JUKIM
ADMI Jurnal Ilmiah Multidisiplin

JURNAL JUKIM Vol 3 No. 2 Maret 2024 | P-ISSN: 2829-0488 E-ISSN: 2829-0518, Hal. 83-93

ANCAMAN SIBER DAN PENGUATAN KEDAULATAN DIGITAL INDONESIA DARI PERSPEKTIF GEOPOLITIK DIGITAL

BRM. Yehizkia Y. Kristalia[1], Indra Wisnu Wibisono[2]
[1, 2] Hubungan Internasionali, Universitas Kristen Satya Wacana Salatiga

Article History
Received : 16-Febuari-2024
Revised : 17- Febuari-2024
Accepted : 30-Maret-2024
Published : 31-Maret-2024

Corresponding author*:
Indra Wisnu Wibisono

Contact:
Indra.wibisono@uksw.edu

Cite This Article:
Kristalia, B. Y. Y., & Wibisono , I. W. . (2024). ANCAMAN SIBER DAN PENGUATAN KEDAULATAN DIGITAL INDONESIA DARI PERSPEKTIF GEOPOLITIK DIGITAL. Jurnal Ilmiah Multidisiplin, 3(02), 83–93.

DOI:
https://doi.org/10.56127/jukim.v3i02.1584

Abstract: *Digital Sovereignty is a new form of state sovereignty in cyberspace. Cyberspace has no definite boundaries and is borderless. Although borderless, the state has the right and sovereignty over the utilization of its cyberspace as an integral part of state sovereignty. Indonesia has taken significant steps in digitizing cyberspace and has become a country with great cyber sovereignty in line with the high level of cyberspace usage by its citizens. This paper aims to look at the various dynamics that exist in cyberspace, especially seeing digital space as a new geopolitical arena. The concept of digital geopolitics is theoretically a derivative concept of geopolitical studies that explains the relationship between geography and cyberspace as well as politics or the role of government policies in it. Indonesia's cyberspace is currently attracting the attention of many people, especially when viewed from cases of cyber threats experienced such as data breaches that attack and harm many public sectors in Indonesia. This research was conducted using a qualitative descriptive method to see the cyber threats that occur in Indonesia, especially in the public sector and strengthening Indonesia's digital sovereignty from a digital geopolitical perspective. The results of this study illustrate that there are many cyber threats that occur in Indonesia, especially in the public sector. The government as an actor who has digital sovereignty responds to this phenomenon through the creation of various Digital regulations to strengthen Indonesia's cyber sovereignty spaces. Cyber space as a new geopolitical arena or what is referred to as Digital geopolitics must get more serious attention, especially in the implementation of various regulations related to cyber space.*
Keywords: *Digital Sovereignty, Digital Geopolitics, Cyberspace*

Abstrak: Kedaulatan Digital merupakan bentuk baru dari kedaulatan negara yang berada di ruang siber. Ruang siber tidak memiliki batas yang pasti dan bersifat borderless. Meskipun borderless namun negara memiliki hak dan kedaulatan atas pemanfaatan ruang-ruang siber yang dimilikinya sebagai bagian integral dari kedaulatan negara. Indonesia telah mengambil langkah signifikan dalam digitalisasi ruang-ruang siber dan menjadi negara dengan kedaulatan siber yang besar sejalan dengan tingkat pemakaian ruang siber yang besar oleh warga negaranya. Tulisan ini bertujuan untuk melihat berbagai dinamika yang ada di ruang siber terutama melihat ruang digital sebagai sebuah arena geopolitik baru. Konsep geopolitik digital secara teoritis merupakan konsep turunan dari kajian geopolitik yang menjelaskan tentang keterkaitan antara geografis dengan ruang siber serta politik atau peran, kebijakan pemerintah didalamnya. Ruang siber Indonesia dewasa ini menarik perhatian banyak kalangan terutama jika dilihat dari kasus-kasus cyber threat yang dialami seperti pembobolan data yang menyerang dan merugikan banyak sektor publik di Indonesia. Penelitian ini dilakukan menggunakan metode deskriptif kualitatif untuk melihat ancaman siber yang terjadi di Indonesia terutama pada sektor publik dan penguatan kedaulatan digital Indonesia dilihat dari perspektif geopolitik digital. Hasil dari penelitian ini menggambarkan bahwa terdapat banyak sekali ancaman siber yang terjadi di Indonesia terutama pada sektor-sektor publik. Pemerintah selaku aktor yang memilki kedaulatan digital merespon feneomena ini melalui pembuatan berbagai macam regulasi Digital untuk menguatkan ruang-ruang kedaulatan siber Indonesia. Ruang siber sebagai arena geopolitik baru atau yang disebut sebagai geopolitik Digital harus mendapatkan perhatian lebih serius lagi terlebih dalam implementasi berbagai regulasi terkait ruang siber.
Kata Kunci: Kedaulatan Digital, Geopolitik Digital, Cyberspace

PENDAHULUAN

Kedaulatan merupakan kekuasaan tertinggi negara yang diturunkan dalam hak-hak berdaulat (sovereignty right) dan merupakan hak yang hanya dimiliki oleh negara (Adolf, 2011). Konsep kedaulatan modern muncul pasca Perjanjian Westphalia dimana negara merupakan aktor utama yang memiliki hukum yang mendukung dan ditentukan oleh legislasi, kemampuan negara yang mengikat, serta mempunyai keabsahan untuk menggunakan kekuatannya (Amsir, 2021). Dalam dinamika global yang terus mengalami perkembangan terutama dengan hadirnya revolusi teknologi dan informasi menciptakan

sebuah transfomasi baru bagaimana konsep kedaulatan tidak hanya bersinggungan dengan pemanfaatan ruang-ruang atau wilayah teritorial. Relevansi dari perkembangan teknologi yang meningkat dengan konsep kedaulatan itu sendiri ada pada ruang interaksi baru yang terbentuk melalui internet dan berkembang pesat di tengah perkembangan masif teknologi yang kemudian melahirkan terminologi kedaulatan digital. Konsep kedaulatan digital atau kedaulatan siber menurut Piere Belangger, 2020 mengargumentasikan bahwa "digital sovereignty is a control of our present and destiny as manifested and guided by the use of technology and computer network" (Gueham, 2017). Dalam perkembanganya masih terdapat beberapa hal abstrak terkait dengan kedaulatan digital ini, terutama dalam aspek intervensi peran pemerintah dalam mengatur ruang internet sebagai sebuah negara yang berdaulat. Perubahan kedaulatan klasik, kedaulatan modern (modern state), menjadi kedaulatan digital akan menjadi tantangan baru bagi suatu negara dalam menyatakan kedaulatannya sebagai negara yang merdeka dan berdaulat

