TANTANGAN DAN UPAYA PEMERINTAH INDONESIA DALAM MELINDUNGI MASYARAKAT

STUDI KASUS: KEJAHATAN SIBER

Imam Budiman

Program Studi Ilmu Hubungan Internasional, Universitas Pasundan

Email: Imam.Budiman@unpas.ac.id

Reza Ardiansyah Pradana

Email: reza22004@mail.unpad.ac.id

Mahasiswa Magister Hubungan Internasional Universitas Padjadjaran

Abstrak

Kemajuan teknologi di era-Globalisasi sekarang tidak dapat dihindarkan. Semua negara di Dunia berlomba lomba dalam mengembangkan teknologi guna mempemudah kehidupan manusia. Kemajuan teknologi ini pun tidak terlepas dari ancaman yang mengintai di setiap aktifitas nya. Tentu peran negara sebagai aktor yang harus melindungi warga negaranya dari setiap ancaman termasuk ancaman teknologi. Hal tersebut membuat keamanan siber diperlukan oleh seluruh negara, termasuk Indonesia. Dengan berbagai tantangan yang dihadapi, serta beberapa kebijakan yang diimplementasi, Indonesia masih menjadi negara yang rentan untuk diserang diruang siber. Dengan menggunakan metode penelitian kualitatif di mana berfokus dengan mendeskripsikan fenomena melalui literatur-literatur yang dibaca, penelitian ini menyimpulkan bahwa upaya yang dilakukan oleh pemerintah masih belum efektif dan optimal dalam menjaga keamanan siber Indonesia.

**Kata Kunci: Keamanan Siber; Ruang Siber; Teknologi.**

*Abstract*

*Technological advances in the current era of globalization are unavoidable. All countries in the world are competing in developing technology to facilitate human life. Technological advances are inseparable from the threats that lurk in every activity. Of course, the role of the state as an actor must protect its citizens from every threat, including technological threats. This makes cyber security needed by all countries, including Indonesia. With various challenges faced and several policies implemented, Indonesia is still a country that is vulnerable to cyber-attacks. By using qualitative research methods which focus on describing phenomena through the literature read, this study concludes that the efforts made by the government are still not effective and optimal in maintaining Indonesian cybersecurity.*

***Keywords: Cybersecurity; Cyberspace; Technology***

**Pendahuluan**

Seiring berjalannya waktu, teknologi informasi menjadi salah satu alat yang paling signifikan digunakan dalam membantu manusia menjalani kehidupannya sehari-hari. Menurut William (2005, dalam Kidi, 2018), teknologi informasi adalah suatu bentuk universal yang menggambarkan tiap teknologi yang membantu mencipta, memanipulasi, menyimpan, menghubungkan, dan/atau menyampaikan informasi. Alat yang terlahir berkat arus globalisasi tersebut memiliki banyak sekali manfaat, baik dalam bidang kesehatan, pendidikan, perekonomian, dan lainnya bagi suatu negara.

Pada era revolusi 4.0 di mana hampir seluruh aspek kehidupan manusia tak dapat lepas dari teknologi sehingga membuat aktivitas dan proses berbagai sektor mengalami transformasi digital. Dalam upaya digitalisasi ini, terlahir inovasi *Artifical Intelligence* (AI) dan *Internet of Things* (IoT) yang memudahkan setiap perangkat terkoneksi dengan jaringan komputer, seperti internet. Melansir *data International Telecommunication Union* (ITU) yang dikutip oleh World Bank, terdapat sebanyak 49% dari populasi dunia yang menggunakan internet di tahun 2017— terhitung melesat sejak tahun 2000 yang hanya sekitar 6,7%. Tak hanya itu, *Internet World Stats* juga memperkirakan bahwa pada tahun 2021, jumlah tersebut akan menyentuh hingga kisaran 64,2%. Ramainya pengguna internet tersebut secara tidak langsung menjadi bumerang, sebab juga sekaligus meningkatkan ancaman dalam siber. Keamanan siber menjadi salah satu solusi yang ditawarkan.*International Organization for Standardization* (ISO) mendefinisikan keamanan siber sebagai langkah yang diupayakan untuk menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), serta ketersediaan (*availability*) dari informasi di ruang siber. Sementara itu, menurut CISCO, keamanan siber ialah upaya perlindungan jaringan, sistem, serta suatu program dari ancaman digital. Ancaman-ancaman yang dimaksud biasanya variatif, seperti pengaksesan, perubahan, atau penghancuran informasi sensitif, pemerasan harta pengguna, hingga penghambat operasional suatu bisnis. Maka dari itu, Permatasari (2021) menyimpulkan bahwa keamanan siber merupakan langkah preventif untuk melindungi sistem dari aksesibilitas illegal.

