KEAMANAN SIBER INDONESIA ERA PEMERINTAHAN JOKO WIDODO BERDASARKAN PERSPEKTIF SEKURITISASI

Raden Agung Prio
Wicaksono Satriya
Wibawa

Program Studi Hubungan Internasional Universitas Padjadjaran

Abstrak

Keberadaan pengguna internet yang masif di Indonesia menjadi sebuah tantangan yang serius bagi Pemerintah untuk menjaga keamanan dalam ruang siber Indonesia. Badan Sandi dan Siber Negara menunjukkan dalam 3 tahun terakhir telah terjadi lebih dari 1 miliar serangan siber terhadap Indonesia. Diantara masifnya serangan tersebut, kemunculan serangan siber oleh Bjorka di tahun 2022 dan serangan pada Pusat Data Nasional Sementara di tahun 2024 menunjukkan celah keamanan bagi Pemerintah Indonesia. Artikel ini Konsep Keamanan Siber dan Teori Sekuritisasi Buzan yang dikembangkan oleh Hansen dan Nissenbaum digunakan untuk memahami upaya pemerintah Indonesia di bawah kepemimpinan Joko Widodo dalam memosisikan dan merespons ancaman siber melalui perspektif siber. Melalui pendekatan penelitian kualitatif deskriptif, tulisan ini mencoba untuk menggambarkan dinamika keamanan siber Indonesia, penerapan proses sekuritisasi pada ruang siber, dan implikasi strategi keamanan siber pada ruang siber Indonesia. Temuan pada tulisan menunjukkan Indonesia telah memosisikan isu ancaman siber sebagai permasalahan keamanan yang cukup serius, namun belum sepenuhnya telah berhasil melakukan sekuritisasi secara penuh melainkan berada pada tahap Politisasi menuju Sekuritisasi.

Kata kunci: Ancaman Siber; Keamanan Siber; Indonesia; Sekuritisasi

Abstract

The massive presence of internet users in Indonesia is a serious challenge for the Government to maintain security in Indonesia's cyberspace. The National Cyber and Crypto Agency shows that in the last 3 years there have been more than 1 billion cyber attacks against Indonesia. Among the massive attacks, the emergence of cyber attacks by Bjorka in 2022 and attacks on the Temporary National Data Center in 2024 show security gaps for the Indonesian Government. This article The Concept of Cyber Security and Buzan's Securitization Theory developed by Hansen and Nissenbaum are used to understand the efforts of the Indonesian government under the leadership of Joko Widodo in positioning and responding to cyber threats through a cyber perspective. Through a descriptive qualitative research approach, this paper attempts to describe the dynamics of Indonesian cybersecurity, the application of the securitization process in cyberspace, and the implications of cybersecurity strategies in Indonesian cyberspace. The findings in the paper show that Indonesia has positioned the issue of cyber threats as a fairly serious security problem, but has not yet fully succeeded in carrying out full securitization but is

at the stage of Politicized towards Securitized.

Keywords: Cyber Threats; Cybersecurity; Indonesia; Securitization

PENDAHULUAN

Peningkatan teknologi informasi dan komunikasi pada dunia memberikan beragam perubahan masif dalam pola interaksi antar manusia dan antar kelompok. Keberadaan perubahan ini datang sebagai dampak utama dari kemunculan globalisasi, sebagai proses integrasi dunia menjadi satu melalui hubungan timbal balik antar entitas. Dalam menunjukkan adanya integrasi dunia ini, McGrew (2023) menjelaskan bahwa ekonomi global yang saat ini berjalan telah terikat melalui jaringan kompleks perdagangan internasional, keuangan global, digitalisasi dan jaringan produksi. Berangkat dari hal yang serupa, Mansbach dan Pirro (2023) juga menunjukkan hal yang sama di mana integrasi dunia saat ini telah berhasil menyatukan populasi manusia yang terdampak oleh globalisasi.

Menurut data laporan statistik dari Kepios, hingga Januari 2024, terdapat 5.35 Miliar orang atau sekitar 66.2% populasi di dunia menggunakan Internet dan 94.2% di antaranya atau sekitar 5.04 miliar orang adalah orang yang menggunakan media sosial sebagai mode komunikasi utamanya setiap bulan (Kemp, 2024a). Angka tersebut menunjukkan peningkatan yang sangat signifikan mengingat dalam laporan yang sama, ditunjukkan bahwa satu dekade yang lalu, yaitu pada tahun 2014 hanya terdapat 2.73 miliar pengguna internet di dunia, yang berarti saat ini telah mengalami peningkatan dua kali lipat dibandingkan dekade lalu. Lebih lanjut, lapor an tersebut juga menunjukkan bahwa dari Januari 2023 hingga Januari 2024 terdapat 266 juta pengguna media sosial baru, yang berarti menunjukkan bahwa tiap harinya hampir terdapat 730 ribu pengguna baru dalam media sosial (Kemp, 2024a).

Revolusi masif pada pembaharuan teknologi di masa kini dapat memungkinkan seluruh pengguna internet, terlepas dari mana dirinya berasal, untuk tetap dapat mendapat informasi secara cepat dan bebas, dan dapat ikut berinteraksi di dalamnya hingga pada tahap yang sebelumnya tidak dapat dibayangkan. Dalam melihat hal ini, Swara (2014) menunjukkan bahwa tingkat konsumsi informasi masyarakat di era modern membawa masyarakat pada sebuah kondisi sosial yang sulit dalam membedakan kehidupan dunia nyata dengan dunia tidak nyata (dunia internet). Pandangan tersebut menunjukkan bahwa saat ini keberadaan informasi yang masif dalam internet akan dikonsumsi secara sepenuhnya oleh masyarakat, terlepas dari layak atau tidaknya informasi tersebut. Akibatnya, masyarakat yang tidak dapat mencerna informasi dengan baik akan dengan mudah terbawa oleh media informasi, menjadi sebuah ancaman bagi

manusia karena potensi instabilitas keamanan dan potensi konflik antar individu maupun kelompok.

Peningkatan interaksi antar manusia dalam dunia internet tersebut kemudian dipahami lebih dalam sebagai *cyber domain* (domain siber) atau yang lebih dikenal sebagai *cyberspace* (ruang siber). Penggunaan istilah '*cyberspace*' dijelaskan lebih lanjut oleh National Institute of Standards and Technology sebagai sebuah lingkungan domain informasi global yang terdiri atas sistem-sistem komputer yang saling terinterkoneksi melalui internet (Reveron & Savage, 2023). Dari pengertian ini dapat dipahami bahwa ruang siber ini dibangun atas infrastruktur informasi dan komunikasi yang terkomputerisasi dan terhubung satu sama lain. Namun permasalahan dalam domain ini adalah adanya celah keamanan dalam sistem infrastruktur ruang siber yang kemudian dimanfaatkan melalui kemunculan tindakan kriminal tipe baru yang bekerja secara transnasional (United Nations, t. Thn.). Reveron dan Savage (2023) menunjukkan hal ini di mana kemunculan aktor-aktor seperti *hacker*, *phising scam artist*, dan *transnational criminal group* memanfaatkan perubahan melalui ruang siber ini sebagai alat melakukan tindakan jahat. Kemunculan ancaman ini tidak terlepas dari bagaimana *Morris Worm* yang menginfeksi komputer di dunia pada akhir 1988 (Federal Bureau of Investigation, 2018). Lebih lanjut, Reveron dan Savage (2023) menjelaskan bahwa melalui *cyberattack* (serangan dalam ruang siber) tersebut dapat dilakukan dalam beragam cara dengan tingkatan dampak yang berbeda-beda seperti penggunaan virus komputer, serangan *denial-of-service*, spionase, dan sebagainya. Disaat kemunculan ancaman yang masif, Fischerkeller (2021) menyatakan bahwa hukum internasional saat ini masih belum cukup memadai untuk dijadikan sebagai dasar dalam tata kelola ruang siber . Di sisi lain, Savaş dan Karataş (2022) menemukan bahwa penegakkan hukum tersebut dapat didasarkan pada aturan atau undang-undang dalam bidang sistem informasi dan teknologi namun tetap diperlukan konsesi yang komprehensif baik secara domestik maupun internasional untuk menjamin keamanan manusia dalam ruang siber .

Dengan adanya kemunculan ancaman tersebut, hal ini menjadi tantangan tersendiri bagi Indonesia yang sedang menjalani transformasi digital nasional. Dalam tiga tahun terakhir, Badan Sandi dan Siber Negara (BSSN) mencatat total lebih satu miliar serangan terjadi di Indonesia, dengan 266 juta serangan di tahun 2021 (Badan Sandi dan Siber Negara, 2022), 370 juta serangan di tahun 2022 (BSSN, 2023), dan 603 juta serangan di tahun 2023 (BSSN, 2024), dan terjadi lebih dari 1 miliar trafik anomali dalam ruang siber Indonesia pada tahun 2022 (CNN Indonesia, 2023a; Sinambela, 2023). Dalam skala nasional, serangan tersebut juga menjadi

permasalahan di mana data pribadi penduduk Indonesia yang dikelola pemerintah berhasil diretas sebagaimana yang terjadi dalam insiden serangan siber Bjorka di Indonesia pada tahun 2022 (CNN Indonesia, 2022b), serangan peretasan kelompok Brain Chiper pada Pusat Data Nasional Sementara (PDNS) Indonesia di tahun 2024 (CNN Indonesia, 2024a), dan insiden siber Bjorka yang kembali menyerang data Nomor Pokok Wajib Pajak (NPWP) milik masyarakat Indonesia (CNN Indonesia, 2024b). Serangan-serangan tersebut menunjukkan terdapat keterbalikan keadaan, di mana Indonesia mendapatkan peningkatan dalam sistem keamanan sibernya, namun pada praktiknya, serangan besar seperti ini tidak bisa ditangani dengan baik dan terjadi respons lambat dalam upaya penanganan dampak serangan siber.