Indonesia sebagai sebuah negara dengan ruang siber yang besar jika dilihat dari jumlah pemakai ruang digital memiliki perhatian serius dalam penguatan pemanfaatan ruang ini. Presiden Republik Indonesia ke-7 Joko Widodo dalam salah satu pidatonya di kegiatan pengarahan kepada peserta Program Pendidikan Singkat Angkatan (PPSA) XXIV dan alumni Program Pendidikan Reguler Angkatan (PPRA) LXV Tahun 2023 Lembaga Ketahanan Nasional (Lemhannas) di Istana Negara, Jakarta, pada Rabu, 4 Oktober 2023 menyatakan bahwa "Kita harus melindungi kedaulatan digital kita dan betul-betul kita pertahankan yang namanya kandungan lokal, barang lokal. Kalau enggak bisa 100 persen barang kita, ya paling tidak 90 persen, 80 persen kandungan lokalnya. Jaga betul yang namanya aset digital kita, jaga betul data, informasi, akses pasar, semuanya,". Hal ini menandakan keseriusan pemerintah dalam memperkuat kedaulatan digital. Beberapa ancaman siber yang sering terjadi di Indonesia adalah serangan malware yang merupakan sebuah perangkat suatu program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer (CSIRT Kemhan RI, 2021). Malware sangat mengancam terutama pada komputer-komputer tidak hanya milik pribadi melainkan milik pemerintah yang menyimpan aset-aset strategis negara. Salah satu bentuk malware berbahaya yang paling sering dijadikan sebagai alat cyberattack adalah ransomware. Menurut Microsoft.Com, ransomware adalah sejenis program jahat, atau malware, yang mengancam korban dengan menghancurkan atau memblokir akses ke data atau sistem penting hingga tebusan dibayar. Malware dan ransomware sebenarnya menggunakan virus atau cara yang sama, yang membedakan hanya pada permintaan tebusan oleh hacker. Potensi ancaman siber di masa mendatang yang paling ekstreme adalah ancaman cyber warfare yang tindakan serangan siber terorganisir dan sistematis yang dapat dilakukan oleh aktor negara atau organisasi internasional atau aktor-aktor dalam hubungan internasional lainya untuk menyerang dan melemahkan suatu negara dengan cara merusak komputer atau jaringan informasi negara lain melalui virus komputer atau serangan penolakan layanan (Utami, 2022). Ancaman-ancaman siber pada era digital ini akan terus berkembang sehingga perlu menjadi urgensi bagi pemerintahan Indonesia dalam memperkuat tingkat keamanan siber (cyber security) melalui pertahanan siber yang kuat sehingga kedaulatan digital negara dapat tercapai dan terealisasikan.

Keinginan Indonesia dalam memperkuat kedaulatan digital memiliki keterkaitan dengan geopolitik, terutama dalam geopolitik digital. Sederhananya, kedaulatan digital yang disuarakan oleh pemerintah Indonesia sebenarnya merupakan kepentingan geopolitik Indonesia dalam ruang siber, bukan seperti geopolitik yang kita ketahui berkaitan dengan geografis secara fisik. Menurut Ramadhan (2021) "Cyberspace has now become one of the most important domains in terms of geopolitics". Faktor yang kemudian mempengaruhi aspek ruang siber menjadi salah satu isu di geopolitik, salah satunya ada pada ancaman-ancaman yang dapat diberikan oleh negara lain seperti cyber attack, cyber terrorism, dan cyber threat lainnya seperti malware atau ransomware yang dilakukan oleh negara lain. Oleh karena itu, geopolitik yang menggunakan konsep lama seperti letak geografis dan sumber daya alam perlahan mulai bertransformasi kepada sumber daya digital seperti jaringan informasi strategis negara. Konsep geopolitik mengalami perkembangan dengan melahirkan istilah geopolitik digital karena perkembangan teknologi yang menciptakan ruang baru yaitu ruang siber atau cyberspace dimana menjadi wilayah atau domain baru bagi arena geopolitik global. Tulisan ini ingin melihat bagaimana kondisi kedaulatan digital denan berbagai dinamika ancaman yang ada dan bagaimana pemerintah melihat ruang siber ini sebagai arena geopolitik baru untuk diperkuat guna kepentingan nasional.

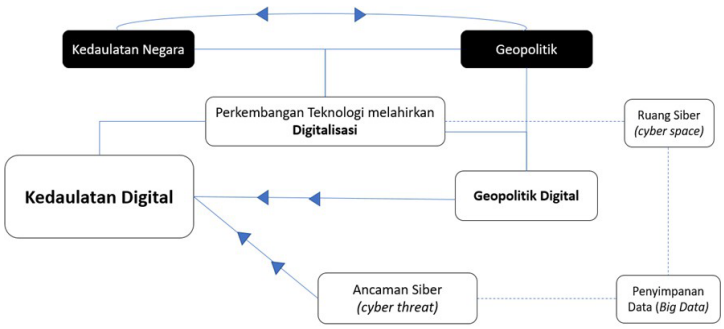
Tulisan ini menggunakan tiga jurnal terdahulu dalam mencari research gap. Jurnal pertama berjudul "Perubahan Geopolitik dan Ketahanan Nasional: Sebuah Penjelajahan Teoretikal" yang ditulis oleh Kusnanto Anggoro, Ph.D. pada tahun 2017 yang menerangkan bahwa perubahan geopolitik masa kini dipengaruhi oleh perkembangan teknologi yang menggeser tujuan dari geopolitik yang awalnya ingin

menguasai suatu wilayah karena adanya sumber daya alamnya dan beralih menjadi keinginan negara dalam menguasai akses yang ada. Tindakan negara yang ingin mendominasi akses ini kemudian mempengaruhi beberapa aspek domestik seperti krisis kepribadian nasional negara yang ter-kolonialisme dan sulitnya memastikan kedaulatan suatu negara. Dalam jurnal yang kedua yang ditulis oleh Iqbal Ramadhan dengan judul Implikasi "Ruang Siber Terhadap Geopolitik Negara" yang dipublikasi pada tahun 2021 menjelaskan relevansi dan keterkaitan antara ruang siber dengan geopolitik, penelitian ini melihat bahwa ruang siber juga merupakan ruang yang berada dalam kekuasaan negara sehingga akan sangat berkaitan erat dengan kepentingan-kepentingan negara, sehingga kehadiran ruang siber memberikan dampak, resiko, dan konsekuensi yang nyata pada geopolitik suatu negara. Jurnal terakhir dengan judul "Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia" yang ditulis oleh Muhammad Alfi, dkk pada tahun 2023 menganalisa beberapa peran Indonesia dalam transformasi digital yang jelas akan menghadapi berbagai resiko seperti kebocoran big data yang dialami oleh beberapa sektor publik, analisa ini menjelaskan bahwa tingkat keamanan siber di Indonesia masih sangat kurang dan harus menjadi urgensi bagi pemerintah.