Indonesia merupakan salah satu negara dengan pengakses internet terbanyak. Dikutip dari DataIndonesia.id, terdapat sebanyak 205 juta pengguna internet di Indonesia. Berdasarkan data tersebut, berarti ada sebanyak 73,7% dari total populasi masyarakat Indonesia. Dengan jumlah yang signifikan besar tersebut, Indonesia juga rentan menjadi target ancaman siber. Bahkan pada 2019, CNN sudah memperhatikan kerentanan keamanan siber di Indonesia. Menurut David Chinn, *Senior Partner and Global Leader Cybersecurity Practice*, setidaknya terdapat 4 (empat) alasan mengapa Indonesia menjadi negara yang rentan perihal siber, yakni 1) terbatasnya perencanaan mengenai tanggapan jika terjadi insiden yang berkaitan dengan keamanan siber; 2) perlunya peningkatan kebijakan keamanan siber; 3) risiko siber yang dipandang sebagai permasalahan teknologi, bukan bisnis; serta 4) rendahnya kesadaran masyarakat atas isu siber sehingga seringkali tak waspada dalam mengirim atau membuka tautan yang berbahaya.

**LANDASAN TEORI**

**Sekuritisasi**

Sekuritisasi dipahami sebagai proses masalah politik yang sebelumnya bukan masalah militer menjadi selesai menjadi masalah keamanan dengan melihat masalahnya dari sudut pandang kemanan (*security*), sehingga hal ini dijadikan agenda nasional suatu negara atau bahkan agenda global. Studi keamanan tidak hanya mengenai negara dan militer, tetapi juga beberapa bidang lainnya, yaitu ekonomi, politik, sosial, dan lingkungan (Buzan et.al, 1998). Keamanan siber termasuk ke dalam sosial, tapi juga dapat mencakup ranah politik. Sekuritisasi di sini digunakan untuk mengetahui transisi fokus di mana pada mulanya siber tidak mendapatkan perhatian dalam keamanan, tapi pascadigitalisasi mulai menjadi salah satu aspek yang dapat mengancam suatu negara.

Keamanan Non tradisional setelah konsep Keamanan Tradisional mulai berkembang, Barry Buzan pun semakin memperluas definisinya dengan pernyataan yang berbunyi jika kemanan tidak hanya mencakup bidang militer dengan aktor negara semata, tetapi juga mengikutsertakan elemen-elemen non- militer, serta non-negara. Secara singkat, Buzan (1998) menyimpulkan bahwa Keamanan Nontradisional berfokus kepada permasalahan ancamanan non-militer dan peran-peran yang dimainkan aktor-aktor non-negara. Pernyataan Buzan sebelumnya kemudian melahirkan sebuah sikap dari PBB pada tahun 1990-an mengenai arti konsep keamanan. Dalam sikapnya tersebut, PBB mengubah definisi tersebut menjadi “Konsep keamanan harus beralih dari penekanan yang ekslusif terhadap keamanan nasional” dan kemudian meresmikan identitas Keamanan Nontradisional sebagai salah satu konsep yang dipakai oleh para pemikir Hubungan Internasional.

