OF TOTAL WAR STRATEGY

Devis Lebo¹, Syaiful Anwar²

Prodi SPS Fakultas Strategi Pertahanan Universitas Pertahanan
(devislebo@ymail.com)

Abstrak – Perkembangan Teknologi Informasi dan Komputer (TIK) saat ini telah membuat perubahan yang berpengaruh pada konsep keamanan. Dampak dari perkembangan TIK ini menimbulkan ancaman siber terhadap Infrastruktur informasi kritis nasional (IIKN) . Upaya pemberdayaan komunitas siber bertujuan untuk membantu pemerintah, Lembaga dan pihak swasta terkait bidang TIK dalam menjaga dan mengamankan IIKN dari serangan siber yang dampaknya dapat meruntuhkan suatu negara jika tidak diantisipasi lebih awal. Untuk itu diperlukan strategi yang mampu mendukung pemberdayaan komunitas siber oleh pemerintah dalam perspektif perang semesta. Didalam penulisan artikel ini, penulis menggunakan metode dengan cara mengumpulkan data dan informasi melalui bantuan bermacam -macam materi yang terdapat dalam kepustakaan (buku) atau disebut juga jenis penelitian fenomenologis yang dikaitkan dengan deskriptif kualitatif. Dari hasil penelitian pustaka yang penulis dapatkan diketahui bahwa komunitas siber belum sepenuhnya ikut membantu pemerintah dalam pertahanan negara, ada sebagian komunitas siber yang belum dilibatkan, dibutuhkan peran pemerintah, Lembaga dan pihak swasta terkait TIK untuk dapat mewujudkan pemberdayaan komunitas siber oleh Pemerintah dalam perspektif perang semesta.

Kata Kunci: Pemberdayaan, Komunitas Siber, Pemerintah RI, Strategi Perang Semesta

Abstract – *The development of Information Technology and Computers (ICT) has made changes that affect the concept of security. The impact of these ICT developments poses a cyber threat to the National Critical Information Infrastructure (IKN). The cyber community empowerment effort aims to help the government, institutions and private parties related to the ICT sector in safeguarding and securing IKN from cyber attacks whose impact can collapse a country if it is not anticipated earlier. For that we need a strategy that is able to support the empowerment of the cyber community by the government in the perspective of universal war. In writing this article, the author uses a method by collecting data and information through the help of various materials contained in the literature (books) or also known as the type of phenomenological research associated with qualitative descriptive. From the results of the literature research that the authors get, it is known that the cyber community has not fully helped the government in national defense, there are some cyber communities that have not been involved, it takes the role of government, institutions and private parties related to ICT to be able to realize cyber community empowerment by the Government in the perspective of universal war.*

Keywords: Empowering, Cyber Communities, Indonesian Government, Total War Strategy

¹Program Studi Perang Semesta, Fakultas Strategi Pertahanan, Universitas Pertahanan

²Fakultas Strategi Pertahanan, Universitas Pertahanan

Pendahuluan

Sistem pertahanan negara Indonesia bersifat semesta dengan melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya. Oleh Sebab itu sistem pertahanan semesta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah dan keselamatan segenap bangsa dari segala ancaman.

Keterpaduan itu merujuk pada elemen kekuatan yang dibangun dalam sistem pertahanan semesta, yang memadukan kekuatan pertahanan militer dan kekuatan pertahanan nirmiliter³.

Konsep pertahanan semesta yang selalu melibatkan seluruh kemampuan yang dimiliki oleh bangsa ini semestinya di data, diolah dan digunakan sebaik-baiknya demi mendukung perang semesta.

Dalam UU No.29/1954 'pertama kali' menyebut bahwa perang semesta sebagai perang rakyat semesta. Didalam buku Letjen TNI JS.Prabowo disingkat menjadi "perang semesta"⁴.

Menurut Prabowo, perang semesta dimasa datang juga tidak pasti bisa secara harfiah disamakan dengan perang gerilya dan dan tidak sepenuhnya sama dengan perang kemerdekaan Republik Indonesia (1945-1950).

Perang semesta sama sekali bukan sesuatu yang sederhana, dan dapat dideskripsikan secara sederhana. Apapun pengertian tentang perang semesta yang menggunakan cara-cara militer untuk menyelesaikan konflik sejauh mungkin harus dihindari.

Menurut Sun Tzu: "Untuk apa kita sibuk memperdebatkan musuh akan menyerang atau tidak, lebih baik kita bersiap menyambutnya".

Dalam pengelompokan generasi perang, maka di zaman ini sudah masuk pada peperangan generasi keempat (4GW) yang merupakan peperangan asimetris dan non-linier yang menggunakan seluruh sarana dan prasarana serta sistem senjata yang ditujukan terutama untuk menghancurkan 'kemauan' bertempur musuh.

Didalam peperangan asimetris dan non-linier, kekuatan pertahanan nirmiliter

³Purnomo Yusgiantoro, "Pedoman Pertahanan Siber. Biro Tata Usaha Sekjend Kemhan" dalam content /uploads/2016/10/Permenhan-No.-82 Tahun-2014-tentang-Pertahanan-Siber.pdf, 17 Oktober 2014 diakses pada 28 Oktober 2020.

⁴ J.Suryo Prabowo, Pokok-Pokok Pemikiran tentang Perang Semesta (Cetakan Ke tiga), (Jakarta: PT. Tamaraprint Indonesia, 2019), hal.ii.

merupakan bagian dari peperangan tersebut. Salah satu yang dapat menjadi ancaman bagi kekuatan pertahanan nirmiliter adalah TIK (teknologi informasi dan komunikasi).

Perkembangan TIK khususnya di ranah siber yang berkembang begitu cepat hingga saat ini dan seakan tidak terbendung, apalagi penggunaan TIK sudah memasuki seluruh aspek kehidupan masyarakat seperti : ideologi, politik, ekonomi, sosial, budaya, hukum, pendidikan, pertahanan dan keamanan. Kebutuhan akan TIK sudah sangat mutlak saat ini baik, di rumah, kantor, industri, bisnis dan dimana saja tidak akan lepas dari TIK.

Kegiatannya berupa komunikasi, interaksi dan gerakan melalui media sosial sudah sangat masif sehingga sangat penting dan menjadi perhatian di setiap negara. Perkembangan TIK ini jika dikaitkan dalam industri maka sudah memasuki pada tahap yang lazim disebut revolusi industri 4.0 Hal ini menimbulkan bentuk ancaman yang semakin kompleks, sehingga cara bertindak musuh akan semakin bervariasi dan akurat Hal ini juga dapat menjadi ancaman bagi pertahanan nirmiliter Indonesia⁵. Dalam revolusi industri 4.0, masalah ancaman

nirmiliter menjadi perhatian berbagai kalangan baik di luar negeri maupun di dalam negeri. Akibat adanya revolusi Industri 4.0 tersebut, maka timbul suatu ancaman baru yaitu ancaman siber. Ancaman siber ini sudah sangat serius, karena tidak menggunakan pasukan yang banyak dalam melakukan serangan namun dampaknya sangat besar untuk menghancurkan suatu target dan pemulihannya butuh waktu yang sangat lama.

TIK semakin hari semakin canggih dan modern, hal ini berpengaruh pada taktik yang digunakan oleh orang-orang yang tergolong ingin melakukan kejahatan siber. Kondisi saat ini kejahatan siber sudah melanda Indonesia, mereka menyerang perbankan, pembangkit tenaga listrik, pusat bisnis *e-commerce* (bukalapak, Tokopedia), *e-style*, transportasi, rumah sakit, kegiatan pilkada bahkan di bidang pertahanan dan keamanan. Hal ini membuktikan bahwa serangan siber sudah sangat serius dan sangat membahayakan terhadap infrastruktur informasi kritis nasional (IIKN) yang kita miliki.

Berdasarkan informasi *The Global cyber security 2017* yang dirilis oleh the UN

⁵Hadi Tjahjanto, S.I.P, Keputusan panglima tentara nasional indonesia No. Kep/555/VI/2018, (Mabes TNI dan Angkatan, 2016), hal.15

International Telecommunication Union (ITU), Indonesia termasuk negara dalam keamanan siber yang paling lemah⁶

Situasi yang dialami Indonesia ini tidak jauh berbeda dengan negara-negara di Amerika Selatan seperti Brasil dan juga negara di Afrika yang rentan terhadap serangan siber. Lemahnya keamanan siber ini berdampak dengan meningkatnya serangan siber. Indonesia berada di peringkat 70 Dari 195 negara, dengan skors 0,424. Peringkat pertama adalah Singapura disusul oleh Amerika Serikat di peringkat kedua dengan sistem keamanan siber terbaik⁷.

Menurut Sigit Kurniawan kepala sub direktorat identifikasi kerentanan dan penilaian risiko infrastruktur informasi kritical nasional III badan siber dan sandi negara (BSSN) bahwa "sesuai data pada penilaian terhadap 76 negara, pada penilaian 2019 Indonesia berada pada rangking kedua terburuk setelah Algeria, namun segera membaik pada 2020, pada peringkat 21⁸.