Melihat perkembangan yang terjadi, (Nugraha, 2020; Sulistyo, 2020) menjelaskan bagaimana ancaman siber dapat mengancam kestabilan keamanan nasional Indonesia, dan dapat berkembang secara cepat dan masif seperti potensi *cyberterrorism* dan *cyberconflict*. (Rachmawati, 2019; Li & Liu, 2021; Hapsari & Pambayun, 2023; Setiawati et al., 2024) menjelaskan ancaman tersebut disebabkan oleh peningkatan yang sangat masif atas ruang siber, baik yang mengancam keamanan nasional maupun keamanan data milik masyarakat. Kemudian, (Klingova, 2013; Geelen, 2016; Ulum, 2017; Cavelty & Egloff, 2021; Wulan, 2021; Sutra & Haryanto, 2024) telah menunjukkan penggunaan teori sekuritisasi dalam ruang siber untuk menjelaskan bagaimana negara di dunia melakukan proses sekuritisasi terhadap ruang sibernya. Melalui uraian tersebut, dapat dipahami tulisan ini akan berfokus pada penggalian tentang bagaimana upaya-upaya pemerintah Indonesia dalam mengelola dan mengamankan ruang siber , dan memahami bagaimana Indonesia memosisikan serta memproses ancaman dalam ruang siber melalui perspektif teori sekuritisasi. Dengan kebaharuan yang telah disebutkan sebelumnya, Penulis berupaya untuk menjelaskan lebih lanjut mengenai bagaimana pemerintah Indonesia pada era Pemerintahan Joko Widodo dalam memanfaatkan, mengelola, dan mengamankan ruang siber Indonesia.

KERANGKA TEORI

Keamanan Siber

Keamanan siber memiliki definisi yang sangat beragam, terutama bergantung pada bidang kajian yang digunakan untuk memahami permasalahan dalam *cuberspace.* Secara sederhana, dalam tulisan ini keamanan siber dapat dipahami sebagai upaya mengamankan dunia maya dari segala *cyber threats* (ancaman siber) (Alam, 2022). Clark et al. (2014), mendefinisikan hal ini dengan lebih luas sebagai proses pencegahan dan mitigasi dampak atas tindakan negatif yang terjadi di dalam dunia

maya yang sekaligus dapat memengaruhi dunia nyata. Pandangan lain yang lebih komprehensif datang dari Schatz et al. (2017) dalam Alam (2022) yang menyatakan keamanan siber sebagai proses manajemen penanggulangan risiko keamanan oleh organisasi dan negara untuk melindungi kerahasiaan, integritas, dan ketersediaan data serta aset yang digunakan dalam dunia maya oleh para pengguna.

Kemudian, dalam pendekatan keamanan ini, meskipun terlihat memerlukan suatu konsesi internasional untuk membangun rezim siber yang universal, hingga saat ini belum terdapat peraturan, pedoman, atau konsep inti keamanan siber yang baku dan dapat diterima secara universal oleh seluruh negara di dunia. Meskipun terdapat beragam pendapat mengenai prinsip dasar keamanan siber, Ruthberg & McKenzie di tahun 1977 memperkenalkan hal tersebut melalui tiga prinsip dasar keamanan siber yang mereka sebut CIA Triad, yaitu *Confidentiality* (pencegahan pencurian data dan akses ilegal), *Integrity* (pencegahan modifikasi atau manipulasi data), dan *Availability* (kontinuitas layanan serta kemampuan pemulihan) (Alam, 2022). Penjelasan lebih lanjut datang dari Schiliro (2022) menyoroti lima elemen inti dalam keamanan siber, yaitu (1) *Prevention*, upaya inti dalam keamanan siber untuk mencegah potensi ancaman dalam mengakses atau menyerang sistem melalui pencegahan fisik, jaringan perangkat keras, dan perangkat lunak. (2) *Detection,* rangkaian proses untuk memeriksa dan mengidentifikasi ancaman terhadap sistem keamanan pada tahap awal, selama, dan setelah serangan terjadi. (3) *Respond,* penerapan langkah-langkah konkret untuk memitigasi dampak aktivitas berbahaya dalam sistem atau jaringan komputer. (4) *Internet of Things,* mengacu pada bagaimana keamanan siber menjadi relevan dan sangat penting karena integrasi konektivitas dalam aktivitas manusia dengan Internet. Serta (5) *Major Security Domains*, area dimana keamanan siber digunakan seperti *critical infrastructure security* (isolasi pada sistem jaringan sensitif), *application security* (mengamankan kelemahan dan celah perangkat lunak), *network security* (mengamankan kerentanan dalam transmisi data), dan *cloud security* (mengamankan data dalam infrastruktur komputasi awan).

Kemudian, Lewis (2009) dalam Reveron (2012) menunjukkan bahwa serangan yang dilakukan dalam ruang siber sangat sulit dibedakan antara berbagai intensitas dan intensi serangan. Ketidakmampuan negara dalam mengkategorikan serangan ini dapat menghambat negara sebagai aktor utama keamanan dalam menangani dan memitigasi *cyberthreats* di masa depan. Berdasarkan ini, Reveron (2012) juga menyebutkan bahwa, meski tidak sebagai panduan yang baku, ancaman dalam ruang siber dapat di analisis melalui aktor pelaku, target serangan, dan bagaimana serangan dilakukan

Sekuritisasi

Menurut Buzan et al., Sekuritisasi merupakan rangkaian langkah yang diambil oleh pemegang kekuasaan dalam membingkai suatu isu atau permasalahan melalui tindakan *speech acts* sehingga isu tersebut menjadi isu politik dengan sebutan *special politics* atau *above politics* (Buzan et al., 1998). Dari sudut pandang ini, sekuritisasi dapat diartikan sebagai pengidentifikasian isu-isu tertentu untuk dijadikan agenda keamanan yang memerlukan tindakan ekstrem, dengan aktor dominan berupa negara. Singkatnya, suatu isu telah melalui tiga tahap pembingkaian, yaitu tahap non-politis (*non-politicized*), politik (*politicized*), dan tersekuritisasi (*securitized*) (Buzan et al., 1998). Tahapan tersebut dimaknai oleh Buzan sebagai sebuah proses perubahan yang disebut sebagai proses perubahan isu publik menjadi isu politik. Proses pertama menurut Buzan, *Non-Politicized*, dapat dipahami sebagai tahap di mana suatu isu telah menjadi bahan perbincangan publik namun belum dianggap sebagai permasalahan bagi pemerintah. Proses kedua, *Politicized*, terjadi ketika pemerintah mulai menanggapi isu tersebut, yang berarti pemerintah mulai memberikan perhatian hingga terjadinya perundingan terkait permasalahan. Proses terakhir, *Securitized*, dipahami sebagai tahap akhir di mana negara mengakui keberadaan isu tersebut sebagai ancaman bagi keamanan nasional dan memulai perencanaan dalam perspektif keamanan darurat untuk menanggulangi atau mengatasi ancaman. Buzan menunjukkan dalam keseluruhan proses ini diperlukannya tindakan *speech acts* yang dapat diterima oleh masyarakat, sehingga masalah yang telah terjadi dan yang kemungkinan akan terjadi dapat dimitigasi dan dicegah melalui kebijakan atau strategi keamanan negara (Buzan et al., 1998).

Dalam proses sekuritisasi, *securitizing actors* (pelaku sekuritisasi) akan mengonstruksi objek yang terancam, atau disebut *referent objects*, sebagai fokus utama dalam tindakan pengamanan. Keberagaman atas *referent objects* yang dikonstruksi ini dapat dipengaruhi oleh berbagai hal, terutama adalah melalui bagaimana pelaku sekuritisasi melihat target pengamanan dari ancaman serta keberadaan *functional actosr* yang memengaruhi dinamika dalam konstruksi *referent objects* (Floyd, 2021). Dari proses konstruksi ini, pelaku sekuritisasi melakukan tindakkan *speech acts* sebagai upaya menarasikan ancaman (Buzan et al., 1998).

Dari tindakan tersebut, terdapat beberapa komponen penting bagi negara untuk dapat melakukan proses sekuritisasi. *Existential Threats* merupakan adanya ancaman yang dipandang mengganggu keamanan dan kestabilan negara atau mengganggu kepentingan negara. *Referent Objects* merupakan adanya objek yang dianggap penting yang perlu diamankan akibat dari ancaman. *Securitizing Actors*

merupakan adanya aktor yang melakukan tindakan *speech act* untuk menarasikan ancaman. *Audiences* merupakan adanya target (biasanya masyarakat publik) yang menjadi tujuan atas *speech act* yang dilakukan *securitizing actor. Functional actors* merupakan adanya aktor yang memberikan dinamika atas dilakukannya proses sekuritisasi, ini menunjukkan bahwa aktor ini dapat membantu terealisasinya sekuritisasi atas suatu isu ataupun menggagalkan proses sekuritisasi yang berjalan meskipun tidak terlibat secara langsung dalam prosesnya. (Buzan et al., 1998; Floyd, 2021).