Ketiga penelitian terdahulu menjadi dasar dalam tulisan ini untuk melihat kedaulatan digital Indonesia dan perubahan arena geopolitik yang menyesuaikan dengan tantangan global era digital. Tulisan ini juga berusaha menggambarkan bagaimana urgensi negara dalam melaksanakan implementasi dari penguatan siber (cyber security dan cyber defense) karena isu siber akan menjadi isu konflik masa depan yang sulit dihadapi jika tidak dipersiapkan sejak sekarang. Mempertahankan kedaulatan merupakan kewajiban utama suatu negara. Di era digital ini, ditengah perkembangan global yang semakin terdigitalisasi membuat negara harus berfokus juga pada penciptaan kedaulatan dalam ranah digitalnya.

METODE PENELITIAN

Penelitian ini menggunakan pendekaan deskriptif kualitatif untuk menganalisa dan menggambarkan ancaman siber di Indonesia dan pembangunan kedaulatan igital berdasarkan perspektif geopolitik Digital. Penelitian ini menggunakan metode pengambilan data melalui studi literatur dimana data-data yang digunakan daam penelitian diperbandingkan dari sumber-sumber referensi yang berasal dari jurnal, buku-buku, artikel ilmiah, peraturan perundang-undangan dan berbagai macam artikel ilmiah serta berita dari situs-situs yang kredibel. Simplifikasi dari penelitian ini apat dilihat dari kerangka berpikir berikut ini**.**



Gambar 1 : Kerangka Pikir

Kerangka pikir dalam tulisan ini ada pada dua isu yang saling mempengaruhi satu sama lain, yaitu kedaulatan negara atau *state sovereignty* dan geopolitik. Kedua isu ini kemudian sama-sama saling terpengaruh dengan adanya perkembangan teknologi dan digitalisasi yang tengah marak dan masif berkembang dalam dinamika global. Kedaulatan negara yang pada awalnya berupa sebuah kedaulatan yang bersifat fisik dan realistis bergeser pemaknaannya akibat dari kemajuan teknologi dan teritorial baru dalam ruang siber menjadi kedaulatan digital. Sedangkan Geopolitik yang sebelumnya merupakan konsep bersifat geografis fisik juga mengalami pergeseran akibat dari berkembangnya ruang baru dalam dinamika global yaitu ruang siber yang kemudian disebut sebagai geopolitik digital. Jika dilihat dari latar belakang kedua isu tersebut, perubahan yang terjadi diakibatkan oleh hal yang sama yaitu digitalisasi yang merupakan hasil dari perkembangan teknologi yang menciptakan ruang siber atau *cyber space*.

Dalam ruang siber tidak hanya menjadi sebuah wadah interaksi antar masyarakat melainkan juga sebagai ruang baru dalam menyimpan data-data pribadi maupun dimanfaatkan negara untuk menyimpan data-data rahasia milik negara. Dengan adanya data-data penting negara yang tersimpan dalam ruang siber, justru melahirkan sebuah ancaman baru yang mengancam data-data milik negara seperti malware dan ransomware serta, jika data itu berhasil diretas oleh aktor yang tidak bertanggung jawab dan menciptakan kebocoran data strategis negara maka akan dapat berakibat fatal bagi kelangsungan negara tersebut.
Menanggapi berbagai *cyber threat* yang terjadi, maka perlu adanya peran negara dalam menegaskan posisinya sebagai pemegang kepentingan dalam teritorialnya pada ruang siber. Mengingat juga bahwa keamanan data-data nasional maupun data pribadi warga negara yang tersimpan dalam ruang siber tidak hanya menjadi tanggung jawab pribadi, melainkan juga tanggung jawab negara sebagai sebuah negara yang memiliki hak-hak dalam mengatur teritorialnya terkhusus di ruang siber. Walaupun dalam ruang siber, batas-batas menjadi semakin kabur namun kedaulatan digital suatu negara perlu ditegakkan. Perspektif geopolitik digital digunakan dalam tulisan ini untuk menunjukkan betapa pentingnya kondisi geopolitik era digitalisasi. Geopolitik digital menjelaskan tentang kondisi dimana negara tidak hanya akan berfokus pada hal-hal terkait perang fisik, maupun perebutan minyak bumi dan sumber daya alam lainnya. Dinamika hubungan intermasional juga tengah berada dalam kondisi yang baru dan memerlukan penyesuaian dan pada akhirnya juga mempengaruhi geopolitik tiap negara, terkhusus pada bidang teknologi yang terus berkembang dan semakin meningkatnya konflik ruang siber. Konsep geopolitik digital ini mencoba untuk menjelaskan *the new era of Indonesia geopolitics*, dan seberapa berpengaruhnya terhadap kedaulatan negara melalui pemakaian ruang-ruang digital.

HASIL DAN PEMBAHASAN

Geopolitik Digital

Terdapat berbagai definisi tentang geopolitik, beberapa diantaranya ada definisi dari Colin Flint yaitu *"geopolitics as a study that connects a region's characteristics with its political dynamics".* Selain itu juga definisi geopolitik dari Saul B. Cohen adalah *"geopolitics as a constitutional science concerned with the management of territories through political doctrine"*. Dari beberapa definisi diatas dapat secara umum bahwa geopolitik berkaitan erat dengan pemanfaatan ruang, wilayah, dan teritorial serta berhubungan dengan politik negara. Konsep geopolitik tersebut masih menggunakan konsep teritorial yang berkaitan batas-batas negara yang jelas. Dalam perkembangan teknologi di era digitalisasi menciptakan fenomena pergeseran makna dan definisi tentang geopolitik yang mulai menyentuh dan menyesuaikan dengan perkembangan ruang digital. Sebagai akibatnya munculah ruang baru yang disebut dengan ruang siber atau *cyberspace* yang menjadi domain atau teritorial baru dengan batas-batas teritorial yang tiak jelas dan berlawanan dengan konsep geopolitik klasik. Menurut Martin Dodge dan Rob Kitchen, *"cyberspace as the geography of an information society"*. Ini terjadi akibat dari meningkatnya interaksi masyarakat yang saling berbagi informasi di ruang siber. Interaksi ini jika tidak dikontrol dan dikendalikan dengan baik oleh negara dapat menjadi potensi ancaman karena informasi yang tidak terkontrol atau palsu dan dimanipulasi dapat memecah belah suatu bangsa. Selain itu informasi-informasi penting strategis yang menjadi sumber daya pengambilan strategi kebijakan negara yang tidak dijaga dengan baik juga dapat membahayakan keselamatan negara dalam interaksi hubungan internasional yang anarkis.