Dengan melihat situasi ini maka dalam rangka upaya melindungi wilayah kedaulatan Indonesia, khususnya di ranah siber, dibutuhkan keterlibatan seluruh sumber daya yang ada dalam menjaga kedaulatan negara yang dilaksanakan melalui sistem pertahanan dan keamanan rakyat semesta (*sishankamrata*), yang menempatkan TNI sebagai kekuatan utama dan rakyat sebagai komponen cadangan dan pendukung, dimana setiap warga negara mempunyai kewajiban untuk ikut serta dalam usaha pertahanan negara sesuai dengan isi UUD 1945 pasal 30 ayat 1 dan 2.

Keterlibatan warga negara dalam menghadapi perang semesta merupakan tanggung jawab yang perlu dipikul bersama agar masalah yang dihadapi dapat dicegah sedini mungkin. Semenjak berkembangnya teknologi, semua kegiatan di dalam masyarakat selalu menggunakan teknologi seperti tersedianya alat atau hal pendukung lainnya, seperti komputer, koneksi internet, *gadget*, *provider*, dan lainnya⁹. Masyarakat pengguna TIK inilah yang biasa disebut komunitas siber. Komunitas siber pada

⁶Sanou Brahim, "Global Cybersecurity Index (GCI) 2017", dalam https://www.itu.int/dms_pub/itud/opb/str/D-STR-GCI.01-2017-PDF-E.pdf, diakses pada 28 Oktober 2020

⁷Kristian Erdianto, "Bagaimana Upaya Pemerintah Menangkal Maraknya Serangan Siber?", Kompas.com 21 November 2017, diakses pada 28 Oktober 2020.

⁸M.Ikhsan, "BSSN Sebut Keamanan Siber RI 2020 Naik, Serangan Meningkat", dalam <https://www.cnnindonesia.com/teknologi/2020>, diakses pada 28 Oktober 2020.

⁹Bumibelumbulat "Komunitas Siber", dalam <https://bumibelumbulat.wordpress.com/2016/05/21/komunitas-siber/>, 21 Mei 2016, diakses pada 28 Oktober 2020

awalnya kecil dan berkembang menggunakan pola jaring laba-laba sehingga terbentuklah masyarakat yang besar. Komunitas siber melibatkan seluruh masyarakat yang menggunakan *gadget*, komputer dan jaringan.

Saat melaksanakan virtual, mereka tidak pernah bertemu muka dan tidak mempunyai batas teritori, mereka berinteraksi dengan menggunakan teknologi dan jaringan internet yang dimiliki. Keberadaannya Komunitas siber dalam melakukan komunikasi, sangat penting untuk diteliti.

Penulis melihat bahwa keberadaan komunitas siber ini sudah banyak di Indonesia, sering berkumpul saling tukar informasi, namun mereka sifatnya tertutup tidak mau dikenal orang atau sering disebut *underground/anonymous*. Keberadaan mereka ini perannya sangat penting dalam dunia siber (maya).

Komunitas siber memiliki kemampuan yang dapat diandalkan dalam mencegah kehancuran akibat serangan siber. Komunitas siber merupakan bagian didalam masyarakat yang saat ini belum tersentuh dan menjadi prioritas negara untuk dilibatkan dalam usaha pertahanan negara.

Komunitas siber perlu ikut menjaga IKN yang merupakan aset bangsa.

Mengenai pembentukan Komunitas siber sampai dengan saat ini masih menjadi perdebatan, beberapa kalangan masih melihat komunitas siber dalam bentukan yang nyata dalam suatu ikatan wilayah, meskipun tidak semua orang yang berada dalam satu lingkungan yang sama dapat dikatakan komunitas, dapat dikatakan komunitas jika anggota anggota yang ada didalamnya memiliki pengalaman yang sama dan rasa sebagai suatu komunitas “sense of community”¹⁰.

Diperlukan strategi agar pemberdayaan komunitas siber ini diperhatikan keberadaannya sebagai aktifitas dalam melakukan pencegahan dan pengamanan terhadap sumber daya telematika sehingga tidak terjadi kriminalitas di dunia siber. Perlu diketahui bahwa pembelaan terhadap negara dalam menghadapi perang semesta selain merupakan kewajiban hukum, juga menjadi hak dan kehormatan sebagai warga negara. Strategi dalam meneliti pemberdayaan komunitas siber sangat diperlukan agar pemberdayaan komunitas siber yang berada ditengah-tengah perkembangan teknologi

¹⁰Hendri Prasetyo, “Cyber Community, Cyber Cultures : Arsitektur Sosial Baru Masyarakat Modern”, dalam file:// C: / Users / Andromeda 190-

Anonymous Manuscript for Review-322-1-10-20160425.pdf , 1 Desember 2010, diakses pada 29 Oktober 2020.

dapat dilibatkan secara tepat guna dalam mendukung perang semesta, ini sesuai dengan Undang-Undang Nomor 20 Tahun 1982 tentang Ketentuan-Ketentuan Pokok Pertahanan Keamanan Negara Republik Indonesia, pasal 17 hingga pasal 25¹¹.

Kondisi Komunitas siber masih sibuk dengan dunianya sendiri, mereka hanya mementingkan pribadi atau kelompoknya masing-masing. Terkadang komunitas siber ini ada yang melakukan kegiatan melanggar hukum, ini terjadi karena tidak adanya kontrol dan pembinaan yang jelas dari pemerintah.

Kondisi karakter dan jiwa untuk membantu negara merupakan hak dan kewajiban bagi setiap komunitas siber yang diselenggarakan melalui usaha pertahanan negara untuk menegakkan kedaulatan negara, menjaga keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa.

Pemberdayaan komunitas siber dilaksanakan atas dasar kesadaran serta keyakinan pada kekuatan sendiri yang ditumbuh kembangkan melalui usaha mempertahankan negara.

Keberadaan komunitas siber yang luar biasa banyak ini agar dapat lebih bermanfaat

bagi negara dalam menghadapi perang semesta. Oleh sebab itu dalam tulisan ini, penulis bermaksud menjelaskan bagaimana pemberdayaan komunitas siber dapat dilakukan oleh pemerintah Indonesia dalam perspektif perang semesta sehingga komunitas siber dapat turut mengambil bagian sebagai komponen pendukung yang akan membantu pemerintah dalam menjaga kedaulatan negara dibidang pertahanan dengan kemampuan TIK yang dimiliki.

Didalam buku *Art of War*, Sun Tzu (403-221) mengatakan “*The supreme art of war is to subdue the enemy without fighting.*” ini berarti bahwa “Perang merupakan seni, menaklukkan musuh tanpa pertempuran adalah seni perang tertinggi.” Dari pendapat tersebut sangat relevan dengan kegiatan siber saat ini, dimana dalam menghancurkan musuh dilakukan tersembunyi tidak perlu membawa pasukan yang besar, cukup menggunakan kemampuan dan keahlian yang dimiliki, namun dampak kerusakannya sangat besar bahkan dapat meruntuhkan suatu negara serta untuk kembali pulih dibutuhkan waktu yang lama.

Menurut *Thomas Rid & Peter McBurney* yang mendefinisikan sebagai berikut: “Sista siber adalah bagian dari persenjataan yang

¹¹Mery Panjaitan, “Peran pemuda sebagai kader bela negara dalam mendukung pertahanan dan keamanan maritim”, *Jurnal Pertahanan*, hal.53-65.

didesain untuk mengancam atau membahayakan fisik, fungsional atau mental suatu struktur atau sistem atau sistem kehidupan”¹².

Teori ini sangat relevan karena serangan siber dampaknya sangat besar terhadap informasi dan budaya yang berlaku di masyarakat saat ini seperti peristiwa 'Arab Spring', dimana runtuhnya suatu negara akibat serangan siber melalui *hoax*, *FOF*, *Post Truth* yang sangat handal, membentuk opini publik sehingga terjadi polarisasi dalam masyarakat yang mengakibatkan timbulnya disintegrasi bangsa, chaos dan negara runtuh.

Serangan siber terhadap target fisik dan *logic* juga tidak kalah hebatnya, seperti yang terjadi di Estonia Mei 2007, Ukraina Desember 2017, karena kejadiannya pada musim dingin, listrik padam dan alat pemanas tidak berfungsi menyebabkan jatuhnya korban jiwa. Dari peristiwa tersebut akan sangat mungkin bisa saja terjadi di Indonesia. Oleh sebab itu pemberdayaan komunitas siber di negara ini sangat dinantikan untuk dapat membantu pemerintah menyelesaikan masalah-masalah di dunia siber.

Sebagaimana diketahui bahwa kata “pemberdayaan ” adalah terjemahan dari bahasa Inggris “Empowerment”, pemberdayaan berasal dari kata dasar “power” yang berarti kekuatan berbuat, mencapai, melakukan atau memungkinkan. Awalan “em” pemberdayaan dapat berarti kekuatan dalam diri manusia, suatu sumber kreativitas.

Pemberdayaan menekankan bahwa orang memperoleh keterampilan, pengetahuan, dan kekuasaan yang cukup untuk mempengaruhi kehidupannya dan kehidupan orang lain yang menjadi perhatiannya.

Menurut 'person' bahwa pemberdayaan adalah sebuah proses dengan yang menjadikan seseorang cukup kuat untuk berpartisipasi dalam mengontrol dan mempengaruhi terhadap kejadian-kejadian serta lembaga-lembaga yang mempengaruhi kehidupannya.

Jika dikaitkan dengan komunitas siber maka mengandung arti bahwa suatu kegiatan yang dilakukan oleh komunitas siber untuk menunjukkan kemampuannya dalam melakukan kegiatan yang dapat mempengaruhi hidupnya yang lebih baik dan bermanfaat bagi orang lain.