Keberadaan ancaman tersebut dapat dipahami sebagai bentuk ancaman yang sangat kompleks. Ancaman yang bersifat teknis dapat dipolitisasi keamanannya melalui tindakan sekuritisasi keamanan siber. Lacy dan Prince (2017) menyebutkan keunikan atas sifat dari ancaman siber yang semakin rumit karena keterbukaan dunia maya, memaksa negara-negara untuk tetap dinamis dalam mengatasi celah kerentanan dan menjamin keamanan bagi mereka di dunia maya. Hal ini disebutkan melalui tulisan Hansen dan Nissenbaum (2009) yang menunjukkan kompleksitas keamanan dalam dunia maya. Berangkat dari pemikiran Buzan et al. (1998), Hansen dan Nissenbaum (2009) menunjukkan bahwa pendekatan sekuritisasi keamanan ini bekerja karena adanya ikatan ancaman terhadap *referent object* bagi negara. Adanya ancaman ini kemudian diklasifikasikan ke dalam tiga sektor keamanan, yang disebut sebagai *Hypersecuritization*, *Everyday Security Practice,* dan *Technification* (Hansen & Nissenbaum, 2009). *Hypersecuritization* mengacu terhadap suatu perluasan masalah yang diakibatkan oleh ancaman sehingga tindakan respon balik yang dilakukan dapat dibesar-besarkan, menandakan adanya ancaman yang harus segara di tanggulangi. *Everyday Security Practice* mengacu pada bagaimana cara aktor sekuritisasi untuk mengamankan jaringan, membuat publik untuk memahami keamanan dan mengamankan dirinya, dan membuat skenario *hypersecuritization* layak dilakukan serta dipahami oleh segala pihak. Dan terakhir, *Technification* yang mengacu pada bagaimana proses pembingkaian permasalahan teknologi ruang siber dapat menjadi ancaman terhadap keamanan dari suatu negara, ini terjadi karena adanya kerenggangan pemahaman dari masyarakat, publik, dan pemerintah dalam memersepsikan ancaman (Hansen & Nissenbaum, 2009).

METODE PENELITIAN

Dalam melakukan mendalami pokok bahasa penelitian ini penulis menggunakan metode penelitian kualitatif. Creswell & Creswell (2023) menunjukkan metode ini mencoba untuk mengembangkan dan memberikan gambaran kompleks atas suatu isu atau permasalahan melalui suatu perspektif berdasarkan interpretasi penulis

atas data atau informasi yang didapatkan. Penelitian Kualitatif Deskriptif digunakan penulis karena memungkinkan untuk menjelaskan gambaran yang lebih mendalam terkait pemerintah Indonesia pada era Pemerintahan Joko Widodo dalam memanfaatkan, mengelola, dan mengamankan ruang siber Indonesia. Sumber data ditekankan pada sumber data sekunder yang ditelusuri kemudian dikumpulkan melalui studi literatur yang mencakup buku, artikel jurnal, berita, peraturan terkait keamanan siber di Indonesia, dan tulisan lain yang penulis anggap memiliki relevansi dan dapat berkontribusi terhadap topik penelitian. Data yang diperoleh pada penelitian akan dianalisis melalui pendekatan analisis konten kemudian dikategorisasikan, namun tidak dibatasi, menjadi tiga tema utama yaitu Kondisi Keamanan Siber Indonesia, Ancaman dan Serangan Siber di Indonesia, dan Proses Sekuritisasi Keamanan Siber melalui *Speech Act*. Teori Sekuritisasi digunakan bersamaan dengan Konsep Keamanan Siber untuk memahami upaya-upaya Pemerintah Indonesia dalam mengelola dan mengamankan ruang siber Indonesia, dan memahami bagaimana Pemerintah Indonesia dalam memitigasi serangan siber Indonesia melalui perspektif teori Sekuritisasi. Kemudian, analisis dilakukan pada tingkat negara dengan mempertimbangkan dimana Keamanan Siber dianggap sebagai salah satu bagian vital dalam Keamanan Nasional Indonesia.

PEMBAHASAN

Dinamika Perkembangan Keamanan Siber di Indonesia

Perkembangan penegakan keamanan siber Indonesia dalam dekade juga telah mengalami perubahan yang besar. Fondasi kuat pada keamanan siber dibangun melalui transformasi Lembaga Sandi Negara menjadi BSSN di tahun 2017 sebagaimana diatur dalam Peraturan Presiden (Perpres) Nomor 53 Tahun 2017. Pembentukan BSSN dapat dianggap sebagai keseriusan Indonesia dalam upaya untuk meningkatkan sistem keamanan pada ruang siber Indonesia yang kemudian diperkuat dengan dibuatnya perubahan melalui Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara untuk penyesuaian terhadap ancaman dan perkembangan teknologi dunia, dan memperjelas tugas dan fungsi BSSN. Lebih lanjut, Priyandita (2024) menunjukkan peran BSSN tersebut juga didukung melalui peran dari Kementerian atau lembaga negara lain seperti Kementerian Komunikasi dan Informatika dalam pengendalian konten dan penyedia layanan, Kementerian Pertahanan dalam menjaga pertahanan dan keamanan siber pada objek vital dan infrastruktur negara, dan Jaksa serta Kepolisian Nasional Indonesia dalam penegakkan hukum di ruang siber Indonesia. Lebih lanjut, BSSN juga bekerja sama dengan sektor swasta dan masyarakat sipil untuk

membangun kesadaran, kapasitas, dan berbagi informasi seperti misalnya kerja sama dengan dibentuknya Honeynet Indonesia, dan pengembangan kapasitas sistem teknis dengan perusahaan teknologi seperti Cisco, Microsoft, dan Huawei (Priyandita, 2024).

Sejalan dengan upaya pembangunan fondasi sistem keamanan siber, regulasi terkait keamanan siber juga telah diberlakukan untuk memperkuat tata kelola dan pengamanan dalam ruang siber Indonesia. Undang-Undang Republik Indonesia (UU RI) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan peraturan siber pertama di Indonesia yang telah diperbarui (amandemen) sebanyak dua kali, yaitu dalam Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Melalui peraturan ini, Indonesia memiliki kemampuan untuk memberikan perlindungan atas kegiatan-kegiatan dalam ruang siber, termasuk penindakan atas kegiatan penyalahgunaan atau kejahatan dalam ruang siber.

Kemudian, untuk mendukung penguatan pada tata kelola ruang siber Indonesia juga turut diatur melalui Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Aturan ini memberikan kepastian hukum kepada pemilik data dalam ruang siber dengan mewajibkan penyelenggara sistem elektronik (PSE) untuk menjamin keamanan data publik yang dikelolanya.

Kemudian terkait mitigasi ancaman, Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital juga menjelaskan siapa yang bertanggung jawab terhadap sektor strategis di dunia maya yang berada di bawah pengelolaan kementerian guna mencegah terjadinya gangguan, kerusakan, atau musnahnya infrastruktur informasi vital akibat ancaman apapun. Peraturan Presiden (Perpres) Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber kemudian mengatur bagaimana cara kementerian dan lembaga negara dalam melindungi aset informasi nasional, ekosistem digital, dan infrastruktur vital.

Meskipun regulasi yang ada terlihat cukup memadai, Indonesia masih belum memiliki undang-undang yang secara khusus mengatur keamanan dan ketahanan siber. Meskipun proses penyusunan rancangan undang-undang tersebut telah dilakukan, Wakil Kepala BSSN menunjukkan bahwa rancangan ini setidaknya tidak dapat diselesaikan dalam waktu singkat (Nugroho, 2024). Hal ini dapat dipahami mengingat bahwa hingga saat ini, hukum internasional terkait keamanan siber baru saja mencapai tahap penyusunan konvensi internasional terkait *cybercrime*

(kejahatan siber), yang telah disahkan oleh Komite Ad Hoc PBB untuk Penyusunan Konvensi Internasional Komprehensif tentang Penanggulangan Penggunaan Teknologi Informasi dan Komunikasi untuk Tujuan Kriminal pada 9 Agustus 2024 (United Nations, 2024).

Selanjutnya dalam hal upaya peningkatan kemampuan siber dan peran Indonesia dalam menjaga keamanan siber regional dan internasional, Pemerintahan Indonesia di bawah kepemimpinan Presiden Joko Widodo telah mengikuti secara aktif dalam berbagai inisiatif. Sebagai contoh seperti ASEAN Regional Forum yang menegaskan terkait kerjasama dalam menjaga keamanan siber di Asia Tenggara (Natalia, 2021) dan kemudian direalisasikan melalui ASEAN Cyber Capacity Program (Rosandry, 2018), dan ASEAN-Japan Cyber Exercise (BSSN, 2019). Melalui inisiatif tersebut, Indonesia dan negara mitranya berfokus pada peningkatan kerjasama regional untuk dapat meningkatkan dan memperbaiki respons insiden siber, meningkatkan keahlian SDM dalam menanggulangi ancaman siber, dan menjaga kestabilan keamanan siber di wilayah Asia Tenggara. Dalam tingkat internasional, Indonesia juga berperan secara aktif dalam mendorong stabilitas siber dunia sebagaimana dalam pertemuan Dewan Keamanan PBB pada tahun 2020 (Kementerian Luar Negeri Indonesia, 2020). Kemudian dalam kemitraan antarnegara, Indonesia juga bermitra seperti dengan negara Australia untuk berpartisipasi dalam berbagai dialog strategis seperti IISS Shangri-La Dialogue di tahun 2019, dengan tujuan untuk membahas peningkatan kapabilitas siber negara-negara di dunia (Chotimah, 2019).