Faktor penting yang menjadi kepentingan negara dalam ruang siber salah satunya ada pada big data atau data-data penting milik negara yang ada di ruang siber dimana negara sebagai entitas yang berdaulat memiliki kewajiban untuk mengatur serta membuat kebijakan untuk dalam menjamin keamanan big data tersebut terutama dari intervensi atau potensi kebocoran data. Sangat penting bagi negara untuk dapat merekonstruksi kepentingan keamanannya dalam ruang siber yang pada era digital ini yang rentan terhadap berbagai ancaman seperti *malware*, *ransomware* hingga *cyberwarfare*. Walaupun konsep geopolitik mengalami transformasi jauh dari yang awalnya bersifat fisik dan beruah menjadi sebuah konsep ruang siber tanpa adanya letak dan batas teritorial yang jelas, akan tetapi negara mau tidak mau menjadikan ruang siber hal penting dan sama besarnya dengan wilayah fisik (Ramadhan, 2021). Geopolitik digital merupakan sebuah konsep baru yang menjelaskan terkait hubungan antara faktor-faktor geografis digital atau ruang siber dengan kebijakan-kebijakan politik yang. Negara menjadi aktor utama pada konsep geopolitik ini sebagai pembuat regulasi dan entitas yang memiliki kepentingan untuk mengamankan ruang-ruang sibernya dari potensi gangguan dan ancaman aktor-aktor lain.

KEDAULATAN RUANG DIGITAL DI INDONESIA

Kedaulatan digital merupakan hal baru dalam kajian hubungan internasional yang terjadi akibat dari perkembangan teknologi yang masif dan dampaknya ada pada ruang baru yang tercipta yaitu ruang siber. Konsep kedaulatan Menurut C.F Strong, kedaulatan berarti superioritas yang dalam konteks kenegaraan mengisyaratkan adanya kekuasaan untuk membuat hukum (Annisa, 2023). Jika dilihat dari aspek geografisnya, maka superioritas negara terlihat jelas batas-batasnya dan wilayah kekuasaan negara terlihat jelas dalam bentuk fisiknya. Sedangkan akibat dari perkembangan teknologi yang menciptakan ruang baru yaitu ruang siber yang tidak memiliki batas negara yang jelas atau borderless, namun masyarakat atau warga negara berinteraksi dalam ruang siber, sehingga mengharuskan pemerintah untuk mempertegas otoritasnya dalam ruang siber. Maka, konsep kedaulatan perlu mengikuti perkembangan jaman yang ada dan bergeser menjadi kedaulatan digital. Menurut Kementerian Komunikasi dan Informatika Indonesia, kedaulatan digital adalah (negara) berkuasa sepenuhnya terhadap konten maupun peredaran informasi di dunia internet. Artinya, negara memiliki otoritas penuh dan superioritas di ruang siber sebagai wadah interaksi masyarakat yang baru dan negara memiliki tanggung jawab yang besar dalam menjaga keamanan terkhusus dalam bidang siber. Hal yang perlu dijaga dalam ruang siber ada pada beberapa tantangan sekaligus ancaman pada kedaulatan digitalnya seperti malware, ransomware, hingga cyberwarfare yang merupakan perang siber antar satu negara dengan negara lainnya, atau hegemonisasi suatu negara pada akses internet seperti perusahaan Google milik Amerika Serikat.

Implementasi kedaulatan digital Indonesia diuraikan menjadi empat bentuk oleh pemerintah, yang pertama adalah lewat pembentukan perundang-undangan. Konsep kedaulatan digital di Indonesia muncul dalam Pasal 2 UU ITE, melalui penegasan bahwa UU ITE berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam UU ITE, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia; yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia. Kedua, melalui kontrol terhadap konten, dimana pemerintah atau negara memiliki kewajiban untuk menjaga penggunaan informasi elektronik yang berisi hal-hal ilegal maupun terlarang dan negara memiliki kuasa untuk memutus akses-akses yang melanggar serta membahayakan keamanan siber. Kemudian, yang ketiga adalah kontrol terhadap data yaitu peranan negara dalam melindungi data-data informasi pribadi maupun data-data nasional yang bersifat rahasia milik negara seperti data-data milik sektor pelayanan publik KIP maupun BPJS yang jelas menyimpan berbagai data pribadi milik warga negara. Terakhir yaitu yang keempat merupakan pengembangan infrastruktur, dimana negara berperan dalam mengembangkan berbagai infrastruktur seperti telekomunikasi dan penguatan keamanan siber di Indonesia.

Di Indonesia, terjadi sebuah transformasi digital dimana layanan-layanan bagi masyarakat kini menggunakan internet dan akan menjadi tantangan tersendiri untuk kedaulatan digital Indonesia terutama jika pengelolaan big data tidak dilakukan secara mandiri dengan *server* yang berada diluar wilayah Indonesia. Penerapan dari menjaga kedaulatan dilakukan oleh para stakeholder, terdapat tiga stakeholder di lingkup pemerintahan. Pertama, pemerintah pusat yang bertugas untuk menjaga dan menciptakan kedaulatan digital Indonesia serta menjaga kepentingan nasional Indonesia dan menciptakan kemandirian digital. Kedua adalah pemerintah daerah yang bertugas menjaga sistem layanan publik seperti pada sektor kesehatan maupun perpajakan yang pada saat ini menggunakan layanan berbasis internet. Pemerintah daerah seperti pemerintah kota maupun kabupaten adalah pemerintahan yang paling dekat dengan masyarakat dan berhubungan langsung dengan berbagai layanan-layanan bagi masyarakat sehingga sebagai pihak yang secara langsung terlibat, pemerintah daerah juga memiliki peranan penting dalam menciptakan kedaulatan digital. Ketiga adalah ASN atau Aparatur Sipil Negara yang merupakan warga negara yang bekerja sebagai pegawai pemerintahan turut langsung menjadi aktor yang ikut bertanggung jawab dalam menciptakan kedaulatan digital. Hal ini dikarenakan ASN atau pegawai negeri adalah warga negara yang bekerja secara langsung dan merasakan transformasi digital yang terjadi di pemerintahan, sehingga peran dalam menjaga kedaulatan digital di Indonesia juga dipegang oleh ASN atau pegawai negeri.

Transformasi digital yang dilakukan oleh pemerintah Indonesia adalah segala jenis proses yang memanfaatkan teknologi digital (Condrobimo, 2023). Maksudnya adalah, transformasi digital adalah penggunaan teknologi dalam melakukan berbagai hal yang sebelumnya dilakukan secara analog atau fisik, sehingga berbagai sektor seperti pendaftaran, pembuatan KTP, dan berbagai bidang layanan masyarakat yang ada dialihkan ke digital. Sebenarnya, transformasi digital yang terjadi di Indonesia memberikan dampak baik terhadap kedaulatan digital Indonesia, hal ini dilihat melalui kemampuan

negara dalam mengembangkan kemandirian digitalnya dengan membentuk sebuah sistem-sistem digitalnya. Namun sebaliknya, transformasi digital juga membawa ancaman terhadap kedaulatan digital dimana transformasi digital ini tidak diikuti dengan peningkatan cyber security atau keamanan siber. Alasannya adalah berjalannya sistem ini, maka berbagai data-data pribadi maupun data nasional disimpan dalam ruang siber dan bila tingkat keamanan siber masih rendah, maka akan sangat berbahaya jika data tersebut dapat dibobol oleh oknum-oknum tidak bertanggung jawab, atau bahkan data tersebut dapat diambil oleh negara lain. Beberapa kasus kebocoran maupun pembobolan data sudah sering terjadi dialami oleh Indonesia dan akan terus berlanjut bila negara tidak bertindak, kedaulatan digital juga akan semakin sulit dicapai, terkhusus pada era perubahan transformasi digital yang kini menjadi salah satu program pemerintah.