¹²Fikri Asyrafi, Berfikir strategic tentang serangan cyber”, dalam <https://mirmidons.wixsite.com/taktik/single->

[post/2016/11/23/Analisis-Perang-Cyber](https://mirmidons.wixsite.com/taktik/single-post/2016/11/23/Analisis-Perang-Cyber) Part-2-Akhir, 23 November 2016, diakses pada 28 Oktober 2020.

Dalam UU Nomor 23 tahun 2019 tentang Pengelolaan Sumber Daya Nasional untuk Pertahanan Negara (PSDN), dapat digunakan sebagai dasar dalam merekrut komunitas siber untuk dididik menjadi kader belanegara.

Menurut Letjen TNI JS. Prabowo bahwa perang semesta kini dan dimasa depan tidak mesti dilakukan dengan mobilisasi penduduk “habis-habisan” untuk diperankan sebagai kombatan dalam pertempuran.

Didalam UU No. 3 Tahun 2002 tentang Pertahanan Negara, pertahanan negara adalah segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara.

Sistem pertahanan negara Indonesia bersifat sistem pertahanan semesta, yaitu melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut untuk menegakan kedaulatan negara, keutuhan wilayah dan

keselamatan segenap bangsa dari segala ancaman.

Didalam buku putih pertahanan Indonesia tahun 2015 hal.22 disampaikan bahwa ancaman saat ini dan masa depan dapat digolongkan menjadi tiga jenis yaitu ancaman militer baik bersenjata maupun tidak bersenjata, ancaman nonmiliter, dan ancaman hibrida. Sumber ancaman dapat berasal dari dalam maupun luar negeri, serta dilakukan oleh aktor negara maupun nonnegara, yang bersifat nasional, regional dan internasional.

Ancaman siber merupakan ancaman non militer yang dapat berasal dari dalam dan luar negeri serta dapat dikategorikan dalam ancaman nyata baik saat ini maupun yang akan datang¹³.

Metode Penelitian

Penelitian ini merupakan jenis penelitian dengan mengumpulkan data dan informasi melalui bantuan bermacam-macam materi yang terdapat dalam kepustakaan (buku) atau disebut juga jenis penelitian fenomenologis. Jenis penelitian ini merupakan suatu penelitian yang ditujukan untuk mendeskripsikan fenomena masyarakat yang menggunakan daring, peristiwa, aktifitas sosial, sikap, kepercayaan, persepsi,

¹³Ryamizard Ryacudu, Buku Putih Pertahanan Indonesia 2015, (Cetakan ketiga) (Jakarta:

Kementerian Pertahanan Republik Indonesia, 2105), hal.22.

pemikiran orang secara individu maupun kelompok. Untuk mendeskripsikan fenomena pemberdayaan komunitas siber secara mendalam, maka penelitian menggunakan studi pustaka yang dikaitkan dengan deskriptif kualitatif fenomenologis. Dengan studi pustaka maka temuan-temuan empiris dapat dideskripsikan secara rinci, lebih jelas dan lebih akurat terutama berbagai hal yang berkaitan dengan komunitas siber. Untuk itu, melalui tulisan ini, diharapkan studi pustaka dapat membantu penelitian dalam berpikir dan berimajinasi, secara abstrak.

Penelitian fenomenologi dapat dimulai dengan memperhatikan dan menelaah fokus fenomena yang hendak diteliti, yang melihat berbagai aspek subjektif dari perilaku objek. Kemudian, peneliti melakukan penggalian data berupa bagaimana pemaknaan objek dalam memberikan arti terhadap fenomena terkait.

Penggalian data ini dilakukan dengan melakukan pengambilan data sekunder dari literatur yang telah dibaca, informasi ini akan dibawa dalam penelitian pustaka yang mengacu pada Hammersley & Atkinson (sekitar 2007) yang mempelajari data-data

yang diperoleh untuk pengembangan konsep-konsep terkait konflik sosial di media sosial¹⁴.

Fokus dalam penelitian ini adalah tentang pemberdayaan komunitas siber dalam perspektif perang semesta, tujuannya adalah untuk menyiapkan komunitas siber dalam menghadapi perang semesta. Guna mendalami fokus tersebut penelitian ini akan menggunakan metode kualitatif. Penelitian kualitatif yang dipilih karena fenomena yang diamati perlu pengamatan melalui studi pustaka, karena lebih mudah berhadapan dengan realitas, sehingga didapatkan data sekunder yang mendalam. Penelitian kualitatif ini digunakan dengan tujuan untuk mengeksplorasi kekhasan pengalaman seseorang atau kelompok yang datanya diambil dari studi pustaka ketika mengalami suatu fenomena sehingga fenomena tersebut dapat dibuka dan dipilih untuk dicapai suatu pemahaman yang ada.

Seperti yang telah diutarakan sebelumnya bahwa strategi yang digunakan dalam penelitian kualitatif ini adalah fenomenologi. Menurut Creswell, fenomenologi dipilih karena didalamnya peneliti akan mengidentifikasi tentang suatu

¹⁴Dony A. Triantoro, "Konflik Sosial dalam Komunitas Virtual di Kalangan Remaja", Jurnal Komunikasi, Volume 13, Nomor 2, April 2019, hal 135-150.

fenomena tertentu, serta mengharuskan peneliti mengkaji subjek dengan terlibat langsung untuk mengembangkan pola dan relasi yang bermakna.

Dalam konteks penelitian yang akan dikaji ini, fokus utamanya dalam penelitian ini adalah melaksanakan pencarian data melalui studi pustaka tentang komunitas siber karena pada umumnya bersifat tertutup, semua kegiatan dilaksanakan di dunia siber (maya) dan sedikit sekali untuk bertatap muka. Penulis akan menggali kegiatan yang dilaksanakan komunitas siber saat ini, status sosialnya baik pekerjaan dan juga latar belakang pendidikan, serta semangat komunitas siber dalam menjaga IKN dari serangan siber demi mewujudkan pertahanan negara yang akan penulis kaitkan dengan strategi perang semesta.

Sedangkan lokasi penelitian adalah tempat dimana penelitian akan dilakukan.

Penetapan lokasi penelitian merupakan tahap yang sangat penting dalam penelitian kualitatif, sehingga mempermudah penulis melakukan penelitian. Lokasi ini bisa diwilayah tertentu atau suatu lembaga tertentu dalam

masyarakat. Untuk memperoleh data sekunder maka lokasi penelitian berdasarkan data-data yang diperoleh melalui buku-buku, jurnal dan media elektronik lainnya.

Hasil dan Pembahasan

Perlu diketahui bahwa berdasarkan data yang diperoleh pada tahun 2019, pengguna internet di Indonesia ada 56% atau 150 juta orang, semua tanpa pengamanan siber dimana resiko yang akan dihadapi akan sangat besar, karena banyaknya ancaman keamanan¹⁵.

Dalam menghindari upaya pencurian data pribadi tentang transaksi daring melalui ancaman siber maka Komunitas siber dapat diandalkan menjadi garda terdepan¹⁶.

Komunitas siber dalam kegiatan sehari-hari ketika berinteraksi selalu menggunakan *gadget*, komputer dan jaringan, sehingga komunitas siber merupakan suatu kajian baru yang saat ini menjadi pusat perhatian bagi pengguna TIK. Dunia maya ini menjadi realitas baru, yang

¹⁵Tangguh Chairil, "Mewujudkan keamanan siber bagi Indonesia: Apa yang harus dilakukan?," dalam <https://theconversation.com/mewujudkan-keamanan-siber-bagi-indonesia-apa-yang-harus-dilakukan-116813>, 9 Mei 2019, diakses pada 29 Oktober 2020.

¹⁶Fetry Wuryasti, "Masyarakat Perlu Dilibatkan Dalam Kurangi Ancaman Kejahatan Siber," dalam <https://mediaindonesia.com/read/detail/349210>, 1 Oktober 2020a, diakses pada 30 Oktober 2020

telah menjadi dunia komunitas kedua setelah dunia nyata itu sendiri.

Berdasarkan hasil penelitian tentang keberadaan komunitas siber, bahwa komunitas siber ini dibagi dalam dua kelompok, *pertama* kelompok milenial atau anak muda, yang pendidikannya mulai dari tingkat sekolah dasar, sekolah menengah pertama, sekolah menengah atas dan perguruan tinggi.

Ketertarikan kaum milenial terhadap dunia siber (dunia maya) semakin tinggi karena didukung oleh berbagai jenis aplikasi *chatting* dalam media sosial seperti *whatsapp*, *blackberry messenger* (BBM), *facebook*. Saat ini di media sosial ada satu fitur yang paling diminati oleh kalangan milenial, fitur ini adalah *whatsapp group*. *Whatsapp group* menjadi primadona di kalangan remaja dalam melakukan interaksi sosial dengan teman-teman sejawat.

Kalangan milenial menggunakan *whatsapp group*, untuk dapat bertemu dan berkumpul untuk saling bertukar pikiran, menyapa/kopi darat, *sharing* informasi dan bahkan bercanda bersama dan *Kedua*, kelompok komunitas siber lain berasal dari kalangan dewasa baik yang bekerja maupun tidak bekerja. kelompok milenial dan

dewasa mempunyai pengetahuan tentang dunia siber (dunia maya) berbeda-beda, ada yang hanya sekedar melakukan interaksi untuk melaksanakan komunikasi sesama pengguna *gadget*, mengeluarkan semua aspirasi baik dalam menilai, menanggapi ataupun mengkritik informasi yang diberikan anggota lainnya¹⁷.