Meski dengan adanya peran aktif dan peningkatan yang baik dalam sistem keamanan sibernya, keamanan milik Indonesia tentu tidak luput dari ancaman besar yang ada dalam domain siber ini. Laporan dari Datareportal menunjukkan hingga Januari tahun 2024, terdapat 185.3 Juta orang atau sekitar 66.5% dari total penduduk Indonesia adalah pengguna internet dan 139 juta orang atau sekitar 50% dari total penduduk Indonesia adalah pengguna media sosial (Kemp, 2024b). Keberadaan pengguna internet yang masif ini sayangnya tidak diiringi dengan penerapan sistem dan kebijakan yang baik. Dalam laporan yang sama ditunjukkan Indonesia dengan populasi pengguna internet terbesar ke-4 di dunia dan ke-1 di Asia Tenggara. Namun berdasarkan laporan Global Cybersecurity Index 2020 dari International Telecommunication Union (2021) yang mengevaluasi komitmen dan kesiapan negara dalam hala keamanan siber, Indonesia menempati posisi ke-24 dari 194 negara, dan laporan dari National Cyber Security Index (2024) yang mengevaluasi kesiapan negara dalam mencegah ancaman siber dan mengelola insiden siber, dari tahun 2020 hingga 2023 Indonesia telah melakukan peningkatan dalam sistem

keamanan sibernya sehingga dalam laporan terbarunya Indonesia menempati posisi 49 dari 174 negara, meningkat cukup baik dibandingkan tahun 2020.

Dalam beberapa tahun terakhir, Indonesia telah menjadi target serangan siber dan aktivitas kriminal dalam dunia maya. Data dari BSSN selama 4 tahun terakhir pada bagian pendahuluan menunjukkan bahwa terdapat peningkatan sangat signifikan terkait jumlah serangan siber yang terdeteksi. Salah satu serangan yang cukup menonjol terkait hal ini adalah mengenai serangan dari seorang individu dengan nama samaran "Bjorka". Laporan dari CNN Indonesia (2022) menunjukkan bahwa Bjorka melakukan serangan siber terhadap ruang siber Indonesia dimulai pada serangan terhadap data pengguna loka pasar digital Tokopedia sebesar 24 *Gigabyte* (GB) pada bulan April tahun 2020, dan lebih dari 26 juta data pengguna layanan komunikasi IndiHome miliki Telkom Indonesia. Lebih lanjut di tahun 2022, pada bulan Agustus peretasan kembali terjadi pada 1.3 miliar data registrasi Kartu Surat Izin Mengemudi (SIM) juga kembali di bocorkan, 105 juta data penduduk dari Komisi Pemilihan Umum dan dokumen rahasia antara Presiden Joko Widodo dengan Badan Intelijen Negara (BIN) periode 2019- 2021 (CNN Indonesia, 2022b).

Selain Bjorka, beberapa aktor lain seperti Desorden, Lolyta, Strovian, dan Kotz juga terlibat dalam aktivitas serangan siber yang menargetkan Indonesia. Pada 23 Agustus 2022, Desorden merilis lebih dari 252 GB data pelanggan dan keuangan Jasamarga (Bestari, 2022), Di saat yang sama, Lolyta mengklaim memiliki lebih dari 17 juta data lengkap pelanggan Perusahaan Listrik Negara (PLN) (Anam, 2022), sementara Strovian mengaku memiliki data agen BIN (CNN Indonesia, 2022b). Dan Kotz, mengklaim memiliki dan menjual sebanyak 279 juta data warga negara Indonesia dari Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan pada tahun 2021 (Menpan.go.id, 2021).

Bergerak pada tahun ini, Indonesia mengalami serangan siber yang berskala lebih masif. Pada Juli 2024 terjadi insiden siber yang lebih masif dimana terjadi serangan *ransomware* oleh kelompok peretas Brain Chiper terhadap Pusat Data Nasional Sementara (PNDS) Indonesia yang berdampak pada terhambatnya aktivitas 210 instansi Pemerintah Pusat dan Daerah selama lebih dari dua minggu (CNN Indonesia, 2024). Adristi dan Ramadhani (2024) menunjukkan bahwa dalam insiden ini, PDNS 2 Surabaya tidak memiliki data cadangan (*backup*) yang memadai dan pemerintah sedang menggodok aturan kewajiban *backup* data. Lebih lanjut, Ulya dan Farisa (2024) menunjukkan bahwa insiden tersebut tidak dapat dimitigasi secara maksimal akibat dari tata kelola PDNS yang kurang sempurna dan upaya pengawasan pada sistem yang tidak maksimal. Di sisi lain, tindakan serangan yang cukup besar lain terjadi di bulan Agustus dan September, yaitu peretasan terhadap

4.7 juta baris data Aparatur Sipil Negara yang di kelola oleh Badan Kepegawaian Negara (BKN) (Aji, 2024), dan peretasan 6 juta baris data Nomor Pokok Wajib Pajak (NPWP) yang dikelola oleh Direktorat Jendral Pajak (DJP) Kementerian Keuangan (Ardyanto, 2024).

Keberadaan insiden-insiden tersebut menunjukkan adanya kelemahan serius dalam tata kelola sistem keamanan siber Indonesia. Meskipun Indonesia telah berhasil dalam mengikuti dinamika teknologi dalam ruang siber yang selalu berkembang, proses implementasi hukum Indonesia masih belum sempurna akibat dari pelaksanaan yang belum maksimal, dan kurangnya kepekaan pemerintah terhadap keseriusan ancaman siber menurunkan efektivitas dalam mitigasi ancaman siber. Selain itu, ketiadaan hukum internasional yang spesifik terkait keamanan siber memperhambat dalam proses mitigasi global karena adanya perbedaan persepsi ancaman yang dilihat oleh negara-negara di dunia.

Proses Sekuritisasi Keamanan Siber Indonesia

Buzan et al. (1998) menunjukkan bahwa proses sekuritisasi atas suatu isu dimulai berdasarkan tindakkan *speech act* yang telah dilakukan oleh pelaku sekuritisasi. Upaya pemerintah untuk melaksanakan proses sekuritisasi ditunjukkan dalam studi ini melalui cara pemerintah dalam menanggapi ancaman siber dalam kasus serangan siber Bjorka pada tahun 2022 dan penyerangan PDNS 2 Surabaya pada tahun 2024. Dalam hal tersebut, komponen-komponen penting dalam sekuritisasi diklasifikasikan berdasarkan tindakan *speech act* yang telah dilakukan pemerintah. *Existential Threats* dalam hal ini merujuk pada tindakan pembocoran data oleh Bjorka yang dilakukan pada bulan September 2022, dan tindakan pembobolan Pusat Data Nasional Sementara (PDNS) 2 Surabaya oleh kelompok Brain Chiper pada bulan Juni 2024. *Referent Objects* dalam hal ini merujuk pada keamanan data dan ketersediaan data dalam ruang siber Indonesia yang dikelola oleh Pemerintah. *Audiences* merujuk pada masyarakat umum yang secara langsung terdampak dari ancaman siber. *Functional Actors* merujuk pada badan lembaga, kementerian atau organisasi lain yang secara langsung bertanggung jawab untuk memberikan solusi teknis atas isu, dalam hal ini Kementerian informasi, dan BSSN akan menjadi fokus utama dalam tulisan. Dan *Securitizing Actors* difokuskan pada tindakan-tindakan dan upaya *speech act* yang dilakukan untuk mengangkat isu dan mendorongnya menjadi ancaman terhadap keamanan nasional, dalam hal ini Presiden Joko Widodo akan menjadi fokus utama dan bagian pemerintah lain akan menjadi *securitizing actor* berdasarkan konteks pernyataan yang diberikan.

Buzan et al. (1998) telah menunjukkan dimana terdapat setidaknya tiga proses tahapan dalam upaya melakukan tindakan Sekuritisasi. Pertama dimulai dengan non-politisasi (*non-politicized*), dimana ancaman yang menjadi masalah masih belum ditindak oleh pemerintah. Pradnyana (2023) dan Ramadhan (2023) menunjukkan dimana tahap ini pemerintah tidak melihat masalah akibat ancaman yang terjadi bukan merupakan sebuah masalah keamanan sehingga tidak diperlukan tindakan lanjutan selain identifikasi dampak dan pemulihan akibat serangan.

Tahap selanjutnya adalah politisasi (*politicized*), dimana ancaman mulai menarik perhatian pemerintah dan menjadi fokus penanggulangan terkait masalah, Nugraha (2020) menunjukkan penggunaan *soft power* menjadi tindakan pertama dalam penanggulangan masalah seperti dilakukannya koordinasi antar lembaga dalam mengidentifikasi dan mencegah perluasan dampak akibat ancaman. Disisi lain Pradyana (2023) juga menunjukkan dimana penggunaan *hard power* dapat mulai digunakan sebagai langkah pengamanan dan pencegahan serangan lanjutan dalam waktu serangan sebelumnya masih belum selesai di mitigasi.

