Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, *307-320*
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Strategi Penanganan Keamanan Siber Di Indonesia

Fahrul Bagus Santoso [1], Riski Pujianto [1], Tedi Ramadhan [1,*]

[1] Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Raya Perjuangan No. 81 Marga Mulya, Bekasi Utara Jawa Barat, 17143, (021) 88955882, 202210715066@mhs.ubharajaya.ac.id, 202210715088@mhs.ubharajaya.ac.id, 202210715084@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202210715084@mhs.ubharajaya.ac.id

Diterima: 9 Jan 25; Review: 9 Jan 25; Disetujui: 14 Jan 25; Diterbitkan: 14 Jan 25

Abstract

This study continues previous research focused on cybersecurity issues in Indonesia. Its objective is to analyze cybersecurity challenges within the framework of strategies implemented by the Indonesian government. The evolution of cyber threats in the country is examined from the perspective of cybersecurity and national defense, which formed the basis of earlier research, and further expanded to explore relevant mitigation strategies.To provide a comprehensive understanding, this study adopts a three-perspective model that maps cyberspace into various logical layers. The research begins by highlighting the condition of Indonesian netizen and the challenges they face, then links these findings to the state's perspective in the context of defense, as well as the connections with the public sector, private sector, and international community.
Keywords: *Cybersecurity, National Defense Strategy, Three-Perspective Model.*

Abstrak

Penelitian ini melanjutkan studi sebelumnya yang berfokus pada isu keamanan siber di Indonesia. Penelitian ini bertujuan untuk menganalisis permasalahan keamanan siber dalam kerangka strategi yang telah diterapkan oleh pemerintah Indonesia. Perkembangan ancaman siber di negara ini ditinjau dari sudut pandang keamanan siber dan pertahanan nasional, yang menjadi dasar penelitian sebelumnya, kemudian diperluas untuk membahas strategi mitigasi yang relevan.Untuk menggambarkan kondisi secara komprehensif, penelitian ini mengadopsi model tiga perspektif yang memetakan ruang siber ke dalam berbagai lapisan logis. Penelitian ini dimulai dengan menyoroti kondisi netizen di Indonesia dan tantangan yang mereka hadapi, kemudian menghubungkannya dengan pandangan negara dalam konteks pertahanan, serta keterkaitan dengan sektor publik, sektor swasta, dan komunitas internasional.
Kata kunci: Keamanan Siber, Strategi Pertahanan Negara, Model Tiga Perspektif.

1. Pendahuluan

Keamanan siber dalam konteks pertahanan negara merupakan aspek yang tak terhindarkan di era modern ini. Era digital telah menjadi bagian penting dalam kehidupan bernegara dan aktivitas sehari-hari. Perubahan perilaku masyarakat, seperti meningkatnya mobilitas dan pola komunikasi, mencerminkan transformasi menuju identitas manusia milenial (Abraham & Harrington, 2015).

Perubahan ini memiliki dampak pada perilaku negara atau pemerintah. Negara merespons dengan berbagai cara, seperti menetapkan regulasi baru terkait dunia siber hingga membentuk badan khusus untuk menangani isu ini. Respons ini merupakan bentuk adaptasi,

meskipun tingkat kesiapan setiap negara berbeda-beda. Negara berkembang dan miskin sering kali memprioritaskan isu ekonomi dan stabilitas politik dibandingkan ancaman dunia siber. (Möckel et al., 2015) mengidentifikasi beberapa tantangan yang dihadapi negara berkembang:

1. Kesiapan dan kemampuan dalam merespons dunia maya, termasuk aspek hukum.
2. Pengetahuan dan kesadaran masyarakat tentang dunia maya.
3. Regulasi domestik dan regional, seperti yang diterapkan di Uni Eropa.
4. Kemandirian dalam hal infrastruktur teknologi.
5. Hubungan antara negara dan sektor swasta, termasuk dalam edukasi.