**Keamanan Siber (Cybersecurity)**

Ruang siber merupakan media elektronik dan jaringan komputer di mana komunikasi terjadi secara daring. Dewi Triwahyuni mengatakan bahwa konsep keamanan siber tak lagi hanya menyentuh ranah teknologi, tapi sudah menjadi suatu ancaman terhadap keamanan nasional. Keamanan siber ditujukan pada isu keamanan informasi bagi pemerintahan, organisasi dan urusan individual yang dihubungkan dengan teknologi ICT, dan secara khusus dengan teknologi internet.

***Internet Censorship***

Keberadaan sistem komunikasi via internet membawa perubahan yang sangat besar terhadap studi Hubungan Internasional. Fenomena yang nampak dari kemunculan internet ini adalah kemunculan komunitas- komunitas maya yang menghubungkan individu dan masyarakat dari suatu negara secara paralel dengan individu dan masyarakat dari negara lain. Teknologi internet ini juga telah mentransformasi pandangan ilmuwan politik tentang negara. Konsep negara modern yang mengisyaratkan bahwa negara adalah komunitas yang memiliki penduduk yang tetap, wilayah yang tetap, pemerintahan yang tetap, serta otonomi kekuasaan politik dan hubungan internasional pada institusi pemerintahan kini tidak lagi mampu menjawab tantangan perubahan zaman yang memunculkan „masyarakat maya‟ atau jaringan individu berbagai bangsa dan etnis. Masyarakat maya ini menggunakan ruang-ruang siber untuk saling bertukar informasi, menjalin hubungan kekerabatan, melakukan transaksi ekonomi dan bisnis, hingga operasi tindak-tindak kejahatan baru dengan skala global yang sulit dikontrol oleh negara.

***Information, Communication, and Technologies (ICT)***

ICT adalah Information and Communication Technologies dan mengacu pada teknologi yang menyediakan akses terhadap komunikasi, di mana dengan menggunakan ICT ini orang dapat berkomunikasi secara realtime dengan orang di negara lain dengan menggunakan instant messaging, Volp (voice over internet protocol) dan video conference. Fenomena kebangkitan ICT menciptakan era baru yang disebut era informasi. Dalam kajian Hubungan Internasional dengan penguasaan ICT jalan suatu negara untuk menyebarkan power dan influence ke negara lain menjadi semakin mudah. Sayangnya, terjadi disparitas kepemilikan kapabilitas di sektor ICT antara satu negara dengan negara yang lain atau antara kelompok negara maju dengan negara berkembang dan tertinggal (Putri, 2015).

**METODE PENELITIAN**

Dalam meneliti permasalahan ini, peneliti menggunakan metode penelitian Kualitatif. Berdasarkan Brady (2015), metode penelitian Kualitatif adalah sebuah metode yang menyediakan peralatan untuk memahami substansi definisi yang berkaitan dengan fenomena yang kompleks prosesnya di dalam praktik kehidupan sosial. Selain itu, pada tahun 2013, Hilal dan Alabri berpendapat jika metode ini merupakan sebuah upaya menjelaskan suatu kejadian dengan didasari oleh perspektif narasumber, berdasarkan realita yang variatif, serta pengembangan pemahaman secara holistik dalam konteks tertentu mengenai kejadian tersebut. Terakhir, Bertens (1987, dalam Eddles-Hirsch, 2015), memiliki argument bahwa metode penelitian Kualitatif menganalisis dan mendeskripsikan suatu fenomena milik individu dalam kehidupannya sehari-hari.

Teknik pengumpulan data yang peneliti gunakan ialah dengan menggunakan studi literatur berdasarkan beberapa sumber, seperti referensi dokumen, artikel, jurnal, buku, baik secara cetak maupun daring, yang berhubungan dengan judul yang sedang diteliti, yakni “Ruang Siber: Tantangan dan Upaya Pemerintah dalam Melindungi Keamanan Siber di Indonesia”.