Kemudian tahap terakhir adalah sekuritisasi (*securitized*), dimana pemerintah telah memutuskan dilakukannya tindakan lanjutan dalam menekan atau mengamankan ancaman. Nugraha (2020) menunjukkan hal serupa dimana pada tahap ini mitigasi ancaman dengan menggunakan *hard power* menjadi dominan digunakan oleh negara seperti misalnya melakukan pemantauan ketat atas target serangan, memberikan sistem keamanan baru yang lebih kompleks, penegakkan hukum dan dibuatnya kebijakan khusus yang dibuat untuk memitigasi ancaman. Selain itu pada tahap ini tindakan ekstrem seperti deklarasi perang akibat ancaman dapat dilakukan negara, sebagaimana yang ditunjukkan oleh Datta & Acton (2022) melalui kondisi Kosta Rika pada tahun 2022 yang mendeklarasikan negara dalam keadaan perang sebagai tindakan mendesak negara melindungi infrastruktur digital vital negara dari serangan siber.

Untuk memaparkan tahapan upaya sekuritisasi terhadap kedua kasus yang diangkat tulisan ini, penulis akan memaparkan pernyataan-pernyataan yang dikeluarkan oleh Pemerintah untuk melihat bagaimana Pemerintah memberikan respons atau memandang keberadaan ancaman pada ruang siber Indonesia.

Tabel 1. Tahapan Sekuritisasi Pemerintah pada serangan Bjorka tahun 2022

Tanggal	Sumber Berita	Pernyataan	*Functional / Securitizing Actors*	Tahapan
6 Juli 2022	Antara	Kebocoran data pelanggan IndiHome tidak terjadi pada *database server*, dan klaim pembobolan data ditemukan beberapa kejanggalan atas validitasnya	*SVP Corporate Communication & Investor Relation,* Telkom Ahmad Reza	Non-politisasi

1 September 2022	CNN Indonesia	Kebocoran data registrasi *SIM Card* bukan dari Kominfo	Sekjen Kementerian Kominfo, Mira Tayyiba	Non-politisasi
1 September 2022	CNBC Indonesia	Kebocoran data registrasi *SIM Card* bukan dari *Database* milik Dinas Kependudukan dan Catatan Sipil	Direktur Jenderal Kependudukan dan Pencatatan Sipil, Zudan Arif Fakrulloh	Non-politisasi
4 September 2022	Ditjen Aptika Kominfo	Akan dilakukan koordinasi untuk menindaklanjuti dugaan kebocoran data kartu SIM	Direktur Jenderal Aplikasi Informatika, Semuel Abrijani Pangerapan	Politisasi
4 September 2022	Kompas	Masyarakat harus berhati-hati dalam penggunaan NIK dan harus bertanggung jawab untuk menjaga keamanan NIK-nya sendiri	Menteri Komunikasi dan Informatika, Johnny G. Plate	Politisasi
6 September 2022	Kompas	Kementerian Kominfo memiliki tanggung jawab atas kebocoran data *SIM Card*	Ketua Komisi I DPR RI, Meutya Hafid	Politisasi
6 September 2022	Kompas	Data yang dibocorkan bukan milik KPU, dan semua sistem keamanan informasi masih kondusif	Koordinator Divisi Data dan Informasi KPU RI, Betty Epsilon	Non-politisasi
7 September 2022	CNN Indonesia	Semua serangan siber atas ruang digital Indonesia menjadi domain teknis dan tugas BSSN bukan Kominfo	Menteri Komunikasi dan Informatika, Johnny G. plate	Politisasi
10 September 2022	CNBC	Seluruh surat atau dokumen milik BIN aman dari kebocoran dan selalu terenkripsi secara maksimal	Juru Bicara Badan Intelijen Negara, Wawan Purwanto	Non-politisasi
10 September 2022	Antara	Tidak ada dokumen rahasia milik Presiden yang bocor	Kepala Sekretariat Presiden, Budi Hartono	Non-politisasi
12 September 2022	BBC Indonesia	Seluruh data yang dibocorkan Bjorka hanya bersifat umum, dan serangannya tidak membahayakan negara	Menteri Koordinator Bidang Politik, Hukum dan HAM, Mahfud MD	Non-politisasi
20 September 2022	Ditjen Aptika Kominfo	Seluruh pengendali data pribadi baik publik maupun privat wajib mematuhinya UU PDP	Menteri Komunikasi dan Informasi, Johnny G. Plate	Politisasi
20 September 2022	CNN Indonesia	Pengesahan Rancangan Undang-Undang tentang Perlindungan Data Pribadi tidak ada kaitannya dengan serangan Bjorka	Menteri Koordinator Bidang Politik, Hukum dan HAM, Mahfud MD	Non-politisasi
23 September 2022	detikNews	Data yang dibocorkan Bjorka merupakan data palsu dan merupakan data usang	Kepala Divisi Humas Polri Indonesia, Dedi Prasetyo	Non-politisasi
24 September 2022	CNN Indonesia	Komisi 1 DPR RI menyetujui kenaikan alokasi anggaran untuk BSSN untuk peningkatan pertahanan siber	Wakil Ketua Komisi I DPR RI, Utut Adianto	Sekuritisasi

13 Oktober 2022	CNN Indonesia	Keamanan siber negara adalah tanggung jawab milik bersama, dan seluruh aspek keamanan siber milik Pemerintah akan diuji ulang	Menteri Komunikasi dan Informasi, Johnny G. Plate	Sekuritisasi
10 November 2022	CNN Indonesia	Kebocoran pada aplikasi MyPertamina sedang di investigasi lebih lanjut	Sekretaris Perusahaan Pertamina Patra Niaga, Irto Ginting	Politisasi
17 November 2022	CNBC Indonesia	Masyarakat harap tenang dan menunggu hasil investigasi terhadap dugaan peretasan data PeduliLindungi rampung	Juru Bicara Kementerian Kesehatan, Mohammad Syahril	Politisasi
23 November 2022	CNBC Indonesia	Kominfo belum menerima hasil investigasi atau tanggapan dari Pertamina	Menteri Komunikasi dan Informasi, Johnny G. Plate	Politisasi
23 November 2022	Ditjen Aptika Kominfo	Kementerian Kesehatan RI masih memproses data dan melakukan uji forensik digital	Menteri Komunikasi dan Informasi, Johnny G. Plate	Politisasi

Sumber: hasil pengolahan data oleh penulis berdasarkan sumber berita

Berdasarkan kumpulan data sebelumnya, dapat diketahui bahwa pemerintah memberikan tanggapan yang sangat bervariatif terkait penanganan dugaan kasus peretasan yang terjadi di sepanjang bulan September hingga Desember 2022. Menurut tanggapan yang telah dikumpulkan tersebut, dapat terlihat jika pemerintah tidak berupaya untuk melakukan proses sekuritisasi pada ruang siber Indonesia melainkan hanya pada batas melakukan tindakan pengamanan terkait dugaan serangan siber yang telah terjadi dan siaran pers. Adapun beberapa tindakan yang berbeda dilakukan oleh beberapa bagian Pemerintah seperti peningkatan alokasi anggaran yang ditetapkan untuk BSSN dan adanya perubahan pernyataan oleh Menteri Komunikasi dan Informasi, Johnny G. Plate, dari yang menyangkal jika serangan siber merupakan tanggung jawab dan tugas milik Kominfo menjadi menerima jika keamanan siber merupakan upaya milik bersama.

Melalui tabel tersebut juga diketahui bahwa para *securitizing actors* dalam kasus ini tidak menganggap kasus serangan yang terjadi memerlukan tindakan pengamanan secara khusus. Tindakan pemerintah yang menyetujui peningkatan pada anggaran BSSN, dan pernyataan dari komisi 1 DPR RI menunjukkan adanya keseriusan pemerintah terhadap upaya pengamanan ruang siber Indonesia. Namun hal tersebut tidak dapat dianggap sebagai tindakan sekuritisasi mengingat Presiden Joko Widodo dalam hal ini tidak memberikan pernyataan secara langsung dalam *speech act*-nya untuk menunjukkan jika penyelesaian permasalahan terkait serangan siber Bjorka akan diselesaikan sebagai sebuah isu keamanan nasional. Adapun pernyataan dari Menteri Koordinator Bidang Politik, Hukum dan HAM, Mahfud

MD, yang menunjukkan jika seluruh serangan yang dilakukan oleh Bjorka tersebut tidak membahayakan keamanan nasional Indonesia. Terlepas dari hal tersebut, perlu disoroti dimana pemerintah pada jangka waktu tersebut mengesahkan Rancangan Undang-undang Perlindungan Data Pribadi (RUU PDP) pada 20 September 2022, dan secara resmi disahkan oleh Presiden Joko Widodo pada 18 Oktober 2022 (CNN Indonesia, 2022a). Melalui pengesahan tersebut, meskipun tidak terkait dengan serangan Bjorka, menunjukkan upaya konkret Pemerintah dalam upaya sekuritisasi terhadap Keamanan Siber Indonesia.

Kemudian, dalam melihat proses pada upaya sekuritisasi Pemerintah Indonesia terhadap kasus penyerangan PDNS 2 Surabaya.

Tabel 2. Tahapan Sekuritisasi Pemerintah pada serangan PDNS 2 Surabaya tahun 2024.