Perlu disadari bahwa kini, kedaulatan digital merupakan salah satu aspek vital milik negara. Sehingga, kedaulatan digital dapat disamakan pentingnya dengan ketahanan dan keamanan militer. Pemerintah pusat memiliki berbagai program untuk menjaga kedaulatan digital Indonesia melalui transformasi digital yang tetap mempertahankan barang-barang atau identitas lokal serta mempersiapkan berbagai ancaman dan juga tantangan dalam menjaga kedaulatan digital Indonesia. Kedaulatan merupakan pride bagi suatu negara dan bila kedaulatan negara tercoreng atau bahkan sampai pada tahap negara tidak mampu menjaganya, maka akan menjadi suatu hal yang sangat memalukan. Oleh sebab itu, Indonesia perlu memperhatikan dinamika global yang kini mulai didominasi oleh teknologi dan bagaimana konflik masa depan akan terjadi. Indonesia perlu bersiap dengan segala tantangan yang akan dihadapi, salah satu caranya adalah dengan penguatan kedaulatan digital dan menyatakan posisi Indonesia yang kuat serta mampu bertahan dalam berbagai dinamika yang terjadi akibat dari pemanfaatan teknologi. Kedaulatan digital harus menjadi salah satu fokus utama pemerintahan Indonesia selanjutnya agar dapat mengimbangi berbagai kekuatan-kekuatan teknologi yang akan terus berkembang di dunia saat ini.

KEAMANAN SIBER DI INDONESIA

Perkembangan teknologi yang melahirkan ruang siber ternyata memberikan dampak fisik terhadap geopolitik, seperti dampaknya terhadap geopolitik negara dan juga dampak pada stabilitas wilayah geopolitiknya (Ramadhan, 2021). Perlu disadari, bahwa dalam pernyataan tersebut disebabkan oleh beberapa kejadian cyberwarfare yang telah berlangsung di dunia global, tepatnya di kawasan Timur Tengah dimana negara seperti Iran, Israel dan Arab Saudi saling melakukan cyber attack. Hal ini menunjukkan bahwa ancaman siber dan konflik masa depan seperti cyberwarfare perlahan-perlahan akan mendominasi dan negara mau tidak mau harus berfokus pada hal tersebut. Permasalahan utama geopolitik digital adalah pada sifat ruang siber yang borderless atau tanpa batas sehingga jika dilihat melalui perspektif kedaulatan negara, akan sulit bagi negara dapat mengatur teritorial yang tidak dikenali. Namun, hambatan tersebut dapat dipatahkan dengan keharusan negara untuk terlibat di ruang siber untuk mencapai tujuan kepentingan geopolitik walaupun akan sangat sulit untuk mencapai resolusi damai (Ramadhan, 2021). Agar geopolitik digital dapat benar-benar diimplementasikan, menurut Iqbal Ramadhan (2021) "Westphalianization is primarily concerned with promoting the establishment of state boundaries in cyberspace". Artinya, pembentukan batas-batas negara di ranah ruang siber, namun hal ini belum terealisasikan mengingat dinamika global belum benar-benar merasa ancaman yang nyata dari kehadiran ruang siber dan perang siber, belum seperti kehadiran nuklir pada masa perang dunia kedua dimana ratifikasi terkait perjanjian perang dunia dilaksanakan setelah banyak orang menjadi korban.

Lebih jauh lagi membahas geopolitik digital Indonesia, pemerintah sepatutnya menyadari berbagai ancaman-ancaman yang sebenarnya sudah terjadi dan menyerang keamanan siber milik negara, ruang siber di Indonesia saat ini berstatus merah dan pemerintah harus waspada akan ancaman yang jauh lebih berbahaya lainnya. Geopolitik merupakan bidang ilmu yang merelevansikan ruang atau teritorial dengan politik, sehingga dalam geopolitik digital, ruang yang dimaksud adalah ruang siber yang menampung banyak data, informasi dan sebagai wadah masyarakat berinteraksi. Pada era digitalisasi, ruang siber Indonesia dapat dikatakan tidak aman, hal ini dikarenakan banyak sekali kejadian, insiden maupun masalah terkait dengan serangan siber, malware dan juga ransomware yang diterima oleh pemerintah Indonesia yang jelas mengancam kedaulatan digital Indonesia. Berikut ini merupakan data mengenai serangan siber pada sektor publik yang diambil dari jurnal milik Muhammad Alfi, dkk dengan judul "Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia".

Tabel 1 : Data Serangan Siber Sektor Publik di Indonesia

Waktu	Jenis Sektor Publik	Peristiwa
Tahun 2017	Kesehatan	Insiden ransomware wannacry yang menargetkan Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais Jakarta. Malware ini menyerang ratusan server dan komputer, mengakibatkan gangguan serius terhadap operasional rumah sakit
Tahun 2020	Berbagai Sektor Publik yang menjalankan program Work From Home (WFH)	Serangan siber yang memanfaatkan isu pandemi Covid-19 pada Aplikasi Zoom, dimana aplikasi ini telah disisipi *Malicious Zoom* yang menggunakan pengkodean berisi modul *metasploit, adware*. Situs DPR RI (www.dpr.go.i d) sempat diretas, dimana peretas mengubah tampilan halaman depan website menjadi "Dewan Penghianat Rakyat). Peretasan tersebut dilatari adanya penolakan pengesahan UU Cipta Kerja (CNN Indonesia, 2020). 8 Mei 2023 Keuangan PT Bank Syariah Indonesia (BRIS) mengalami serangan ransomware dari kelompok *Lockbit*. Serangan tersebut melumpuhkan layanan ATM dan m-banking hingga lebih dari seminggu, sehingga menimbulkan kekhawatiran nasabah. Sementara itu, melalui dark web, Lockbit mengumumkan telah mencuri 15 juta data nasabah yang setara 1,5 terabyte dan meminta tebusan senilai US$ 20 juta
September 2021	Kesehatan	Data sertifikat vaksinasi Covid-19 tahap kedua milik Presiden Joko Widodo yang tersimpan di Sistem Peduli Lindungi, beredar di Twitter. Data yang beredar berisi informasi nama, nomor identitas kependudukan (NIK), tanggal lahir, tanggal vaksin, dan jenis vaksin. Kasus ini masuk kategori penyalahgunaan identitas orang lain untuk mengakses informasi pihak yang tidak terkait. Sejak itu, fitur akses informasi para pejabat pemerintah di Sistem Peduli Lindungi ditutup
Juli 2021	Keuangan	Perusahaan asuransi BRI Life mengalami serangan yang menyebabkan kebocoran 2 juta data nasabah atau setara 250 GB. Data yang bocor dikabarkan dijual secara online seharga US$ 7000 dalam format PDF, yang berisi foto KTP, rekening, NPWP, akte kelahiran, hingga rekam medis
Mei 2021	Kesehatan	Website Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan diduga mengalami peretasan. Serangan ini menyebabkan sekitar 279 juta data penduduk Indonesia bocor dan dijual dalam forum online Raid Forums oleh akun bernama "Kotz". Data yang bocor berisi NIK, nomor ponsel, email, alamat, hingga nominal gaji, yang dijual seharga 0,15 bitcoin