**HASIL PEMBAHASAN**

**Tantangan Keamanan Siber**

Dalam penerapan keamanan siber yang efektif, banyak sekali tantangan mengingat perangkat pendukung yang juga kini mulai bervariasi. Meskipun infrastruktur pendukung keamanan siber diperkokoh, bukan berarti menghapus potensi ancaman-ancaman yang bersifat eksponen. Urgensi dari keamanan siber ini memerlukan tindakan serius dalam membangun rancangan bank informasi dan data yang andal, memenuhi kompetensi, juga pembuatan standardisasi operasional dalam mengelola informasi dan data. Keamanan siber tidak hanya menyerang secara langsung, melainkan juga pada ruang-ruang siber yang begitu luas. Berdasarkan operasi pelaksanaannya, berikut beberapa jenis ancaman siber:

1. Siber Kriminal (Cybercrime)

Dalam ancaman ini, pelaku biasanya terdiri dari mereka yang memiliki keahlian dalam peretasan. Informasi dan data yang diretas biasanya mereka curi untuk melakukan penipuan atau pembobolan rekening. spionase, dan semacamnya.

1. Perang Maya (Cyber Warfare)

Ancaman ini merupakan bentuk peperangan yang terjadi di ruang siber atau ruang maya. Media utama yang diserang oleh ancaman ini merupakan objek siber yang dimiliki atau dikuasai suatu negara.

1. Siber Terorisme (Cyber Terorism)

Ancaman ini biasanya dilakukan oleh para teroris yang memanfaatkan ruang maya untuk menyebarkan terornya melalui ruang siber. Beberapa contoh dari siber terorisme ialah penyerangan website resmi pemerintah, sadar komunikasi politik, pencurian data elektronik, dan sebagainya. Pun, dalam melakukan penyerangan siber, terdapat beberapa metode yang dilakukan oleh para pelaku, yakni:

a. Malware

1)Virus 2) Trojans 3) Spyware 4) Ransomware 5) Adware 6) Botnet

b. Social Engineering

c. Injeksi SQL

d. Email Spam & Pishing

e. Domain Name

1) Cybersquatting

2) Typosquatting

f. Denial of Service (DoS)

Tentu saja, ruang siber memiliki banyak sekali manfaat dalam mempermudah hampir seluruh kegiatan umat manusia. Namun, berkaca pada potensi-potensi tantangan yang ada, ruang siber juga menjadi salah satu fokus negara untuk mempertahankan keamanan nasionalnya, termasuk Indonesia.

**Keamanan Siber di Indonesia**

Dalam jurnalnya, Ardiyanti (2016) menyatakan bahwa Indonesia saat ini tengah dalam keadaan mendesak cybersecurity atau keamanan siber karena melihat kenyataan bahwa tingkat kejahatan siber atau cybercrime di Indonesia sudah mencapai tahap memprihatinkan. Data yang dihimpun oleh CIA menyebutkan bahwa kerugian yang disebabkan karena tindak kejahatan siber di Indonesia telah mencapai 1,20% dari tingkat kerugian akibat cybercrime yang terjadi di dunia.

Indonesia mulai menyikapi keamanan siber melalui pembentukan Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) pada tahun 2007. Tim tersebut ditugaskan oleh Kementerian Komunikasi dan Informatika (Kemkominfo) untuk melakukan pengawasan keamanan jaringan Berbasis protokol internet. Beberapa tugas dari ID-SIRTII di antaranya ialah melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan gangguan pada jaringan, berkoordinasi dengan pihak-pihak terkait, baik di dalam maupun luar negeri, dalam menjalankan tugas pengamanan jaringan telekomunikasi berbasis protokol internet, mengoperasikan, memelihara dan mengembangkan sistem *database* sistem IDSIRTII dengan upaya penyusunan katalog dan silabus yang berkaitan dengan proses pengamanan pemanfaatan jaringan, memberikan layanan informasi atas ancaman dan gangguan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet, menjadi contact point dengan lembaga terkait tentang keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet serta menyusun program kerja dalam rangka melaksanakan pekerjaan yang berkaitan dengan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet.

Pada tahun 2018, *National Cyber Security Index* mengeluarkan sebuah data yang menyatakan bahwa Indonesia menempati peringkat 83 dari 100 negara terkait negara yang paling rentan diretas dengan angka 19,48 poin. Angka tersebut cukup tinggi apabila dibandingkan dengan indeks pengembangan digital Indonesia yang menyentuh angka 50,22 poin (Krisnaduta, 2019).