Tanggal	Sumber Berita	Pernyataan	*Functional* / *Securitizing Actors*	Tahapan
20 Juni 2024	Antara	Gangguan pada sistem imigrasi akibat Pusat Data Nasional yang dikelola Kominfo sedang bermasalah	Direktur Jenderal Imigrasi Kementerian Hukum dan Hak Asasi Manusia, Silmy Karim	Non-politisasi
20 Juni 2024	Antara	Sedang dilakukan pemulihan layanan pada pusat Data Nasional yang sedang mengalami gangguan	Menteri Komunikasi dan Informasi, Budi Arie Setiadi	Non-politisasi
24 Juni 2024	Tempo	Gangguan pada sistem Pusat Data Nasional akibat serangan siber *ransomware* yang dimulai pada 17 Juni 2024	Juru bicara Badan Siber dan Sandi Negara (BSSN), Ariandi Putra	Politisasi
24 Juni 2024	Tempo	Serangan *ransomware* hanya menyasar Pusat Data Nasional Sementara (PDNS) 2 Surabaya, Pusat Data lain aman dari serangan	Kepala Badan Siber dan Sandi Negara (BSSN), Hinsa Siburian	Politisasi
25 Juni 2024	Kompas	Komisi 1 DPR RI menyelenggarakan Rapat Kerja untuk meminta penjelasan lanjutan dari Kominfo dan BSSN terkait serangan siber dan pemulihan PDNS 2 Surabaya	Ketua Komisi I DPR RI, Meutya Hafid	Politisasi
27 Juni 2024	Tempo	Dampak serangan Siber pada PDNS 2 berada pada tingkat *critical* dan *major*	Menteri Komunikasi dan Informasi, Budi Arie Setiadi	Politisasi
27 Juni 2024	Liputan6	Telkom berkolaborasi bersama BSSN, Bareskrim, dan Kominfo bekerja sama untuk memitigasi dampak serangan dan mencegah serangan serupa terjadi	*VP Investor Relation* Telkom Indonesia Tbk., Octavius Oky Prakarsa	Politisasi
27 Juni 2024	Media Indonesia	Keamanan siber Indonesia masih perlu peningkatan dan masih tergolong rendah	Menteri Komunikasi dan Informasi, Budi Arie Setiadi	Politisasi

27 Juni 2024	EMedia DPR RI	Kegagalan dalam melindungi data di PDNS merupakan kegagalan dalam keamanan nasional	Anggota Komisi I DPR RI, Sukamta	Sekuritisasi
28 Juni 2024	DetikNews	Presiden Joko Widodo melakukan rapat terbatas untuk membahas serangan pada PDNS 2	Presiden RI, Joko Widodo	Sekuritisasi
28 Juni 2024	CNN Indonesia	Presiden Joko Widodo memerintah Badan Pengawasan Keuangan dan Pembangunan (BPKP) untuk mengaudit tata kelola PDNS	Presiden RI, Joko Widodo	Sekuritisasi
1 Juli 2024	Pers Sekretariat Kabinet RI	Pelayanan publik pada PDNS akan pulih dibulan Juli, PDN Batam akan ditingkatkan kemampuannya, dan kewajiban pencadangan data milik Kementerian, Lembaga Negara, dan Pemerintah Daerah.	Menteri Koordinator Bidang Politik, Hukum, dan Keamanan, Hadi Tjahjanto	Sekuritisasi
3 Juli 2024	Pers Presiden RI	Evaluasi menyeluruh atas insiden dan penekanan atas kewajiban pencadangan data pada seluruh pusat data nasional	Presiden RI, Joko Widodo	Sekuritisasi

Sumber: hasil pengolahan data oleh penulis berdasarkan sumber berita

Berbeda dengan upaya pemerintah pada kasus serangan Bjorka di tahun 2022, pada kasus ini pemerintah memiliki tahapan proses yang lebih spesifik mengarah pada proses sekuritisasi keamanan siber Indonesia. Proses tersebut ditandai dengan dilakukannya upaya politisasi terhadap kasus penyerangan PDNS 2 tersebut melalui adanya rapat kerja yang secara khusus membahas serangan siber dan pemulihan data pada PDNS 2 Surabaya pada 25 Juni 2024. Hal tersebut ditunjukkan adanya pernyataan dari Anggota Komisi I DPR RI, Sukamta, dimana serangan ini ditunjukkan sebagai kegagalan dalam menjaga keamanan nasional Indonesia. Upaya sekuritisasi juga diperkuat dengan tindakan dan pernyataan Presiden Jokowi untuk dilakukannya audit pada tata kelola PDNS dan penekanan pada kewajiban pencadangan data pada seluruh pusat data nasional. Pernyataan tersebut menunjukkan bahwa Pemerintah Indonesia dalam kasus ini melakukan tindakan sekuritisasi sebagaimana *speech act* yang dilakukan oleh Presiden Joko Widodo yang menganggap kasus ini perlu dilakukan tindakan penting yang harus segera dilakukan.

Implikasi Strategi Keamanan Siber pada Ruang Siber Indonesia

Berdasarkan pembahasan sebelumnya, ditemukan bahwa aktivitas ruang siber Indonesia sudah berada di bawah ancaman siber yang cukup serius. Disamping ancaman yang masif, ancaman-ancaman tersebut berpotensi untuk terulang kembali dengan skala maupun motif yang sangat beragam. Hal ini ditunjukkan melalui

kemunculan rentetan serangan Bjorka di tahun 2022 yang menargetkan data yang dikelola oleh Kementerian dan Lembaga Negara, dan serangan pada PDNS 2 yang mengancam infrastruktur vital negara menjadi bukti nyata dimana ancaman siber memiliki potensi besar terulang kembali dengan cara yang bervariatif sehingga menuntut adanya adaptasi cepat dan fleksibel yang dilakukan oleh Pemerintah Indonesia. Dari sini terlihat di mana regulasi terkait pengamanan ruang siber Indonesia mulai menjadi sangat penting keberadaannya mengingat dampak atas ancaman tersebut yang secara langsung mengganggu stabilitas keamanan masyarakat dan khususnya Pemerintah.

Dalam tulisan ini, telah ditunjukkan dimana Pemerintah Indonesia berperan secara aktif untuk mengatur kehidupan masyarakat dalam ruang siber Indonesia, utamanya dalam tujuannya dalam memberikan kesejahteraan dan memastikan keamanan bagi masyarakat siber. Aji (2023) berpendapat bahwa saat ini, isu-isu dalam ruang siber sangat erat berkaitan dengan permasalahan politik, utamanya terkait dampaknya terhadap pemenuhan kepentingan nasional dan kedaulatan negara atas ruang sibernya. Bagi Indonesia, saat ini UU ITE, dan UU PDP berperan sebagai cara bagi Pemerintah dalam meregulasi dan memecahkan permasalahan perlindungan dalam ruang siber Indonesia. Meskipun sudah memiliki instrumen hukum yang jelas, beberapa ahli menunjukkan bahwa implementasi atas undang-undang tersebut masih tidak optimal (Dzulfikar & Ramadhani, 2022). Hal ini dapat dilihat dimana kasus serangan siber pada PDNS 2 terjadi tanpa adanya deteksi dan penanganan yang memadai diiringi oleh minimnya sumber daya teknis dalam merespons serangan. Namun, seperti yang dapat dilihat sebelumnya jika hingga saat ini pemerintah masih belum dapat secara maksimal dalam menanggulangi ancaman siber yang terjadi mengingat undang-undang yang ada baru berjalan dalam waktu yang cukup singkat sehingga masih dalam tahap penyesuaian, terlebih lagi hingga saat ini dalam level global masih belum ada persamaan persepsi mengenai tingkat ancaman siber bagi negara dan bagaimana menanggulangi ancaman siber sebagai ancaman transnasional.

Sebagaimana telah dibahas oleh Hansen dan Nissenbaum (2009), penggunaan pendekatan sekuritisasi untuk memproses ancaman siber dilakukan dalam tiga klasifikasi bidang keamanan. Dalam konteks *Everyday Security Practice*, melalui kombinasi atas Perpres No. 47 Tahun 2023, UU ITE, dan UU PDP telah mencerminkan strategi nasional Indonesia untuk membangun ekosistem keamanan siber yang lebih baik melalui pemberian kepastian dan penegakkan hukum di ruang siber Indonesia. Namun terlihat seperti yang dijelaskan jika implementasi terhadap regulasi ini masih tidak berjalan secara maksimal dan masih memerlukan regulasi

khusus yang membahasa mengenai strategi dasar keamanan siber, yang mana hingga kini masih dalam tahap penyusunan dalam Rancangan Undang-Undang Keamanan dan Ketahanan Siber.

Dalam konteks *Technification*, terlepas dari adanya pelemparan tanggung jawab sebagaimana yang terjadi dalam kasus Bjorka di 2022, Pemerintah Indonesia telah membangun fondasi utamanya dalam penegakkan keamanan siber Indonesia. Melalui pembentukan BSSN yang berkaitan dengan Kementerian dan Lembaga Negara lain, menunjukkan adanya upaya dalam membingkai isu siber ini dalam konteks keamanan nasional meskipun pada temuan ditunjukkan bahwa Indonesia belum memasuki tahapan sekuritisasi secara penuh dan pelaksanaan atas regulasi ruang siber masih belum secara penuh berjalan optimal melihat dari respons pemerintah terhadap kedua serangan.