Sumber : (Alfi et al., 2023)

Data tersebut masih merupakan data yang terjadi hingga tahun 2021, pada tahun 2022 Indonesia dihebohkan dengan kasus Bjorka, sebuah akun dari dark web yang dimiliki oleh seseorang atau kelompok. Sosok bernama Bjorka ini mengklaim memiliki 26 juta history browsing milik pelanggan Indihome, 1,3 miliar data registrasi SIM Card, dan 105 juta data KPU (Dewi, 2022). Lalu, pada tahun 2023 BSSN mengeluarkan Lanskap Keamanan Siber Indonesia 2023 yang berisikan berbagai informasi tentang serangan siber dalam bentuk malware maupun ransomware yang telah ditangani oleh BSSN beserta penjelasan strategi keamanan siber untuk tahun 2024. Pertengahan tahun 2024, Indonesia dikejutkan dengan kasus ransomware yang menyerang PDN atau Pusat Data Nasional yang meminta

tebusan sebesar 8 juta US Dollar atau setara dengan 131 miliar Rupiah (WISANGGENI, 2024). Akibat dari kasus ransomware ini, berbagai layanan masyarakat seperti; Layanan Penerimaan Peserta Didik Baru (PPDB) mengalami gangguan, layanan digital Direktorat Jenderal Imigrasi Kementerian Hukum dan Hak Asasi Manusia tidak berfungsi, serta sebanyak 282 layanan instansi pemerintah terganggu (BBC News, 2024). Ruang siber Indonesia sangat terancam dengan keberadaan serangan-serangan siber yang masih tidak dapat ditangani dengan baik, jika pemerintah sudah melakukan upaya, nampaknya upaya tersebut masih belum mumpuni karena kasus-kasus dari tahun 2017 hingga 2024 masih terus berlanjut dan tidak berkurang sama sekali. Hal ini juga merupakan bukti bahwa penguatan kedaulatan digital Indonesia akan sulit dicapai jika tata kelola serta tingkat keamanan siber yang dimiliki Indonesia masih sangat rendah.

Setelah mengetahui bagaimana kondisi 'geografis' digital Indonesia, maka yang akan dilihat selanjutnya adalah bagaimana implementasi kebijakan-kebijakan yang dimiliki oleh pemerintah Indonesia terkait dengan ancaman siber. Pertama, BSSN atau Badan Siber dan Sandi Negara memiliki Strategi Keamanan Siber Indonesia sebagai acuan bersama seluruh pemangku kepentingan keamanan siber nasional dalam menyusun dan mengembangkan kebijakan keamanan siber di instansi masing-masing (BSSN, n.d.). Strategi Keamanan Siber Indonesia menyangkut ancaman dan tantangan, arsitektur kontemporer siber, manajemen keamanan dan kontijensi, kolaborasi internasional, inovasi dan kreativitas, dan terakhir adalah penegakan hukum (BSSN, n.d.). Kedua, Indonesia memiliki Pedoman Pertahanan Siber milik Kementerian Pertahanan Republik Indonesia yang merupakan kesadaran dalam memperhatikan ruang siber sebagai ruang yang dimanfaatkan untuk mendukung berbagai kegiatan di berbagai sektor yang menimbulkan ancaman-ancaman baru (KEMENHAN, 2017). Dalam Pedoman Pertahanan Siber berisi beberapa hal terkait dengan: urgensi pertahanan siber; pokok-pokok seperti prinsip, sasaran, tugas, peran dan fungsi pertahanan siber; dan terakhir adalah penyelenggaraan pertahanan siber (KEMENHAN, 2017). Adapun disebutkan dalam Pedoman Pertahanan Siber mengenai kebijakan dasar untuk regulasi pertahanan siber yaitu: Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11/2008; Undang-Undang No. 3 Tahun 2002 tentang Pertahanan Negara; Peraturan Pemerintah Penyelenggara Sistem dan Transaksi Elektronik (PP PSTE) No. 82/2012; Peraturan Menhan Nomor 16 Tahun 2010 tentang Organisasi dan Tata Kerja Kemhan.

Selain dari beberapa kebijakan dan peraturan yang telah diciptakan, pemerintah juga sempat mengupayakan pengesahan RUU Rancangan Undang-Undang Keamanan Siber yang sejak tahun 2019 disahkan. RUU ini merupakan upaya merespons ancaman siber yang meningkat terhadap infrastruktur kritis pemerintah, Dewan Perwakilan Rakyat (DPR) dan BSSN untuk menulis RUU yang akan memayungi seluruh UU dan peraturan keamanan siber di Indonesia, (Anjani, 2021). Sejak tahun 2019, pemerintah Indonesia rupanya sudah mengantisipasi ancaman dari terciptanya ruang siber sebagai ruang baru geografi, namun disisi lain juga, pengesahan RUU yang nantinya menjadi undang-undang yang sah harus tertunda bahkan tidak pernah disahkan. Alasannya ada pada berbagai kekurangan yang ada dalam RUU tersebut seperti tidak ada penjabaran terkait dengan wewenang BSSN dengan lembaga pemerintah lainnya, juga pembatasan keterlibatan sektor swasta dan hanya melibatkan pemerintah pusat, pemerintah daerah dan masyarakat yang masih bermakna luas (Anjani 2021). Selanjutnya dalam RUU tersebut tidak membedakan antara infrastruktur digital atau aplikasi yang membutuhkan tingkat keamanan yang berbeda-beda (Anjani, 2021). Lagi-lagi, indonesia masih lambat dalam melakukan tindakan pencegahan akan ancaman siber yang akan terjadi dengan tidak bertindak cepat dan serius hingga masih terjadi berbagai serangan-serangan siber dari tahun ketahun. Jika kondisi Indonesia seperti ini terus menerus, maka tak heran jika nantinya kedaulatan digital Indonesia tidak akan tercapai. Padahal sudah banyak bentuk serangan siber yang telah diterima oleh pemerintah