Kebijakan dan Tantangan Keamanan Siber di Indonesia

a. Legalitas

Pembentukan ID-SIRTII pada tahun 2007 menjadi pintu awal Indonesia dalam membentuk kebijakan mengenai keamanan siber di Indonesia. Landasan hukum keamanan siber saat ini dibangun berdasarkan dasar UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012, serta surat edaran menteri dan peraturan menteri. Akan tetapi, legalitas pencegahan kejahatan di dunia siber masih lemah. Sebab, meskipun memiliki peraturan perundang- undangan yang melarang bentuk penyerangan ataupun perusakan sistem elektronik dalam UU Informasi dan Transaksi Elektronik No.11 Tahun 2008, masih belum ada perundang- undangan yang mengatur secara khusus terkait serangan siber dan penanganannya sehingga sulit untuk diproses oleh aparat hukum.

Dalam hal legalitas, mengembangkan keamanan siber adalah tentang memiliki dokumen kebijakan keamanan yang bersifat dokumen sebagai suatu standar yang digunakan sebagai acuan dalam pelaksanaan semua proses yang berkaitan dengan keamanan informasi. Pengembangan dan penguatan kebijakan keamanan siber Indonesia harus diintegrasikan dengan strategi nasional untuk membangun ekosistem keamanan siber nasional yang disiapkan oleh pemerintah.

b. Teknikal & Prosedural

Secara umum, Gautama menjelaskan beberapa masalah terkait upaya pembangunan keamanan siber, yakni:

1.Lemahnya pemahaman negara terkait dengan dunia siber yang memerlukan pembatasan pengunaan layanan yang servernya berada di luar negeri dan diperlukan adanya pengunaan secured system.

2. Legalitas penanganan penyerangan di dunia siber.

3. Pola kejadian *cyber-crime* sangat cepat sehingga sulit ditangani.

4.Tata kelola kelembagaan cyber- security nasional.

5. Rendahnya awareness atau kesadaran akan adanya ancaman *cyber-attack* internasional yang dapat melumpuhkan infrastruktur vital suatu negara.

6. Masih lemahnya industri Indonesia dalam memproduksi dan mengembangkan perangkat keras atau hardware terkait dengan teknologi informasi yang merupakan celah yang dapat memperkuat ataupun memperlemah pertahanan dalam dunia siber. Penanganan kejahatan siber masih bersifat parsial dan tersebar, serta ketiadaan koordinasi yang baku dalam masalah keamanan siber. Terkait kebijakan keamanan siber di Indonesia, perlu dibuat kebijakan yang mengatur berbagai elemen terkait keamanan siber dengan cara yang berbeda.

Elemen utama keamanan siber yang harus dipenuhi selama ketersediaan infrastruktur informasi adalah media yang berperan dalam kelangsungan operasi informasi, termasuk perangkat keras dan perangkat lunak. Selanjutnya, dalam keamanan siber, dari segi teknis, adalah peningkatan perangkat yang terhubung dengan komputer, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan totalitas informasi yang dikirimkan dan/atau disimpan di dunia siber.

c. Struktur Organisasi

Tantangan lainnya adalah bahwa penanganan keamanan siber dalam pertahanan negara masih bersifat sektoral dan tidak terkoordinasi dan tidak terintegrasi. Salah satu alternatif kebijakan untuk memerangi kejahatan siber yang telah mencapai tingkat mengkhawatirkan adalah dengan menempatkan keamanan siber dalam konteks pertahanan. Suatu organisasi yang terkait dengan keamanan siber harus menyesuaikan dengan organisasi penggunaan sistem teknologi informasi dengan berfokus pada empat hal utama, yaitu: 1) sistem informasi; 2) persaingan organisasi; 3) sistem informasi dan pengambilan keputusan organisasi (information systems and decision making in organization); serta 4) pengorganisasian penggunaan sistem informasi (organizational use of information systems). Berbagai konsep dan langkah yang terkait dengan peningkatan organisasi dan pengelolaan lembaga yang bergerak di bidang keamanan yang diterapkan untuk mencapai dan menjaga sifat keamanan organisasi dan pengguna terhadap persyaratan yang relevan, baik di tingkat institusi maupun di tingkat nasional, dalam mengurangi risiko keamanan siber.