Terakhir dalam *Hypersecuritization*, upaya pemerintah melalui dua kasus serangan siber menunjukkan tidak adanya upaya pemerintah dalam melakukan sekuritisasi secara penuh ruang siber Indonesia, mengingat tidak adanya struktur kebijakan keamanan nasional yang berubah atau dibuat secara khusus untuk memitigasi hasil dari serangan siber tersebut. Hal ini terlihat dimana Pemerintah hanya melakukan mitigasi dampak serangan yang telah terjadi untuk mencegah kerusakan lebih lanjut dan memastikan pelayanan digital serta keamanan data dapat terus berjalan. Meskipun seperti itu, dapat dilihat jika pemerintah telah memersepsikan ancaman siber sebagai ancaman nyata yang serius bagi keamanan nasional sebagaimana yang terjadi dalam kasus serangan siber PDNS 2. Berkaca pada hasil tiga konteks sekuritisasi keamanan siber tersebut dapat ditunjukkan jika saat ini Pemerintah telah melakukan perubahan yang mulai berfokus dalam menjamin kepastian hukum dan keamanan pengguna dalam ruang siber Indonesia.

Banyaknya keberagaman dalam pengguna internet dalam ruang siber Indonesia menyebabkan terjadinya berbagai risiko dan kerentanan. Melihat banyaknya upaya serangan yang terjadi dan kejadian serangan siber yang telah berlalu, menunjukkan bahwa keamanan siber sudah menjadi hal fundamental yang perlu di amankan demi menjamin kehidupan masyarakat terhindar dari tindakan kejahatan siber. Aji (2023) menunjukkan hal ini dimana pemahaman Pemerintah terhadap urgensi untuk melindungi ruang siber Indonesia perlu dimaksimalkan dalam waktu dekat. Lebih lanjut, peran warga negara pun juga perlu diperhatikan karena dalam proses sekuritisasi sangat memerlukan perhatian dari warga negara sebagai *target audiences* untuk turut mengakui bahwa isu serangan tersebut merupakan isu keamanan yang penting. Kemudian, Butarbutar (2023) juga menunjukkan jika kejahatan siber terhadap individu saat ini sudah semakin marak

terjadi sehingga masyarakat tidak dapat hanya bergantung pada penyedia layanan keamanan ataupun Negara tetapi juga harus memahami beragam tindakan kejahatan siber yang secara langsung menargetkan keamanan, privasi, dan kesejahteraan individu.

Komitmen Pemerintah Indonesia dalam kepemimpinan Presiden Jokowi menunjukkan arah perbaikan dalam tata kelola infrastruktur informasi dan sistem keamanan siber Indonesia. Melalui regulasi yang telah disahkan, arah kebijakan Pemerintah Indonesia telah mulai bergerak menuju melakukan upaya sekuritisasi siber di Indonesia. Hal ini dapat dilihat melalui pergerakan BSSN dalam mendorong penyusunan RUU Keamanan dan Ketahanan Siber dalam rencana kerja prioritas pemerintah di tahun 2025-2029 (Nugroho, 2024). Selain itu, kemunculan wacana pembentukan angkatan siber dalam Tentara Nasional Indonesia menunjukkan adanya respon baik dari Pemerintah meskipun masih dalam tahap pertimbangan (CNN Indonesia, 2023b; CNN Indonesia, 2023c). Hatim et al. (2024) menunjukkan peran Satuan Siber TNI dan *Cyber Police* POLRI merupakan aspek penting dalam menjaga keamanan dan pertahanan siber negara, serta menjamin ruang digital yang aman dan bersih. Melalui wacana pembentukan angkatan siber menunjukkan bahwa pemerintah dapat melakukan upaya sekuritisasi lebih lanjut terhadap keamanan siber Indonesia, dan berpotensi untuk menjadi negara yang berdaulat atas ruang sibernya sendiri dengan mengombinasi regulasi komprehensif, infrastruktur yang memadai, dan sumber daya manusia yang berkualitas untuk menjamin stabilitas keamanan dan pertahanan siber Indonesia.

KESIMPULAN

Melalui proses tahapan Sekuritisasi Buzan, terlihat jika Pemerintah melakukan dua cara yang berbeda dalam menangani kedua kasus yang diangkat pada tulisan. Pendekatan Sekuritisasi lebih terlihat dilakukan oleh Pemerintah pada kasus serangan pada Pusat Data Nasional (PDNS) 2 Surabaya. Hal ini dilihat dari pendekatan serius dan terfokus yang dilakukan oleh Pemerintah dalam memitigasi serangan siber tersebut. Hal ini dapat dipahami mengingat Pemerintah Indonesia memosisikan PDNS sebagai sebuah infrastruktur informasi vital yang menyangkut kelangsungan pelayanan digital secara nasional sehingga dengan adanya serangan tersebut pemerintah mengambil tindakan lebih tegas dalam memitigasinya.

Kemudian, melihat sekuritisasi atas ruang siber yang dikembangkan oleh Hansen dan Nissenbaum terlihat Pemerintah Indonesia telah melakukan beberapa upaya sekuritisasi. *Everyday security practice* telah diwujudkan melalui dibentuknya kebijakan siber seperti UU ITE, UU PDP, Perpres No. 47 Tahun 2023, dan

perencanaan atas RUU PDP. Kemudian *Technification*, telah diwujudkan melalui pembentukan BSSN yang berkaitan dengan kementerian dan lembaga negara lain yang diatur dalam Perpres No. 82 Tahun 2022. Terakhir, *Hyperpersecuritization,* melalui kedua serangan ditunjukkan jika Pemerintah Indonesia tidak melakukan tindakan lain selain mitigasi serangan sehingga dapat disimpulkan jika Pemerintah telah melakukan tindakan politisasi isu tersebut ke dalam isu politik dan menunjukkan adanya arah perkembangan untuk membawa isu tersebut ke dalam isu keamanan.

DAFTAR PUSTAKA

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi). *Politica. 13*(2), 222-238. DOI: 10.22212/jp.v13i2.3299

Aji, R. (2024, 12 Agustus). *BKN Buka Suara Soal Data ASN Diduga Bocor dan Dijual*. Tersedia dalam CNBC Indonesia: https://www.cnbcindonesia.com/news/20240812062338-4-562142/bkn-buka-suara-soal-data-asn-diduga-bocor-dan-dijual

Alam, S. (2022). *Cybersecurity: Past, Present and Future.* Tersedia dalam Cornell University Cryptography and Security ArXiv. DOI: 10.48550/arXiv.2207.01227

Andryanto, S. D. (2024, 23 September). *6 Juta Data NPWP Bocor Termasuk Milik Jokowi, Pegiat Keamanan Siber: Bjorka Paham Dinamika Politik Indonesia*. Tersedia dalam Tempo Nasional: https://nasional.tempo.co/read/1919567/6-juta-data-npwp-bocor-termasuk-milik-jokowi-pegiat-keamanan-siber-bjorka-paham-dinamika-politik-indonesia

Badan Siber dan Sandi Negara. (2021). Laporan Tahunan Honeynet Project 2020. Jakarta: Deputi Bidang Operasi Keamanan Siber dan Sandi BSSN.

Badan Siber dan Sandi Negara. (2022). Laporan Tahunan Honeynet Project 2021. Jakarta: Deputi Bidang Operasi Keamanan Siber dan Sandi BSSN.

Badan Siber dan Sandi Negara. (2023). Laporan Tahunan Honeynet Project 2022. Jakarta: Deputi Bidang Operasi Keamanan Siber dan Sandi BSSN.

Badan Siber dan Sandi Negara. (2024). Laporan Tahunan Honeynet Project 2023. Jakarta: Deputi Bidang Operasi Keamanan Siber dan Sandi BSSN.

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economic Law Journal. 2*(2), 299-317. DOI: : 10.21143/TELJ.vol2.no2.1043

Buzan, B., Wæver, O., & Wilde, J. (1998). *Security: A New Framework for Analysis*. London: Lynne Rienner Publisher.

Cavelty, M. D., & Egloff, F. J. (2021). Hyper-Securitization, Everyday Security Practice and Technification: Cyber-Security Logics in Switzerland. Swiss Political Science Review. 27(1), 139 - 149. DOI: 10.1111/spsr.12433.

Clark, D., Berson, T., & Lin, Herbert. (2014). *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington, DC.: National Research Council.

CNN Indonesia. (2022a, 18 Oktober). Jokowi Teken UU Perlindungan Data Pribadi, Pelanggar Didenda Rp6 M. Tersedia dalam CNN Indonesia: https://www.cnnindonesia.com/teknologi/20221018190144-185-862275/jokowi-teken-uu-perlindungan-data-pribadi-pelanggar-didenda-rp6-m

CNN Indonesia. (2022b, 30 Desember). *10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-ramai Bantah*. Tersedia dalam CNN Indonesia: https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah.

CNN Indonesia. (2023a, 19 Januari). *BSSN: Hampir 1 Miliar Serangan Siber Hantam RI di 2022.* Tersedia dalam CNN Indonesia: https://www.cnnindonesia.com/teknologi/20230119144028-192-902537/bssn-hampir-1-miliar-serangan-siber-hantam-ri-di-2022.

CNN Indonesia. (2023b, 10 Agustus). *Prabowo Sebut Wacana Pembentukan Angkatan Siber TNI Ide Bagus.* Tersedia dalam CNN Indonesia: https://www.cnnindonesia.com/nasional/20230810192836-20-984575/prabowo-sebut-wacana-pembentukan-angkatan-siber-tni-ide-bagus

CNN Indonesia. (2023c, 10 Agustus). Komisi 1 DPR Sambut Usulan Angkatan Siber Lengkapi TNI AD, AL, dan AU. Tersedia dalam CNN Indonesia: https://www.cnnindonesia.com/nasional/20230810123057-32-984303/komisi-i-dpr-sambut-usulan-angkatan-siber-lengkapi-tni-ad-al-dan-au

CNN Indonesia. (2024a, 24 Juni). *210 Instansi Pusat dan Daerah Kena Dampak Peretasan PDN.* Tersedia dalam CNN Indonesia: https://www.cnnindonesia.com/teknologi/20240624152147-192-1113476/210-instansi-pusat-dan-daerah-kena-dampak-peretasan-pdn

CNN Indonesia. (2024b, 19 September). Bjorka kembali beraksi, bocorkan data NPWN Jokowi hingga Sri Mulyani. Tersedia dalam CNN Indonesia: https://www.cnnindonesia.com/teknologi/20240919093355-192-1145913/bjorka-kembali-beraksi-bocorkan-data-npwp-jokowi-hingga-sri-mulyani

Creswell, J. W., & Creswell, J. D. (2023). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (*6th ed*.). Thousand Oaks: Sage Publications.