Ada yang digunakan untuk melakukan kegiatan bisnis sehingga meraih keuntungan bahkan ada yang digunakan untuk mendukung pekerjaan di kantor atau yang mendukung reputasinya, bahkan tidak menutup kemungkinan ada yang memanfaatkan teknologi ini untuk melakukan kejahatan, seperti kelompok *anonymous*.

Anonymous cenderung tertutup dan tidak mau dikenal identitas dirinya. Mereka ini merupakan aktivis *hacker* yang dibentuk pada tahun 2003. Ciri khas mereka berupa topeng *Guy Fawkes* atau yang biasa dikenal *V for Vendetta*. Aktivis-aktivis seperti ini sudah banyak tersebar di Indonesia.

Dalam kehidupan sehari-hari, kebanyakan orang didalam mengutarakan pendapat, biasanya enggan menyampaikannya secara langsung karena merasa diperhatikan oleh orang di

¹⁷Dony A. Triantoro, "Konflik Sosial dalam Komunitas Virtual di Kalangan Remaja", Jurnal Komunikasi, Volume 13, Nomor 2, April 2019, hal.138.

sekitarnya atau singkatnya punya beban mental, sedangkan melalui komunitas siber seseorang lebih leluasa untuk memberikan pendapatnya karena tidak terlihat langsung oleh anggota lainnya.

Terkadang anggota komunitas siber dapat saling berbagi pengalaman serta menikmati konten yang disediakan pada media siber (maya). Bila pada komunitas di dunia nyata dibutuhkan pertemuan secara tatap muka untuk menjalin komunikasi, namun di komunitas siber tidaklah diperlukan pertemuan secara tatap muka, Bahkan cenderung menutup diri dan tidak saling mengenal.

Keberadaan komunitas siber ada yang formal dan non formal, dimana yang formal memiliki kantor atau tempat berinteraksi yang *representative* seperti komunitas siber kemhan, siber BSSN, Siber Polri, komunitas siber di Universitas, siber TNI, siber Angkatan, siber di Kelembagaan lainnya dan dan siber di instansi swasta yang mempunyai kepentingan dengan bidang TIK.

Biasanya fasilitas komunitas siber formal ini sangat lengkap, karena mereka pada umumnya memiliki tugas sebagai *Cyber defence* yang bertujuan melindungi dan menjaga data pada komputer dari serangan siber sedangkan siber yang non formal, keberadaan mereka ada dimana

saja, bisa di rumah, di *café*, di taman dan sebagainya. Mereka tidak ada tujuan untuk melindungi data penting, mereka hanya memerlukan *gadget*, komputer serta adanya sambungan jaringan internet untuk melaksanakan interaksinya.

Kemampuan komunitas siber yang formal, banyak diperoleh dari bangku pendidikan dan kursus-kursus terutama menyangkut ilmu TIK, sedangkan yang non formal kebanyakan diperoleh dari belajar mandiri, melalui aplikasi-aplikasi yang tersedia seperti *Youtube*, *google* selanjutnya diaplikasikan dilapangan.

Mereka tidak mempunyai tugas khusus seperti komunitas siber yang formal, mereka kebanyakan sebagai *anonymous*, seperti yang sudah kami jelaskan sebelumnya. *Anonymous* ini biasanya aktif sesuai keinginannya masing-masing. *Anonymous* biasanya anti terhadap paham *scientology*, *homophobia* dan korupsi.

Padahal pada awalnya, kelompok komunitas siber ini dibuat untuk tujuan senda gurau, saling menyapa dan tukar pikiran. *Anonymous* yang tersebar saat ini hanya kelompok-kelompok kecil dan bukan suatu organisasi, tapi lebih cenderung kepada sekumpulan orang yang memiliki minat yang sama. Mereka selalu memperjuangkan hak kebebasan internet selain itu mereka juga punya beragam misi,

yang salah satunya adalah menentang adanya sensor dalam dunia internet dan juga pengawasan dunia internet oleh pemerintah.

Anonymous dalam bertindak akan melakukan pengawasan terhadap pemerintah dengan melakukan aksi, melayangkan protes melalui cara menyerbu *website* pemerintah. Kemampuan lain yang dimiliki oleh *Anonymous* adalah sebagai peretas atau bahasa Inggrisnya disebut *hacker*¹⁸.

Peretas merupakan orang yang sangat tertarik untuk mempelajari, menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan. Peretas atau *hacker* merupakan suatu keinginan untuk mengetahui secara mendalam mengenai kerja suatu sistem, komputer atau jaringan komputer, sehingga menjadi orang yang ahli dalam bidang penguasaan sistem, komputer atau jaringan komputer.

Istilah *hacker* yang sering kita salah artikan mengenai hal-hal yang merusak/hack seperti *hack facebook*, *hack email*, *hack jaringan* dan lain-lain. Tetapi sebetulnya Hacking adalah Ilmu seni, seni keamanan

jaringan komputer. Sedangkan saingannya adalah *cracker*. *Cracker* ini sebutan buat mereka yang suka masuk ke sistem komputer orang lain dan *cracker* lebih bersifat destruktif, pada jaringan komputer, mem-*bypass password* atau lisensi program komputer, secara sengaja melawan keamanan komputer, men-*deface* (merubah halaman muka web) milik orang lain bahkan hingga men-*delete* data orang lain, dan mencuri data dari sistem.

Diketahui bahwa kegiatan yang dilaksanakan oleh *hacker* dan *cracker* mempunyai rencana tertentu sehingga melahirkan suatu hasil yang mereka inginkan, maka dari itu berdasarkan data yang diperoleh menjelaskan bahwa sifat dari *hacker* itu sendiri masih mau berbagi ilmu, memberitahukan sistem administrator akan adanya kerentanan (*vulnerability*) di keamanan yang dilihat, tidak mengambil keuntungan yang tidak *fair dari hack*, tidak mendistribusikan dan mengumpulkan *software* bajakan serta tidak pernah mengambil risiko yang bodoh sedangkan sifat dari pada *cracker* adalah mampu membuat suatu program bagi kepentingan dirinya sendiri dan bersifat destruktif atau merusak dan menjadikannya suatu

¹⁸Kevin Sullivan, "Fakta-Fakta Tentang Anonymous yang Bakal Bikin Kamu Tercengang", dalam <https://www.idntimes.com/hype/fun-fact/kevin->

[sullivan/fakta-fakta-tentang-anonymous-yang-bakal-bikin-kamu-tercengang-c1c2](https://www.idntimes.com/hype/fun-fact/kevin-sullivan/fakta-fakta-tentang-anonymous-yang-bakal-bikin-kamu-tercengang-c1c2), 26 April 2017, diakses 30 Oktober 2020

keuntungan, Sebagai contoh : mengirim Virus, pencurian kartu kredit, pembobolan rekening Bank, pencurian password *E-mail/Web Server* dan sebagainya.

Cracker bisa berdiri sendiri atau berkelompok dalam bertindak, mempunyai *website* atau *channel* dalam IRC yang tersembunyi, hanya orang-orang tertentu yang bisa mengaksesnya, *Internet Relay Chat* atau IRC adalah suatu bentuk komunikasi di Internet yang diciptakan untuk komunikasi *interpersonal* terutama komunikasi kelompok di tempat diskusi yang dinamakan *channel* (saluran), tetapi juga bisa untuk komunikasi jalur pribadi¹⁹.

Cracker juga mempunyai *IP address* yang tidak bisa dilacak, kasus yang paling sering ialah *Carding* yaitu pencurian kartu kredit, kemudian pembobolan situs dan mengubah segala isinya menjadi berantakan. Didalam dunia *e-commerce*, *hacker* banyak membantu perusahaan untuk menemukan kerentanan-kerentanan pada aplikasi yang dimiliki.

Dari penjelasan diatas mengenai *hacker* dan *cracker* diketahui bahwa bahwa Hacker adalah orang yang mengetahui apa

yang dilakukannya, menyadari seluruh akibat dari apa yang dilakukannya, dan bertanggung jawab atas apa yang dilakukannya. Sementara *Cracker* adalah orang yang tahu apa yang dikerjakannya, tetapi seringkali tidak menyadari akibat dari perbuatannya, dan ia tidak mau bertanggung jawab atas apa yang telah diketahui dan dilakukannya itu²⁰.

Indonesia, merupakan negara dengan pertumbuhan pengguna internet terbesar keempat di dunia, maka hal ini merupakan suatu peluang dan sekaligus dapat menjadi ancaman besar dengan perkembangan teknologi digital dan internet, bahkan ada perusahaan konsultan *McKinsey* berpendapat bahwa Indonesia dapat meningkatkan pertumbuhannya hingga US\$150 miliar, atau setara 10% dari Produk Domestik Bruto (PDB), pada 2025 jika dapat merangkul teknologi digital²¹. Dari keuntungan yang didapat tersebut maka akan ada tantangan lain yang akan dihadapi dengan perkembangan teknologi, yaitu berupa ancaman siber.