d. Peningkatan Kapasitas

Program pelatihan dan pengembangan keterampilan keamanan siber dilaksanakan berkoordinasi dengan gugus tugas Pusat Operasi Keamanan Siber (Cyber Defence Operation Centre). Selain itu, perlu adanya pengembangan sumber daya manusia tentang pentingnya keamanan siber untuk meningkatkan kesadaran akan tindakan preventif pencegahan segala kejahatan siber. Mengingat pesatnya perkembangan teknologi, pengelolaan sumber daya keamanan siber harus diposisikan sebagai sebuah proses manajemen bisnis. Hal ini diperlukan karena berurusan dengan keamanan siber bukanlah bisnis yang murah dan berkembang pesat. Pengembangan kapasitas infrastruktur dapat mengurangi potensi biaya atau pengeluaran yang terkait dengan pengembangan teknologi dengan memposisikannya sebagai proses manajemen bisnis. Dengan mengelola Sumber Daya Manusia (SDM) yang mahir keamanan siber dengan manajemen bisnis, diharapkan dapat mempercepat kebutuhan SDM yang paham keamanan siber.

e. Kerja Sama Internasional

Kerja sama Indonesia dalam memerangi kejahatan siber antara lain menjadi anggota *ASEAN Network Security Action Council*, menjadi anggota *International Telecommunication Union* (ITU), dan menjadi *steering committee Asia-Pacific Computer Emergency Response Team* (APCERT). anggota *Forum of Incident Response and Security* (FIRST), serta melakukan kerja sama bilateral di bidang keamanan siber dengan Jepang, Inggris dan sejumlah negara lainnya. Persoalannya hingga saat ini belum ada kesepakatan internasional yang mengikat tentang keamanan siber, sehingga Indonesia perlu berinisiatif sebagai negara untuk mengupayakan kesepakatan bersama yang mengikat tentang keamanan siber di tingkat internasional.

Peningkatan kerja sama di bidang teknologi informasi dan keamanan siber diharapkan dapat membuka peluang bagi berkembangnya industri media baru terkait TI di Indonesia sebagai bagian dari pengembangan sektor strategis. Terkait pengembangan kerjasama internasional dalam rangka pembangunan keamanan siber, Indonesia perlu meningkatkan peran aktifnya dalam mendorong berbagai kesepakatan bersama yang dirundingkan di ILO, yang merupakan organisasi terdepan dalam menciptakan ruang siber yang aman bagi negara, pemerintah. masyarakat dan dunia usaha. Akan tetapi, sangat disayangkan, dengan upaya-upaya yang sudah dilakukan, masih terdapat beberapa celah sehingga tak jarang Indonesia menjadi salah satu negara yang diserang oleh para peretas untuk mencuri data-data, baik data masyarakat maupun data negara. Secara tidak langsung, hal tersebut diharapkan dapat menyadarkan pemerintah bahwasanya keamanan siber juga merupakan salah satu hal yang harus diperhatikan demi menjaga keamanan nasional bangsa Indonesia.

Sebagai negara berkembang, Indonesia dapat dikatakan cukup tertinggal dalam permasalahan teknologi informasi (Nur, 1998). Konsekuensi ini dirasakan oleh Indonesia akibat beberapa hal yang sistematis yaitu kurangnya kepekaan Indonesia terhadap riset dan diskursus seputar teknologi. Kurangnya modernitas teknologi di Indonesia mengakibatkan kurangnya pula pengetahuan soal keamanan siber itu sendiri. Di antara negara G20 sendiri, Indonesia menempati posisi yang buruk dalam persoalan keamanan siber, yaitu berada di tingkat 3 dari bawah dengan nilai 38,96 (Annur, 2022).