Datta, P., & Acton, T. (2022). Ransomware and Costa Rica's national emergency: A defense framework and teaching case. *Journal of Information Technology Teaching Cases. 14*(4), 1-12. DOI: 10.1177/20438869221149042

Dzulfikarm, L. T., & Ramadhani, N. F. (2022, 21 September). *Panel ahli: UU Perlindungan Data Pribadi rentan makan korban dan belum jamin proteksi data yang kuat.* Tersedia dalam The Conversation: https://theconversation.com/panel-ahli-uu-perlindungan-data-pribadi-rentan-makan-korban-dan-belum-jamin-proteksi-data-yang-kuat-191018

Federal Bureau of Invetigation. (2018*). The Morris Worm: 30 Years Since First Major Attack on the Internet*. Tersedia dalam FBI News: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

Fischerkeller, M. P. (2021, 22 April). *Current International Law Is Not an Adequate Regime for Cyberspace*. Tersedia dalam Lawfare Media: https://www.lawfaremedia.org/article/current-international-law-not-adequate-regime-cyberspace

Floyd, R. (2021). Securitisation and the function of functional actors. *Critical Studies on Security. 9*(2), 81-97. DOI: 10.1080/21624887.2020.1827590.

Geelen, M. (2016). Cyber Securitization and Security Policy: The Impact of the Discursive Construction of Computer Security on (National) Security Policymaking in the Netherlands. *Thesis.* Leiden: Leiden University Department Crisis and Security Management.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. DOI: 10.1111/j.1468-2478.2009.00572.x

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*. *5*(1), 1-17. DOI: 10.33701/jk.v5i1.3208.

International Telecommunication Union. (2021). *Global Cybersecurity Index 2020: Measuring commitment to cybersecurity*. Geneva: ITU Publications.

International Telecommunication Union. (2024). *Global Cybersecurity Index 2024: 5Th Edition*. Geneva: ITU Publications.

Kemp, S. (2024a, 31 Januari). *Digital 2024: Global Overview Report.* Tersedia dalam Datareportal: https://datareportal.com/reports/digital-2024-global-overview-report

Kemp, S. (2024b, 21 Februari). *Digital 2024: Indonesia*. Tersedia dalam Data Reportal: https://datareportal.com/reports/digital-2024-indonesia

Klingova, K. (2013). Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia. *Thesis*. Vienna: Central European University Department of Political Science.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports. 7*(6), 8176-8186. DOI: 10.1016/j.egyr.2021.08.126.

Mansbach, R., & Pirro, E. (2023). *Introduction to Global Politics (4th Ed.).* New York: Routledge.

McGrew, A. (2023). Globalization and Global Politics. Dalam J. Baylis, S. Smith, P. Owens, *The Globalization of World Politics: An Introduction to International Relations* (*9th Ed.*, hal. 19-38). Oxford: Oxford University Press.

National Cyber Security Index. (2024). *Indonesia Cyber Security Index*. Tersedia dalam NCSI: https://ncsi.ega.ee/country/id_2022/

Nugraha, A. (2020). Penanggulangan Terorisme Siber melalui Media Sosial di Indonesia. *Disertasi*. Bandung: Pascasarjana Universitas Padjadjaran.

Nugroho, N. V. (2024, 26 Juni). *BSSN Dorong Penyusunan RUU Keamanan dan Ketahanan Siber*. Diambil kembari dari Tempo Nasional: https://nasional.tempo.co/read/1884272/bssn-dorong-penyusunan-ruu-keamanan-dan-ketahanan-siber

Peraturan Presiden (Perpres) Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara, Pemerintah Indonesia (2024). Tersedia dalam JDIH Database Peraturan: https://peraturan.bpk.go.id/Details/165493/perpres-no-28-tahun-2021

Peraturan Presiden (Perpres) Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, Pemerintah Indonesia (2023). Tersedia dalam JDIH Database Peraturan: https://peraturan.bpk.go.id/Details/255542/perpres-no-47-tahun-2023

Peraturan Presiden (Perpres) Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara, Pemerintah Indonesia (2017). Tersedia dalam JDIH Database Peraturan: https://peraturan.bpk.go.id/Details/72920/perpres-no-53-tahun-2017

Peraturan Presiden (Perpres) Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, Pemerintah Indonesia (2022). Tersedia dalam JDIH Database Peraturan: https://peraturan.bpk.go.id/Details/211029/perpres-no-82-tahun-2022

Pradnyana, I. P. H. (2023). The Path of Securitization: Transformation of Free Papua Movement (OPM) Terminology from Armed Criminal Groups to Separatist and Terrorist Groups. *Journal of Terrorism Studies. 5*(1), 1-18. DOI: 10.7454/jts.v5i1.1062

Priyandita, G. (2024). Indonesia's Cybersecurity Woes: Reflections for the Next Government. *CSIS Commentaries CSISCOM00624*. Tersedia dalam Centre for Strategic and International Studies Publication: https://csis.or.id/publication/indonesias-cybersecurity-woes-reflections-for-the-next-government/

Rachmawati, C. (2019). Tantangan dan Ancaman Keamanan Siber Indonesia di Era Revolusi Industri 4.0. *PROSIDING: Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO AAU). 1*(1), 299-306. Tersedia dalam SENASTINDO AAU: https://aau.e-journal.id/senastindo/issue/view/2

Ramadhan, I. (2023). The Securitization of Energy Issues from The Perspective of Security Studies. *Indonesian Journal of Energy. 6*(1), 1-12. DOI: 10.33116/ije.v6i1.139

Reveron, D. & Savage, J. (2023). *Security in the Cyber Age: An Introduction to Policy and Technology*. Cambridge: Cambridge University Press.

Reveron, D. (2012). An Introduction to National Security and Cyberspace. Dalam D. S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (hal. 3-20). Washington, DC.: Georgetown University Press.

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law*, 3, 7–34. DOI: 10.1365/s43439-021-00045-4

Schiliro, F. (2022). *Towards a Contemporary Definition of Cybersecurity.* Tersedia dalam Cornell University Cryptography and Security ArXiv. DOI: 10.48550/arXiv.2302.02274

Sinambela, N. M. (2023, 7 Agustus). *Indonesia alami 1,2 miliar serangan siber anomali setiap tahun.* Tersedia dalam ANTARA Megapolitan: https://megapolitan.antaranews.com/berita/254352/indonesia-alami-12-miliar-serangan-siber-anomali-setiap-tahun

Sulistyo. (2020). Diplomasi Siber Indonesia dalam Menghadapi Potensi Konflik Siber. *Disertasi*. Bandung: Pascasarjana Universitas Padjadjaran.

Sutra, S. M., & Haryanto, A. (2024). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Global Political Studies Journal. 7*(1), 56-69. DOI: 10.34010/gpsjournal.v7i1

Swara, E. B. (2014). Youtube sebagai new media pengaruhnya terhadap masyarakat Indonesia menurut pemikiran Jean Baudrillard. *Skripsi*. Depok: Universitas Indonesia.

Ulum, M. (2017). Cyber Culture and Cyber Security Policy of Indonesia: Combining Cyber Security Civic Discourse, Tenets and Copenhagen's Securitization Theory Analysis. *Proceeding: The 1st International Conference on Social Sciences. 1*(1), 39-50. Jakarta: Universitas Muhammadiyah Jakarta

Ulya, F. & Farisa, F. (2024, 29 Juni). Data Kementerian Harus Masuk PDN tapi Tak Ada "Back Up", Komisi I DPR: Konyol Luar Biasa. Diambil kembali dari Kompas Nasional: https://nasional.kompas.com/read/2024/06/29/13021901/data-kementerian-harus-masuk-pdn-tapi-tak-ada-back-up-komisi-i-dpr-konyol.

Undang-undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pemerintah Indonesia (2008). Tersedia dalam JDIH Database Peraturan: https://peraturan.bpk.go.id/Details/37589/uu-no-11-tahun-2008

Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Pemerintah Indonesia (2016). Tersedia dalam JDIH Database Peraturan: https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016

Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pemerintah Indonesia (2022). Tersedia dalam JDIH Database Peraturan: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

United Nations. (2024). *Draft United Nations convention against cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes, A/AC.291/L.15.* Tersedia dalam United Nations Office on Drugs and Crime: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_reconvened_concluding_session/main

United Nations. (T.Thn.). *UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security*. Tersedia dalam UN Office of Disarmament Affairs: https://disarmament.unoda.org/group-of-governmental-experts/

Wulan, N. T. (2021). Kebijakan Cyber Security United Kingdom National Health Service (NHS) Pasca The Ransomware Wannacry Attack Tahun 2017. *Skripsi*. Banyumas: Universitas Jenderal Soedirman.