Didalam menghadapi ancaman siber terhadap infrastruktur informasi kritis

¹⁹Wikipedia, "IRC", dalam <https://id.wikipedia.org/wiki/IRC>, 2 September 2020, diakses pada 30 Oktober 2020.

²⁰ Fajar E. Rasyid, "Hacker dan Cracker", dalam https://www.ubaya.ac.id/2018/content/articles_detail/148/Hacker-dan-Cracker.html, 21 Oktober 2014, diakses pada 30 Oktober 2020

²¹Tanggih Chairil, "Mewujudkan keamanan siber bagi Indonesia: Apa yang harus dilakukan?," dalam <https://theconversation.com/mewujudkan-keamanan-siber-bagi-indonesia-apa-yang-harus-dilakukan-116813>, 9 Mei 2019, diakses 30 Oktober 2020.

nasional (IKN) yang dimiliki bangsa ini, maka komunitas siber diharapkan dapat menjadi andalan buat negara dalam ikut serta menjaga IKN yang dimiliki bangsa Indonesia saat ini seperti sektor penegakan hukum, sektor energi dan sumber daya mineral (termasuk di dalamnya listrik), sektor transportasi, sektor keuangan dan perbankan, sektor kesehatan, sektor teknologi informasi dan komunikasi, sektor pertanian, sektor pertahanan dan industri strategis serta sektor layanan darurat dan Sektor sumber daya air. Menurut Badan Siber dan Sandi Negara (BSSN), 10 IKN diatas dianggap sektor yang paling rawan terhadap serangan siber pada masa yang akan datang sehingga BSSN perlu memetakan IKN yang perlu dilindungi.

Esensi Pemberdayaan Komunitas Siber

Peristiwa *Blackout* (listrik padam total) yang pernah dialami Jakarta, Banten, Jawa Barat dan sekitarnya pada Minggu (4 Agustus 2019) kembali mengingatkan masyarakat Indonesia bahwa pentingnya keamanan siber di era digital. Listrik adalah salah satu kebutuhan primer di era TIK yang semuanya dikendalikan dengan komputerisasi untuk memudahkan kehidupan manusia ²².

Perlindungan terhadap IKN seyogyanya sudah mulai diperhatikan lebih serius, oleh Pemerintah, apalagi kondisi negara ini baru saja berbenah dan mulai membangun semua sarana prasana yang telah dituangkan dalam sembilan agenda prioritas atau Nawacita oleh Presiden Jokowi. Kesemuanya itu perlu dilindungi dari serangan siber. Menurut teori pemberdayaan bahwa pelibatan komunitas siber untuk ambil bagian dalam melindungi negara ini dari serangan siber merupakan suatu hal yang wajib dilakukan karena komunitas siber ini mempunyai kekuatan di dalam diri mereka masing-masing dan ini merupakan suatu sumber kreativitas. Menurut teori pemberdayaan tersebut bahwa dengan pemberdayaan komunitas siber, mereka akan memperoleh keterampilan, pengetahuan, dan kekuasaan yang cukup untuk mempengaruhi kehidupannya dan kehidupan orang lain yang menjadi perhatiannya.

Komunitas siber harus merasa memiliki negara ini, karena pendiri bangsa ini sudah bersusah payah berjuang meraih kebebasan dari belenggu penjajah dengan waktu yang sangat panjang. Komunitas siber diharapkan memiliki kesadaran untuk menjaga dan membangun bangsa ini sesuai

²²Arif Rahman, Selain Listrik, BSSN Telah Petakan 10 Infrastruktur Kritis”, dalam

<https://cyberthreat.id/read/1929/> html, 5 Agustus 2019, diakses pada 30 Oktober 2020.

talenta yang dimiliki, jangan berpikir menghancurkan bangsa ini dengan kemampuan dan kepintaran yang dimiliki.

Saat ini sebagaimana yang telah dijelaskan sebelumnya bahwa perkembangan TIK sudah demikian pesat, sehingga ancaman di ranah siber terhadap IIKN akan berjalan secara seimbang mengikuti perkembangan tersebut. BSSN, kelembagaan terkait, Mabes TNI, Mabes Angkatan Polri yang memiliki *Cyber Operation Center* dan juga pihak swasta yang bergerak di bidang TIK telah melaksanakan pemantauan setiap harinya terhadap infrastruktur informasi kritis yang dimilikinya, namun pengamatan dan pelaporan hasil operasi ini belum terintegrasi dengan baik serta belum ada kerja sama dan saling berkolaborasi. Tugas yang dilaksanakan sesuai dengan aturan yang dikeluarkan masing-masing Lembaga atau satuan tersebut.

Saat ini dan kedepan, serangan siber akan selalu meningkat, perang terhadap siber perlu direncanakan baik antara pemerintah, Lembaga terkait dan pihak swasta di bidang TIK. Meningkatnya serangan siber akhir-akhir ini, tidak bisa diatasi oleh lembaga-lembaga resmi

pemerintah saja tetapi keterlibatan komunitas siber sangat dibutuhkan. Perlunya ada kolaborasi antar pemerintah, pihak swasta dan komunitas siber.

Dalam pernyataan Letjen TNI JS. Prabowo bahwa perang semesta kini dan dimasa depan tidak mesti dilakukan dengan mobilisasi penduduk “habis-habisan” untuk diperankan sebagai kombatan dalam pertempuran²³. Pernyataan ini sangat relevan dengan kegiatan siber saat ini, bahwa komunitas siber memang bukan kombatan, namun dapat melemahkan sistem TIK yang berdampak pada pemerintahan dan sosial masyarakat.

Komunitas siber yang tersebar baik di jalur formal seperti lembaga resmi pemerintah antara lain di BSSN, Kelembagaan, Satsiber TNI, Angkatan, Polri, pihak swasta dan juga komunitas siber yang berada di jalur non formal, bisa bersama-sama bersatu melakukan pencegahan dan juga mitigasi terhadap serangan siber.

Dari pernyataan “Sun Tzu” yang sudah disampaikan sebelumnya bahwa perang itu merupakan seni, seni tertinggi adalah tanpa melaksanakan pertempuran. Teori ini sebagai gambaran bahwa untuk bisa meraih kemenangan tidak harus berperang, namun

²³J.Suryo Prabowo, Pokok-Pokok Pemikiran tentang Perang Semesta (Cetakan Ke tiga), (Jakarta: PT. Tamaraprint Indonesia, 2019), hal.39.

dengan cara diplomasi atau menyerang tanpa menggunakan senjata dan tidak melibatkan banyak prajurit. Ini kalau dilihat sangat relevan dengan adanya serangan siber yang tidak memerlukan senjata namun dapat membawa korban jiwa manusia seperti peristiwa di Ukraina 2017²⁴.

Saat pandemi Covid ini, bukan saja virus Covid yang dapat membunuh manusia, namun serangan *ransomware* terhadap sistem komputer rumah sakit yang dapat mengambil kendali komputer sehingga pengguna tidak bisa mengakses komputer tersebut. seperti serangan di salah satu rumah sakit di Jerman sehingga membuat seorang wanita kehilangan nyawanya²⁵.

Sejarah Indonesia telah membuktikan bahwa kemerdekaan yang diperoleh saat ini merupakan perjuangan seluruh rakyat Indonesia pada waktu itu. Semua warga negara ikut berjuang saling bantu dan bahu-membahu terlibat dalam perjuangan untuk membantu TKR melawan penjajah. Jenderal Soedirman beserta pasukannya dan rakyat masuk ke hutan melaksanakan perang gerilya untuk menyerang pasukan Belanda.

Serangan umum 1 Maret 1949 merupakan peristiwa yang mengangkat nama bangsa Indonesia dimata dunia saat itu dan telah membuktikan bahwa bangsa ini masih memiliki tentara adalah Peristiwa yang membuat dilaksanakannya konferensi meja bundar (KMB) di Belanda pada tanggal 23 Agustus-2 November 1949, yang salah satu isi perjanjiannya adalah : Belanda mengakui kedaulatan kepada Republik Indonesia Serikat pada bulan Desember 1949. Berkat perjuangan seluruh warga negara maka apa yang telah dinanti-nantikan cukup lama akhirnya tercapai juga. Perang gerilya yang dilaksanakan saat itu merupakan kerjasama (Tentara Keamanan Rakyat) TKR sekarang TNI dengan rakyat. Jenderal A.H Nasution punya handil besar dalam memberikan masukan kepada Jenderal Soedirman untuk melaksanakan taktik-taktik perang gerilya. Jabatan Jenderal A.H Nasution ketika itu sebagai wakil Panglima TKR yang dilantik pada Februari 1948²⁶.

Keberhasilan dari perang gerilya tersebut menjadi dasar yang kuat untuk Indonesia dimasa kini dalam membuat

²⁴Andy, "Serangan siber 2017 di Ukraina" dalam https://en.m.wikipedia.org/wiki/2017_cyberattack_s_on_Ukraine, 20 Juni 2017, diakses 30 Oktober 2020

²⁵Dedy D. Nasution, "Wanita Jerman Meninggal Akibat Serangan Ransomware" dalam

<https://republika.co.id/berita/qgtv6l383>, 18 September 2020, diakses pada 3 November 2020

²⁶Rusman Siregar, "Jenderal Besar AH Nasution, Ahli Strategi Perang Gerilya Diakui Dunia," 9 Februari 2019, diakses pada 11 November 2020

aturan perundang-undangan agar dalam menghadapi segala ancaman dapat melibatkan seluruh sumber daya yang dimiliki.