UPAYA PENGUATAN KEDAULATAN DIGITAL INDONESIA

Kondisi dan implementasi geopolitik digital di Indonesia masih sangat memprihatinkan, hal ini dibuktikan dengan masih banyaknya kasus serangan siber yang mengakibatkan bocornya data-data nasional maupun data pribadi milik warga negara. Padahal kondisi tersebut sudah menunjukkan bahwa Indonesia tengah berada di krisis geopolitik digital yang akan sangat mempengaruhi kedaulatan digitalnya, namun masih tidak ada kemajuan. Bagaimana tidak, menciptakan, menetapkan dan mengimplementasikan kebijakan yang memang selayaknya tanggung jawab negara dalam mempertahankan kedaulatan negara masih tidak disanggupi. Ancaman siber yang menyerang ruang siber di lingkup teritorial negara seperti data maupun wadah interaksi masyarakat masih rawan terkena malware dan juga ransomware. Padahal, sudah terdapat peraturan seperti milik BSSN yaitu Strategi Keamanan Siber Indonesia dan milik Kementerian Pertahanan yaitu Pedoman Pertahanan Siber. Namun faktanya masih banyak pembobolan dan juga kebocoran data yang dialami pemerintah Indonesia sejak

tahun 2017 hingga 2024 yang baru saja terjadi pada bulan Juni sehingga kosistem ruang siber Indonesia yang tidak aman dan dilihat juga dari implementasi dari peraturan maupun kebijakan milik pemerintah yang tidak diterapkan dengan baik. Ketidakstabilan ini akan berdampak pada kedaulatan digital, dimana pemerintah masih belum mampu untuk mandiri dan mampu mempertahankan keamanan dan ketahanan digitalnya. Oleh karena itu, sangat penting bagi negara untuk dapat memberikan perhatiannya di ruang siber dan merekonstruksi ulang tata kelola keamanan siber di Indonesia.

Jika kondisi ketidakamanan siber di Indonesia tidak kunjung terselesaikan, maka efek serta resiko yang akan diterima akan menjadi jauh lebih besar dan jauh lebih rumit. Sebagai contoh kasus kebocoran Pusat Data Nasional pada bulan Juni 2024 yang menyebabkan terhambatnya layanan masyarakat seperti PPDB, pendaftaran paspor, hingga KIP Kuliah menjadi tidak dapat terlaksana dengan baik sehingga tujuan transformasi digital Indonesia jelas sulit untuk dicapai. Bila stakeholder tidak mampu menangani hal tersebut, maka kesulitan-kesulitan kedepannya juga akan sulit untuk ditangani dan tidak dapat dicegah kembali, yang jelas akan merugikan negara dan juga masyarakat. Data pribadi yang didapatkan akibat dari kebocoran data juga dapat dijual oleh pihak tidak berwenang atau pelaku dapat meminta uang tebusan yang akan sangat merugikan negara. Selain itu juga, bila data-data negara yang bersifat rahasia berhasil diketahui oleh negara lain, maka akan sangat berbahaya bagi Indonesia dan mengancam stabilitas keamanan yang ada. Dampak yang akan terjadi bila data-data rahasia suatu negara diketahui oleh negara lain atau negara musuh ada dalam empat jenis dampak, menurut Mark Zaid empat hal itu termasuk informasi itu sendiri, misalnya lokasi pasukan; sumber atau metode pengumpulan data, yang bisa membahayakan individu atau jalur informasi tersebut; kepentingan (negara), yang memungkinkan lawannya untuk mengeksploitasi kelemahan negara; dan pengungkapan terhadap publik, yang bisa membuat malu negara lain, termasuk negara sahabat (Ahdiat, 2023). Selain empat jenis tersebut, kebocoran data rahasia yang diketahui oleh negara lain akan sangat memungkinkan untuk memicu sebuah perang, entah dalam bentuk cyberwarfare maupun dalam bentuk perang militer.

Hubungan diplomatik suatu negara juga akan terputus bila beberapa negara merasa terancam maupun sebaliknya negara lain akan memiliki kesempatan besar untuk menyerang jika data yang dimiliki memuat informasi sisi lemah dari Indonesia. Gambaran sederhana seberapa pentingnya data-data milik negara, sebagai contoh jika negara A memiliki data bocor milik negara Indonesia yang menyatakan bahwa setengah dari populasi penduduk Indonesia belum mendapatkan vaksinasi influenza, sehingga negara A memanfaatkan data tersebut untuk menyerang dengan cara menyebarkan virus, walau terdengar imajinatif, namun akan sangat mengancam dan sangat membahayakan bila benar-benar terjadi. Geografi ruang siber faktanya mampu mempengaruhi sebuah stabilitas keamanan fisik dan mempengaruhi berbagai aspek kehidupan bernegara. Sehingga diperlukan berbagai upaya yang dapat diimplementasikan dan tidak hanya tertuang dalam kertas untuk dapat memperkuat kedaulatan digital Indonesia. Pemerintah pusat harus mempertimbangkan kembali pengesahan RUU keamanan siber dengan melakukan perbaikan dan koreksi terhadap RUU yang sebelumnya serta segera diratifikasi agar dapat terimplementasi di seluruh stakeholder. Kemudian, diperlukan juga keterlibatan pemerintah daerah dan pegawai pemerintahan untuk dapat berhati-hati serta meningkatkan kewaspadaan terhadap berbagai ancaman siber. Peningkatan sumber daya manusia yang mampu, memahami, dan mengerti di bidang siber dan juga keamanan siber juga sangat diperlukan, pemerintah harus bisa mendorong peningkatan sumber daya manusia yang berfokus pada bidang siber agar dapat bekerja dan mengimplementasikan serta mengembangkan keamanan siber milik negara. Perlu adanya standar kualifikasi tiap sumber daya manusia yang memang mampu untuk bekerja dalam peningkatan tingkat keamanan dan pemerintah harus berupaya mendorong hal tersebut. Sehingga, para pekerja, pemegang kepentingan dan penanggung jawab merupakan orang-orang atau warga negara yang benar-benar paham dengan bidang siber. Terakhir adalah dengan melakukan kerjasama dalam bentuk apapun, seperti dalam bidang pendidikan dengan tujuan untuk meningkatkan kemampuan serta kualitas sumber daya manusia. Kerjasama dalam bidang teknologi yang dapat dimanfaatkan untuk meningkatkan keamanan siber di ruang siber juga dapat dilakukan, yang paling terpenting adalah kerjasama antar institusi yang menjadi stakeholder. Serta, yang terpenting adalah dengan meningkatkan keamanan siber di Indonesia akan sangat berpengaruh terhadap beberapa hal sehingga penguatan kedaulatan digital dapat tercapai.