Permasalahan yang dihadapi Indonesia dalam menghadapi isu keamanan siber perlu ditinjau dari status hubungan internasionalnya sebagai negara berkembang. Dalam hal ini beberapa permasalahan yang krusial yang mengakibatkan kurangnya penanganan keamanan siber di Indonesia antara lain: (1) keadaan ekonomi yang belum memungkinkan untuk melakukan peningkatan kualitas siber, (2) keadaan politik yang masih tarik menarik antara otoritarianisme, demokrasi, dan isu-isu populis, dan (3) kurangnya efektifitas pemerintah dalam menanggapi isu-isu siber sehingga terjadinya perubahan yang lambat (Paterson, 2019).

Secara peranan dan fungsionalisasi, diskursus terkait dengan keamanan siber Indonesia memang terkesan harus diarahkan pada basis kebijakan pemerintah dan upayanya, karena secara garis besar peranan masyarakat Indonesia sendiri kurang dalam literasi soal keamanan siber di Indonesia (Rai, Heryadi, & Kamaluddin, 2022). Oleh karenanya, pemerintah diharapkan untuk tidak abai pada hak-hak dasar masyarakat untuk mengakses internet dan informasi harus tetap dijunjung tinggi sembari memastikan keamanan untuk warganya dapat mengakses secara bebas sekaligus bertanggung jawab.

Indonesia membutuhkan kebijakan yang dapat mengatur atau melindungi semua elemen yang berkaitan dengan keamanan siber (Rizal & Yani, 2016). Sebelum mengambil kebijakan, pemerintah harus mengambil langkah yang serius untuk dapat memahami secara komprehensif terkait apa yang dimaksud dengan keamanan siber dan apa ancamannya. Permasalahan yang terjadi di Indonesia sebenarnya berkaitan antara cara kerja pemerintah sekaligus sektor swasta. Indonesia sebagai negara yang berdaulat diharapkan dapat menyadari kapasitasnya dan fungsinya yaitu melindungi segenap warga dari ancaman, termasuk ancaman siber. Kerja sama pemerintah dan swasta adalah salah satu upaya tersebut.

Di era globalisasi ini, Indonesia diharapkan mampu untuk mempertemukan diri dengan standar keamanan siber internasional. Oleh karenanya Indonesia perlu untuk mengembangkan diri secara domestik maupun memperkuat kerja sama internasional maupun kawasan. Alasan di balik mengapa Indonesia harus memperkuat aspek domestik dan internasional terletak pada kesimpulan Herryanto yang mengatakan bahwa kebijakan tentang keamanan siber yang dilakukan oleh Kementerian Pertahanan RI melalui kebijakan MoD masih bersifat sektoral, tidak komprehensif sebagai satu-kesatuan sistem (Herryanto, 2012).

**KESIMPULAN**

Berdasarkan apa yang sudah dijelaskan, maka dapat disimpulkan bahwa globalisasi melahirkan ruang siber dengan berbagai dampak positif dan negatif. Ancaman- ancaman negatif yang berpotensi hadir bervariatif, sehingga diperlukan beberapa strategi atau upaya untuk menanggulanginya. Indonesia, sebagai salah satu negara dengan pengguna teknologi dan pengakses internet terbanyak di dunia, tentunya juga memiliki banyak kerentanan dalam melindungi ruang siber. Hal tersebut menjadi urgensi utama atas eksistensi keamanan siber di Indonesia.