Undang-undang yang telah ada dan berisikan tentang keterlibatan seluruh komponen bangsa dalam perang semesta yaitu mulai dari UUD 1945 pasal 30 ayat 1 berbunyi “Tiap-tiap warga negara berhak dan wajib ikut serta dalam usaha pertahanan dan keamanan negara.” Jika diartikan bahwa pasal tersebut ditujukan kepada setiap warga Indonesia memiliki hak dan kewajiban yang sama untuk ikut ambil bagian dalam pertahanan negara ²⁷.

Pada pasal 30 ayat 2 berbunyi: “Usaha pertahanan dan keamanan negara dilaksanakan melalui sistem pertahanan dan keamanan rakyat semesta oleh Tentara Nasional Indonesia dan Kepolisian Negara Republik Indonesia, sebagai kekuatan utama, dan rakyat, sebagai kekuatan pendukung.”

Kemudian pada undang-undang no 3 tahun 2002 tentang Pertahanan Negara, pada BAB I, Pasal I ayat 2 berbunyi: “sistem pertahanan negara adalah sistem pertahanan yang bersifat semesta yang melibatkan seluruh warga negara, wilayah,

dan sumber daya nasional lainnya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah, dan keselamatan segenap bangsa dari segala ancaman”.

Selanjutnya di dalam buku putih pertahanan Indonesia 2015 hal. 28 menyatakan bahwa : pertahanan negara Indonesia diselenggarakan dalam suatu sistem pertahanan semesta. Bentuk pertahanan yang dikembangkan melibatkan seluruh warga negara, segenap sumber daya, wilayah dan sarana prasarana nasional, yang telah dipersiapkan secara dini oleh Pemerintah, serta diselenggarakan secara total, terpadu, terarah dan berlanjut.

Sistem pertahanan semesta mengintegrasikan pertahanan militer dan pertahanan nirmiliter, melalui usaha membangun kekuatan dan kemampuan pertahanan negara yang kuat dan disegani serta memiliki daya tangkal yang tinggi. Dipersiapkan secara dini berarti sistem pertahanan semesta dibangun secara berkelanjutan dan terus-menerus, untuk menghadapi berbagai jenis ancaman baik ancaman militer, nonmiliter, maupun hibrida.

²⁷GTT, “UUD Pasal 30 Ayat 1: Makna dan Wujud Pelaksanaannya,” 11 September 2020, diakses pada tanggal 7 November 2020

Berbagai jenis ancaman ini secara akumulatif dapat dikelompokkan dalam bentuk ancaman nyata dan belum nyata²⁸.

Dari beberapa teori dan undang-undang yang dimiliki saat ini tentang pelibatan warga negara untuk ikut serta dalam perang semesta merupakan kewajiban mutlak, karena sejarah telah membuktikannya. Komunitas siber merupakan bagian dari warga negara, yang sudah semestinya wajib terlibat didalam perang semesta demi menegakkan kedaulatan dan harga diri bangsa ini dari semua ancaman keutuhan negara kesatuan Republik Indonesia.

Kebijakan pertahanan negara diimplementasikan melalui berbagai upaya dalam pengelolaan sumber daya dan sarana prasarana nasional guna mengatasi berbagai bentuk ancaman. Oleh sebab itu Pemberdayaan komunitas siber dalam pertahanan negara diarahkan untuk memelihara dan mengembangkan seluruh kekuatan dan potensi pertahanan negara secara terpadu dan terarah dengan melibatkan seluruh warga negara, serta memanfaatkan seluruh sumber daya dan sarana prasarana nasional serta seluruh

wilayah negara untuk selalu siap menjadi bagian dari sistem pertahanan negara.

Pemberdayaan komunitas siber dalam pertahanan negara juga bertujuan untuk meningkatkan kesiapsiagaan secara terintegrasi guna menghadapi situasi kontijensi dan eskalasi ancaman sebagai dampak dari dinamika perkembangan lingkungan strategis²⁹.

Dalam konteks ancaman siber yang meningkat saat ini, maka alasan pemberdayaan komunitas siber seyogyanya menjadi fokus utama oleh pemerintah, kelembagaan dan pihak swasta terkait bidang TIK yang selama ini belum menjadi prioritas untuk diperdayakan ditengah-tengah banyaknya serangan siber saat ini. Prioritas pemberdayaan komunitas siber ini bertujuan untuk dapat mengambil bagian dalam menjaga dan mengamankan IKN dari serangan siber yang dampaknya sangat dasyat dan bisa meruntuhkan suatu negara jika tidak diantisipasi lebih awal.

Pemberdayaan Komunitas Siber

Pemberdayaan Komunitas siber bertujuan untuk membentuk manusia yang mandiri serta meningkatkan standar hidup dan memberi kesadaran akan kebebasan setiap

²⁸Ryamizard Ryacudu, Buku Putih Pertahanan Indonesia 2015, (Cetakan ketiga) (Jakarta:

Kementerian Pertahanan Republik Indonesia, 2105), hal.28.

²⁹*Ibid*, hal.45.

orang. Orientasinya pada komunitas yang tidak berdaya. Pemberdayaan komunitas siber merupakan suatu usaha agar komunitas siber dapat bermanfaat bagi negara guna mencegah dan menjaga IIKN dari serangan siber.

Didalam undang-undang no. 23 tahun 2019 tentang PSDN, pasal 1 ayat 4 menyatakan bahwa sumber daya manusia adalah warga negara yang memberikan daya dan usahanya untuk kepentingan bangsa dan negara. Komunitas siber merupakan warga negara yang mempunyai kemampuan di bidang TIK yang dapat digunakan untuk kepentingan nasional.

Pemerintah dalam hal ini kementerian pertahanan semestinya mengambil langkah *preventif* dengan cepat untuk bisa mengelolah, mengarahkan dan mengakomodir komunitas siber untuk dapat dibentuk sebagai komponen pendukung yang siap digunakan untuk kepentingan pertahanan negara dalam menghadapi perang semesta³⁰.

Agar pemberdayaan komunitas siber dapat berjalan sesuai yang diharapkan maka perlu adanya campur tangan baik

pemerintah maupun swasta yang terkait bidang TIK untuk melaksanakan kegiatan pembinaan dalam meningkatkan kemampuan komunitas siber menjaga IIKN dari serangan siber.

Pemberdayaan komunitas siber ini menurut 'Talcots Parsons' merupakan upaya untuk orang mendapatkan ketrampilan, pengetahuan dan kekuasaan yang cukup dapat mempengaruhi kehidupannya dan kehidupan orang lain³¹.

Dengan pemberdayaan komunitas siber maka kemampuan yang dimiliki dapat berkembang dengan adanya kegiatan-kegiatan yang diikuti, disamping itu akan memperoleh keuntungan yang dapat mempengaruhi kehidupan komunitas siber itu sendiri.

Dalam pemberdayaan komunitas siber, langkah pertama yang dilaksanakan oleh Pemerintah dan pihak swasta antara lain melaksanakan kompetisi siber. Kompetisi ini merupakan upaya meminimalisir kegiatan negatif pemanfaatan siber oleh para peretas (*hacker*). Kompetisi ini merupakan ajang lomba keamanan siber yang secara khusus

³⁰Joko Widodo, "Undang Undang Republik Indonesia Nomor 23 Tahun 2019 Tentang Pengelolaan Sumber Daya Nasional Untuk Pertahanan Negara," dalam https://www.jogloabang.com/site/default/files/dokumen/uu_23_2019_pengelolan_sumber_daya_nasional_untuk_pertahanan_ne

gara.pdf, 24 Oktober 2019, diakses 12 November 2020.

³¹Aletheia Rabbani, "Pengertian Pemberdayaan Menurut Ahli," dalam <https://sosiologi79.blogspot.com/2017/07/pengertian-pemberdayaan-menurut-ahli.html> 12 Juli 2017, diakses 14 November 2020

fokus pada aspek operasional pengelolaan dan perlindungan layanan dan infrastruktur sistem informasi.

Tujuan lain yang didapat dari adanya kompetisi siber ini adalah nantinya pemerintah mempunyai data yang otentik tentang keberadaan komunitas siber, sehingga dalam melakukan pembinaan terhadap komunitas siber ini akan lebih mudah.

Penyelenggara kegiatan yang mewakili pemerintah dan peserta sudah bertemu muka dan berinteraksi langsung dengan komunitas siber yang terkesan selalu tertutup. Kompetisi ini menjadi wadah positif bagi para peminat dunia siber di Tanah Air. Sebab, komunitas siber yang sebagian besar anak-anak muda ini sangat pintar dan punya potensi dalam hal *security sistem*. Bila tidak diarahkan, bisa menjadi tidak terkendali.

Mereka ini rata-rata melakukan kegiatan meretas hanya untuk menunjukkan eksistensi bahwa mereka ada dan mempunyai kemampuan seperti mengambil uang di bank dan bahkan ada yang dapat membuat suatu negara runtuh dan butuh waktu lama untuk pemulihan. Kegiatan kompetisi siber, diharapkan lebih sering dilakukan dan memberikan *reward / insentif* yang layak bagi pemenang sehingga dapat

menunjang kehidupan mereka dan menjadi tantangan tersendiri bagi yang belum juara.