KESIMPULAN

Penegakan kedaulatan digital Indonesia memiliki urgensi tinggi karena mempengaruhi berbagai aspek kehidupan. Kedaulatan digital juga merepresentasikan bagaimana kekuatan, kemampuan dan juga kredibilitas suatu negara dalam mengelola dan memanfaatkan ruang-ruang sibernya. Konsepsi Geopolitik digital yang merupakan pendekatan baru dengan pemanfaatan ruang siber sebagai medan geografisnya menjadi salah satu arena politik penting dilihat dari peranan pemerintah melalui berbagai kebijakannya

terutama dalam mengamankan data-data krusial kenegaraan di ruang digital. Kedaulatan digital akan dapat tercapai melalui pemanfaatan akan pemahaman bahwa ruang-ruang siber menjadi sebuah arena atau medan geopolitik penting dan krusial. Sejalan dengan upaya penguatan kedaulatan digital tersebut terdapat berbagai dinamika ancaman dan tantangan yang dialami oleh Indonesia terutama ancaman *cybersecurity* berupa maraknya serangan malware dan ransomware yang menyebabkan kebocoran data-data strategis nasional oleh pihak tertentu. Ancaman siber di Indonesia yang terus berkembang dan peran pemerintah yang masih lambat dalam mengamankan ancaman-ancaman tersebut membuat kedaulatan siber Indonesia masih lemah dan akan mengakibatkan terjadinya bencana siber jika suatu saat nanti terjadi *cyberwarfare* di Indonesia. Dalam beberapa tahun terakhir pemerintah mencoba merespon fenomena tersebut dengan menciptakan RUU maupun peraturan serta strategi baru dalam bidang siber akan tetapi masih terdapat banyak masalah dalam pengimplementasinya. Melihat hal ini Pemerintah harus mulai melihat bahwa ruang-ruang siber ini adalah sebuah ruang kontestasi geopolitik Baru yang dapat dimanfaatkan baik oleh aktor negara maupun aktor-aktor lain yang berusaha untuk melemahkan Indonesia melalui cara-cara pelemahan digital ditegah ekosistem birokrasi Indonesia yang sedang gencar melakukan digitalisasi di berbagai sektor.

DAFTAR PUSTAKA

[1] Adolf, H. Aspek aspek negara dalam hukum internasional. Keni Media. 2011.

[2] Ahdiat, A. "Dampak kebocoran data terhadap keamanan Amerika Serikat". Internet: https://www.antaranews.com/berita/3497292/dampak-kebocoran-data-terhadap-keamanan-amerika-serikat. April. 19, 2023 [4 Juli 2024].

[3] Alfi, M., Yundari, N. P., & Tsaqif, A. Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 6, Januari 2023. Hlm, 1-11. https://doi.org/10.7454/jkskn.v6i2.10082.

[4] Amsir, A. A. Perjanjian Westphalia Dan Momentum Pendirian Negara Modern. Jurnal Wawasan Keislaman, Vol.15, Juni, 2021, https://doi.org/10.24252/sulesana.v15i1.23600.

[5] Anggoro, K. Perubahan Geopolitik dan Ketahanan Nasional: Sebuah Penjelajahan Teoretikal. Jurnal Lemhanas RI, Vol. 5, No.1, Maret, 2017, https://jurnal.lemhannas.go.id/index.php/jkl/article/view/130.

[6] Anjani, N. H. (2021, Maret). Perlindungan Keamanan Siber di Indonesia. Center for Indonesia Policy Studies, 2021.

[7] Annisa. Teori Kedaulatan, Pengertian dan Jenisnya. internet: https://fahum.umsu.ac.id/teori-kedaulatan-pengertian-dan-jenisnya/. Juni. 26, 2023 [4 Juli 2024].

[8] Aprillio, Akbar. Pusat Data Nasional Sementara lumpuh akibat ransomware, mengapa instansi pemerintah masih rentan terhadap serangan siber?. Internet: https://www.bbc.com/indonesia/articles/cxee2985jrvo. June. 27, 2024. [4 Juli 2024].

[9] Hinsa, Siburian. Strategi Keamanan Siber Nasional. Internet: https://www.bssn.go.id/strategi-keamanan siber-nasional/. [4 Juli 2024].

[10] Peraturan Kementerian Pertahanan Republik Indonesia No. 82 tahun 2014 Tentang Pedoman Pertahanan Siber.

[11] Condrobimo, A. R. Memahami Transformasi Digital. Internet: https://sis.binus.ac.id/2023/12/13/memahami-transformasi-digital/. Dec, 13. 2023 [4Juli 2024]

[12] CSIRT Kemhan RI. Apa itu Malware . internet: https://csirt.kemhan.go.id/portal/berita/35. Feb, 04, 2021 [4 Juli 2024]

[13] Dewi, I. R. Bikin Heboh RI, Data Apa Saya yang Dibocorkan Hacker Bjorka?. Internet: https://cnbcindonesia.net/tech/20220914095826-37-371939/bikin-heboh-ri-data-apa-saja-yang-dibocorkanhacker-bjorka. .Sept. 14, 2022 [4 JULI 2024].

[14] Flint, C. (2022). Introduction to Geopolitics. (4th Edition). [on-line]. Available: https://www.routledge.com/Introduction-to-Geopolitics/Flint/p/book/978036 7686758. [4 Juli 2024]

[15] Gueham, F. Digital sovereignty - steps towards a new system of internet governance. Internet: https://www.fondapol.org/en/study/digital-sovereignty-steps-towards-a-new-system-of-internet-governance/. Feb, 2017 [4 juli 2024].

[16] Hukum Online. Mengurai Implementasi Kedaulatan Digital di Indonesia. Internet: https://www.hukumonline.com/berita/a/mengurai-implementasi-kedaulatan-d igital-di-indonesia-lt64a52bbd00af2/. Jul. 5, 2023 [4 Juli 2024]

[17] Hutabarat, J. S., Krismonika, G., & Lofa. "Medan Geopolitik Baru 5.0 Pasca Covid-19". Jurnal Lembaga Ketahanan Nasional Republik Indonesia, Vol. 8, hlm. 183-192, 17 Oktober 2022. https://doi.org/10.55960/jlri.v8i2.321.

[18] KOMINFO. Perjuangan Mewujudkan Kedaulatan Digital. Internet: https://www.kominfo.go.id/content/detail/14309/perjuangan-mewujudkan-kedaulatan-digital/0/sorotan_media. Jun. 09, 2018 [4 Juli 2024].

[19] Maharani, A. D., Luthfitasari, A. R., Rachman, B. A., Rahman, A., & Ediyono, S. "Keamanan Sibernetika dan Tantangan Geopolitik di Era Digital". Jurnal Pemikiran, Penelitian Hukum, Pendidikan Pancasila dan Kewarganegaraan, Vo. 11,No. 1, hlm. 12-16. Maret, 2024.

[20] Ramadhan, I. (2021). The Implication of Cyberspace Towards State Geopolitics. POLITICON : Jurnal Ilmu Politik, 3, 161-184. p-ISSN 2355-6439. e-ISSN 2962-