Selain itu, pemerintah Indonesia sendiri memiliki setidaknya 5 (lima) upaya sebagai upaya peningkatan keamanan sibernya, seperti legalitas, teknikal dan prosedural, struktur organisasi, peningkatan kapasitas, hingga kerja sama internasional Namun, dengan upaya-upaya tersebut, masih terdapat beberapa celah yang diharapkan dapat dibenahi oleh pemerintah dalam menjaga keamanan siber bangsa Indonesia sehingga dapat meminimalisir kebocoran informasi atau data, baik milik masyarakat maupun milik negara. Sebab, informasi ataupun data tersebut merupakan hak milik bangsa Indonesia dan berpotensi untuk memberikan ancaman yang lebih besar dan mengancam kepentingan nasional bangsa

**DAFTAR PUSTAKA**

Annur, C. M. (2022). “Indonesia Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20” dalam tautan: <https://databoks.katadata.co.id/datapublish/2022/09/13/indeks-keamanan-siber-indonesia-peringkat-ke-3-terendah-di-antara-negara-g20>

Brady, S.R. (2015). Utilizing and Adapting the Delphi Method for Use in Qualitative Research dalam International Journal of Qualitative Methods, Vol.14, No.5.

Buzan, B., & Waever, Ole, & Wilde, Jaap de (1998). Security: A New Framework for Analysis. Lynee Rienner Publisher: Colorado, Amerika.

Edless-Hirsch, K. (2015). Phenomology and Educational Research dalam International Journal of Advanced Research, Vol.3, No.8.

Haikal, Muhammad (2018). Kebijakan Censorship Tiongkok Terhadap Perusahaan Multinasional Dalam Bidang Ict (Information Communication Technologies) (Studi Kasus Google Inc.). Skripsi daring Universitas Komputer Indonesia.

Herryanto, E. (2012, November 27). Keynote Speech. *Seminar Nasional Keamanan Infrastruktur Internet tentang Trend Ancaman Infrastruktur Internet 2012*. Bandung, Jawa Barat, Indonesia.

Hilal, A.H.; & Alabri, S.S. (2013). Using Nvivo for Data Analysis in Qualitative Research dalam International Interdisciplinary Journal of Education, Vol.2, No.2, Hlm.181-186.

Karnadi, Alif (2022). Pengguna Internet di Indonesia Capai 205 Juta pada 2022. Artikel daring Data Indonesia.id yang diakses melalui tautan: [https://dataindonesia.id/digital/detai l/pengguna-internet-di-indonesia- capai-205-juta-pada-2022](https://dataindonesia.id/digital/detai%20l/pengguna-internet-di-indonesia-%20capai-205-juta-pada-2022).

Kidi (2018). Teknologi dan Aktivitas dalam Kehidupan Manusia. Artikel daring yang diakses pada 29 September 2022 melalui tautan: https://bpsdmd.ntbprov.go.id/wp- content/uploads/2018/05/Teknologi-dan-aktivitas-dalam-kehidupan manusia.pdf

Krisnaduta, Hegar (2019). Kerjasama Indonesia-Australia di Bidang Keamanan dalam Mengatasi Cyber Crime di Indonesia melalui Program Cyber Policy Dialogue. Skripsi daring yang diakses melalui tautan: <http://repository.unpas.ac.id/46253/>

Nur, M. (1998). “Dilema Pengembangan Infrastruktur Informasi Indonesia”, *Info Komputer*, 12(8), hal. 34.

Permatasari, Dwiyani (2021). Tantangan Cyber Security di Era Revolusi Industri 4.0. artikel daring Kementerian Keuangan Republik Indonesia yang diakses melalui tautan: https://www.djkn.kemenkeu.go.id/kanwil-sulseltrabar/baca-artikel/14190/Tantangan-Cyber- Security-di-Era-Revolusi-Industri- 40.html

Paterson, T. (2019). “Indonesian cyberspace expansion: a double-edged sword”, *Journal of Cyber Policy*, 4(2), hal. 216-234

Putri, Sylvia Octa (2015). Kebijakan E- waste Management Pada Perguruam Tinggi berbasos ICT: Suatu Tinjauan Perspektif Green Thought Dan Hukum Lingkungan (Studi Kasus Universitas Komputer Indonesia (2007-2011).

Rai, I. N. A. S., Heryadi, D., & Kamaluddin, A. (2022). “Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber”, *Politica*, 13(1), hal. 43-65.

Rizal, M., & Yani, Y. M. (2016). “Cybersecurity policy and its implementation in Indonesia”, *Journal of ASEAN Studies*, 4(1), hal. 61-78.