Harapannya dengan mengikuti kompetisi siber ini, semua komunitas akan tertantang untuk lebih giat belajar dan mengembangkan dirinya untuk menghadapi kompetisi berikutnya. Hal ini akan menjadikan komunitas siber lebih berguna bagi dirinya dan juga masyarakat.

Bagi pemenang lomba, pemerintah dapat memberikan fasilitas yang layak dengan memanfaatkan kemampuan mereka untuk bekerja sama dalam menjaga IKN dari serangan siber. Bagi komunitas siber yang mau bekerja sama dengan pemerintah diberikan *take homepay* yang sesuai dengan pekerjaan mereka. Namun sebelum bekerjasama dengan pemerintah, komunitas siber yang belum melaksanakan pelatihan belanegara wajib melaksanakan pelatihan belanegara, agar jiwa nasionalisme mereka dapat terbentuk dengan sepenuhnya untuk membela negara.

Mereka nantinya dididik untuk menjadi komponen pendukung di negara ini baik masa damai maupun masa perang. Kegiatan lain yang dilaksanakan pemerintah dan swasta adalah melaksanakan *forum group discuss* (FGD) seperti yang telah dilaksanakan oleh BSSN. BSSN mengundang komunitas siber untuk saling bekerja sama

dan berkolaborasi untuk mewujudkan ketahanan nasional di ranah siber. Yang disampaikan dalam FGD tersebut adalah saat ini informasi sudah menjadi sebuah komoditas yang sangat penting.

Masyarakat yang sudah berada dalam tataran “information-based society”, sebuah komunitas yang mampu mengakses dan menyediakan informasi secara cepat dan akurat, sehingga kebutuhan ketahanan siber untuk ketahanan nasional dari komunitas siber sangat diperlukan³².

Kegiatan FGD selain di BSSN, telah dilaksanakan juga di Pushansiber Kemhan, Satsiber TNI. Semua ini dilakukan untuk saling menukar informasi tentang perkembangan siber, ancamannya terhadap IKN dan kemampuan sumber daya manusia dan rencana-rencana pengembangannya.

Kalau dilihat dari kerjasama dan kolaborasinya, komunitas siber yang berlatar belakang formal telah memiliki wadah untuk saling berinteraksi namun untuk komunitas siber yang berlatar belakang non formal belum memiliki wadah tersebut. Perhatian terhadap Komunitas siber yang non formal hendaknya jangan diabaikan, karena mereka akan sangat berbahaya bagi bangsa ini. Hal ini sangat

relevan dengan teori dari Thomas Rid & Peter McBurney yang menyatakan bahwa "siber merupakan bagian dari persenjataan yang didesain untuk mengancam atau membahayakan fisik, fungsional atau mental suatu struktur atau sistem atau sistem kehidupan".

Hal ini yang membuat hadirnya pemikiran agar kegiatan komunitas siber non formal dapat terkontrol dan dapat memberikan dampak positif terhadap bangsa ini. Bila perlu dengan kemampuan yang dimiliki bisa dilatih khusus untuk bergabung bersama satuan-satuan Komando, yang tugasnya hanya untuk melaksanakan penetrasi ke daerah musuh, sehingga jalur komando kendali musuh, alat-alat komunikasi yang berbasis komputer namun tidak terhubung dengan internet dapat dilumpuhkan sebelum pasukan utama masuk. Ini mungkin salah satu cara juga agar mereka dapat berbuat yang terbaik bagi bangsa ini.

Pembinaan ini harus jelas, terarah dan terukur serta perlu mendapat perhatian yang lebih dari pemerintah terhadap komunitas siber yang belum terwadahi ini. Jika pembinaan berjalan dengan baik maka komunitas siber ini merasa lebih dihargai

³²Biro Hukum dan Humas, “BSSN Ajak Komunitas Keamanan Siber Indonesia Wujudkan Ketahanan Ranah Siber,” dalam <https://bssn.go.id/bssn-ajak->

[komunitas-keamanan-siber-indonesia-wujudkan-ketahanan-ranah-siber/](https://bssn.go.id/bssn-ajak-komunitas-keamanan-siber-indonesia-wujudkan-ketahanan-ranah-siber/), 7 Desember 2018, diakses 25 November 2020.

dibandingkan hanya melaksanakan perlombaan saja, dan Komunitas siber ini sewaktu-waktu dapat dengan mudah digerakkan dalam mendukung pemerintah baik dimasa damai maupun dimasa perang dalam belanegara sebagai komponen pendukung bangsa.

Hal ini menunjukkan bahwa pemberdayaan komunitas siber dalam melindungi wilayah negara dari serangan siber merupakan suatu kewajiban yang harus dilaksanakan secara sadar dan dengan penuh rasa tanggung jawab.

Komunitas Siber, Peran Pemerintah dan Swasta.

Komunitas siber adalah sumber daya manusia yang mempunyai latar belakang pendidikan formal dan non formal di bidang TIK, melaksanakan kegiatan interaksi di ranah siber (maya) yang bertujuan mendukung sesuatu yang diinginkan.

Keberadaan komunitas siber tersebar dimana saja dan jumlahnya sangat banyak, mereka semua pengguna *gadget*, komputer yang tersambung ke jaringan internet. Komunitas siber yang formal berada di BSSN, Pushansiber Kemhan, Mabes TNI, Mabes Angkatan, di Kelembagaan, Mabes Polri, Universitas, asosiasi profesi dan pihak swasta yang bergerak di bidang TIK seperti: asosiasi penyelenggaraan jasa

telekomunikasi, asosiasi satelit seluruh Indonesia, Asosiasi telepon, asosiasi penyelenggaraan data center Indonesia, asosiasi jasa internet Indonesia. Sedangkan Komunitas siber non formal keberadaannya tidak bisa diperkirakan, mereka bisa ada di rumah, café, taman, kereta, bandara dan dimana saja mereka inginkan. Di dunia nyata mereka sangat tertutup dan merahasiakan kemampuan yang dimiliki, namun jika dapat berinteraksi dengan mereka di dunia maya, mereka akan terbuka namun hanya kesesama komunitas mereka.

Komunitas siber yang berkemampuan sebagai *hacker* maupun *cracker* diketahui ada yang bekerja sebagai satpam, ojek online dan sebagainya untuk sekedar menunjukkan status mereka di dunia nyata.

Peran pemerintah dan lembaga serta swasta terkait bidang TIK dalam membina, membimbing dan mengarahkan komunitas siber agar ikut serta ambil bagian didalam pertahanan negara sebagai komponen pendukung yang dapat direalisasikan melalui program-program belanegara yang berada di Kementerian Pertahanan atau mereka dapat dijadikan *computer emergency response team* (CERT) untuk menangani masalah lokal, regional dan internasional bahkan bila perlu mereka dipermudah untuk direkrut sebagai Pegawai Negeri Sipil (PNS) dan ditempatkan

diseluruh Kementerian/Lembaga, TNI dan Polri dan bila dibutuhkan peluang untuk dilatih sebagai agen penetrasi ke daerah musuh bersama pasukan komando dapat dilaksanakan melalui rekrutmen khusus.

Peningkatan kegiatan lomba antar komunitas siber bagi yang formal maupun non formal, peningkatan kegiatan program FGD, pemberian *reward* / insentif secara rutin bagi komunitas yang membantu pemerintah dalam menjaga IIKN.

Aturan pemberdayaan komunitas siber ini sebenarnya sudah masuk didalam draf Undang-Undang (UU) Keamanan dan Ketahanan Siber versi Mei 2019, di dalam pasal 7 dan 8 yang menyebutkan bahwa penyelenggara keamanan dan ketahanan siber (KKS) terdiri atas lembaga negara, pemerintah pusat dan daerah, serta masyarakat yang terdiri dari internal organisasi dan penyediaan jasa KKS.

Lebih lanjut lagi, pasal 35 menyatakan bahwa setiap penyelenggara KKS harus melakukan upaya pembudayaan KKS agar kualitas pengelolaan risiko meningkat. Upaya pembudayaan ini termasuk pelaksanaan kegiatan promosi, bimbingan teknis dan/atau kegiatan ilmiah untuk

meningkatkan literasi dan kesadaran masyarakat terhadap KKS³³.

Diharapkan dengan hadirnya Undang-undang KKS kedepan maka Pemerintah baik pusat maupun daerah, masyarakat, kelembagaan serta swasta terkait bidang TIK, dapat saling bekerja sama dan berkolaborasi dalam mendukung pembinaan terhadap komunitas siber.

Kesimpulan

Kondisi perkembangan TIK yang sangat pesat saat ini, berdampak pada konsep pertahanan negara dalam menghadapi ancaman nirmiliter, dimana didalamnya terdapat ancaman siber. Pemerintah, Lembaga dan pihak swasta yang terkait bidang TIK telah berupaya melaksanakan pengamanan terhadap IIKN yang sering mendapatkan serangan.

Ada 10 IIKN yang telah ditetapkan oleh BSSN untuk diamankan dari serangan siber. Pemerintah, kelembagaan, universitas dan pihak swasta terkait TIK tidak sendiri dalam menggunakan peralatan siber (maya) tetapi ada sekelompok masyarakat juga yang menggunakan peralatan siber tersebut, mereka berada ditengah-tengah masyarakat. Mereka disebut dengan

³³Fetry Wuryasti, "Masyarakat Perlu Dilibatkan Dalam Kurangi Ancaman Kejahatan Siber," dalam <https://mediaindonesia.com/read/detail/349210>, 1 Oktober 2020, diakses pada 1 Desember 2020

komunitas siber, dimana komunitas siber ini ada yang formal dan non formal.

Pemerintah, kelembagaan, pihak swasta terkait TIK telah berupaya melaksanakan Pemberdayaan terhadap Komunitas siber dalam perspektif perang semesta untuk menghadapi serangan siber. Pemberdayaan dilaksanakan bagi semua komunitas siber melalui kegiatan lomba antar komunitas siber sekaligus melaksanakan penataan dan pendataan untuk digunakan sebagai komponen pendukung, kegiatan lainnya adalah peningkatan kegiatan *forum group discuss* (FGD), peningkatan program Pendidikan belanegara yang dilaksanakan oleh Kementerian Pertahanan, pemberian *reward/insentif* bagi komunitas yang terlibat kerjasama dengan pemerintah, kelembagaan, pihak swasta terkait TIK secara rutin. Kegiatan pemberdayaan komunitas siber oleh pemerintah dalam perspektif perang semesta, ditemukan beberapa kelebihan dan kekurangan, sebagai berikut:

Kelebihan

Pemerintah mendapat perkuatan dalam mengawasi dan mengamankan IIKN dari serangan siber.

Kejahatan siber di Indonesia dapat berkurang dengan bergabungnya

komunitas siber didalam program pemerintah. Komunitas siber sudah menjadi komponen pendukung, sewaktu-waktu dapat digerakkan untuk terlibat dalam perang semesta. Komunitas siber akan mendapat kehidupan yang lebih baik.

Kekurangan

Keberhasilan pemberdayaan komunitas siber bergantung pada semangat individu yang bergabung di dalamnya. Partisipasi setiap individu dalam komunitas siber berbeda-beda, sehingga akan menghambat program pemberdayaan.

Pemberdayaan komunitas siber merupakan wacana baru terutama bagi non formal, maka kemungkinan terjadi perbedaan pendapat antara satu orang dengan lainnya, sehingga muncul konflik baru. Kesiapan anggaran oleh pemerintah dapat menjadikan kendala tersendiri.

Dari kelebihan dan kekurangan yang ada, diperlukan rekomendasi agar pemberdayaan komunitas siber oleh Pemerintah dalam perspektif perang semesta dapat berjalan sesuai yang diharapkan, adapun rekomendasinya sebagai berikut:

Perlunya Badan Khusus dibawa BSSN atau diluar BSSN yang selalu fokus untuk membina dan mengarahkan komunitas siber non formal.

Perlunya adanya regulasi yang mengatur tentang pemberdayaan komunitas siber non formal dengan tujuan mendapatkan *reward* / insentif khusus secara rutin.

Perlunya adanya pembinaan khusus terhadap komunitas siber yang berjiwa militan agar dapat bergabung dalam satuan-satuan komando yang bertugas untuk melakukan penetrasi ke daerah musuh dalam menghancurkan sistem Komando dan kendali musuh.

Kerjasama pemerintah dengan negara-negara maju di bidang Pendidikan siber dalam rangka pembinaan dan pengembangan kemampuan komunitas siber.

Daftar Pustaka

Buku

Panjaitan, M. K. K. B. (2017). *Peran pemuda sebagai kader bela negara dalam mendukung pertahanan dan keamanan maritim*.

Prabowo, L. T. J. (2019). *Pokok-Pokok Pemikiran tentang Perang Semesta* (Cetakan Ke). PT. Tamaraprint Indonesia.

Tjahjanto, H. (2018). *Keputusan panglima tentara nasional indonesia No. Kep/555/VI/2018* (Vol. 1957).

Jurnal

Prasetyo, H. (2010). *Cyber Community, Cyber Cultures : Arsitektur Sosial Baru*

Masyarakat Modern. *Cyber Community, Cyber Cultures : file:///C:/Users/Andromeda/Downloads/190-Anonymous Manuscript for Review-322-1-10-20160425.pdf*

Triantoro, D. A. (2019). *Konflik Sosial dalam Komunitas Virtual di Kalangan Remaja. Jurnal Komunikasi.* <https://doi.org/10.20885>

Web site

Andy. (2017). *Serangan siber 2017 di Ukraina.* Wikipedia. https://en.m.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine

Brahima, S. (2017). *Global Cybersecurity Index (GCI) 2017.* (ITU, theInternational TelecommunicationUnion. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Bumibelumbulat“Komunitas Siber”, dalam <https://bumibelumbulat.wordpress.com/2016/05/21/komunitas-siber/>

Chairil, Tangguh. (2019). *Mewujudkan keamanan siber bagi Indonesia: Apa yang harus dilakukan?* The Conversation. <https://theconversation.com/mewujudkan-keamanan-siber-bagi-indonesia-apa-yang-harus-dilakukan-116813>

Erdianto, K. (2017). *Bagaimana Upaya Pemerintah Menangkal Maraknya Serangan Siber?* Kompas.Com. <https://nasional.kompas.com/read/2017/11/21/22411551/bagaimana-upaya-pemerintah-menangkal-maraknya-serangan-siber?page=2>

Asyraf, Fikri. (2016). *Berfikir strategic tentang serangan cyber,* dalam <https://mirmidons.wixsite.com/taktik/single-post/2016/11/23/Analisis-Perang-Cyber-Part-2-Akhir>

- GTT. (2020). UUD Pasal 30 Ayat 1: Makna dan Wujud Pelaksanaannya. Kumparan. <https://kumparan.com/user-campaign>
- Ikhsan. M. (2020). BSSN Sebut Keamanan Siber RI 2020 Naik, Serangan Meningkat. CNN Indonesia. <https://www.cnnindonesia.com/teknologi/20200925104631-185-550825/bssn-sebut-keamanan-siber-ri-2020-naik-serangan-meningkat>
- Nasution, D. D. (2020). Wanita Jerman Meninggal Akibat Serangan Ransomware. News. <https://republika.co.id/berita/qgtv6l383/wanita-jerman-meninggal-akibat-serangan-emransomwareem>
- Publik, B. K., & Humas, B. H. dan. (2018). (Publik & Humas, 2018). Badan Siber Dan Sandi Negara. <https://bssn.go.id/bssn-ajak-komunitas-keamanan-siber-indonesia-wujudkan-ketahanan-ranah-siber/>
- Ryacudu, R. (2015). *Buku Putih Pertahanan Indonesia* (Cetakan ke). Kementerian Pertahanan Indonesia. <http://sejarah.tni.mil.id/wp-content/uploads/2017/03/BUKU-PUTIH-PERTAHANAN-2015.pdf>
- Rabbani, Aletheia. (2017). Pengertian Pemberdayaan Menurut Ahli. SOSIOLOGI79. <https://sosiologi79.blogspot.com/2017/07/pengertian-pemberdayaan-menurut-ahli.html>
- Rahman, Arif. (2019). Selain Listrik, BSSN Telah Petakan 10 Infrastruktur Kritis. Cyberthreat.id. <https://cyberthreat.id/read/1929/Selain-Listrik-BSSN-Telah-Petakan-10-Infrastruktur-Kritis>
- Rasjid, E. Fadjar. (2014). Hacker Dan Cracker. UBAYA UNIVERSITAS SURABAYA. https://www.ubaya.ac.id/2018/content/articles_detail/148/Hacker-dan-Cracker.html
- Sullivan, Kevin, (2017). Fakta-Fakta Tentang Anonymous yang Bakal Bikin Kamu Tercengang. IDN TIMES. <https://www.idntimes.com/hype/fun-fact/kevin-sullivan/fakta-fakta-tentang-anonymous-yang-bakal-bikin-kamu-tercengang-c1c2/1>
- Siregar, Rusman. (2019). Jenderal Besar AH Nasution, Ahli Strategi Perang Gerilya Diakui Dunia. SINDONEWS.COM. <https://daerah.sindonews.com/artikel/jatim/6693/jenderal-besar-ah-nasution-ahli-strategi-perang-gerilya-diakui-dunia-1?showpage=all#:~:text=Oleh Jenderal AH Nasution%2C taktik,Gerilya Adalah Perang Rakyat Semesta%22.&text=Karier militernya dimulai tahun 1>
- Wuryasti, F. (2020). Masyarakat Perlu Dilibatkan Dalam Kurangi Ancaman Kejahatan Siber. Media Indonesia. <https://mediaindonesia.com/read/detail/349210-masyarakat-perlu-dilibatkan-dalam-kurangi-ancaman-kejahatan-siber>
- Wikipedia. (2020). IRC. Wikipedia Project. <https://id.wikipedia.org/wiki/IRC>
- Widodo, Joko. (2019). Undang Undang Republik Indonesia Nomor 23 Tahun 2019 https://www.jogloabang.com/sites/default/files/dokumen/uu_23_2019_pengelolaan_sumber_daya_nasional_untuk_pertahanan_negara.pdf,
- Yusgiantoro, Purnomo. “Pedoman Pertahanan Siber. Biro Tata Usaha Sekjend Kemhan” dalam [content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf](https://www.jogloabang.com/sites/default/files/dokumen/uu_23_2019_pengelolaan_sumber_daya_nasional_untuk_pertahanan_negara.pdf)