Isu dunia siber termasuk fenomena baru di era milenium. Konsensus antara sektor publik dan swasta menjadi langkah awal untuk mengatasinya, diikuti dengan membangun jejaring komunikasi untuk mengidentifikasi ancaman, mengembangkan sumber daya manusia, serta menggunakan pendekatan komprehensif yang melibatkan berbagai pemangku kepentingan (Mahendra & Pinatih, 2023)

Penelitian ini melanjutkan studi sebelumnya yang memetakan ancaman siber di Indonesia. Temuan sebelumnya menunjukkan bahwa pemerintah Indonesia telah sadar akan pentingnya keamanan siber, terbukti dengan pembentukan BSSN pada 2017. Namun, ada tantangan dalam implementasinya, seperti kurangnya satelit mandiri dan minimnya edukasi kepada masyarakat.Dalam menghadapi tantangan dunia siber, pemerintah perlu fokus pada dua hal utama:

1. Mengurangi dampak ancaman siber terhadap keamanan negara melalui pelatihan khusus dan pengembangan sistem pertahanan siber.
2. Memanfaatkan dunia siber dalam konteks yang lebih luas, termasuk melibatkan sektor swasta.

Selain negara, masyarakat juga rentan terhadap ancaman siber. Data Hootsuite menunjukkan bahwa pada 2019, Indonesia memiliki 150 juta pengguna internet dan 355,5 juta pelanggan mobile, jauh melebihi jumlah penduduknya yang 268 juta. Meskipun internet membawa manfaat, dampak negatif juga perlu diantisipasi, termasuk di tingkat individu. Artikel ini bertujuan untuk menggambarkan kesiapan Indonesia dalam menghadapi isu keamanan siber, termasuk strategi, hambatan, dan tantangannya

2. Metode Penelitian

Bagian ini menjadi inti dari penelitian, di mana peneliti menguraikan secara rinci proses pelaksanaan penelitian, meliputi desain penelitian, teknik pengumpulan data, analisis data, serta alat dan instrumen yang digunakan.

2.1. Desain Penelitian

Desain penelitian berfungsi sebagai kerangka utama yang digunakan dalam penelitian ini. Pendekatan yang diadopsi adalah pendekatan campuran, menggabungkan metode kualitatif dan kuantitatif. Pendekatan kualitatif digunakan untuk memahami perspektif subjektif dan

melakukan analisis kebijakan, sedangkan pendekatan kuantitatif bertujuan untuk mengolah data statistik dan hasil survei.

Penelitian ini bersifat eksploratif dan deskriptif, yang dirancang untuk memberikan pemahaman mendalam terkait isu keamanan siber di Indonesia beserta strategi penanganannya. Kombinasi antara pendekatan kualitatif dan kuantitatif memungkinkan analisis yang lebih menyeluruh.

Sumber data yang digunakan meliputi data sekunder, seperti laporan keamanan siber, dokumen kebijakan, serta data primer yang diperoleh melalui survei dan wawancara. Data sekunder dikumpulkan dengan menganalisis dokumen resmi, sementara data primer dikumpulkan melalui wawancara dan survei. Instrumen untuk wawancara dan survei dikembangkan berdasarkan kerangka teori dan tujuan penelitian.

2.2. Populasi dan Sampel

Populasi penelitian mencakup berbagai pemangku kepentingan, seperti perwakilan pemerintah, ahli keamanan siber, pengguna internet, serta perwakilan sektor publik dan swasta yang relevan dengan keamanan siber di Indonesia. Sampel penelitian dipilih berdasarkan karakteristik setiap kelompok pemangku kepentingan menggunakan teknik purposive sampling untuk wawancara dan survei.

2.3. Prosedur Penelitian

Populasi penelitian terdiri atas kelompok-kelompok berikut:

1. Instansi pemerintah.
2. Perusahaan swasta.
3. Pengguna internet di Indonesia.
4. Pakar keamanan siber.

3. Hasil dan Pembahasan

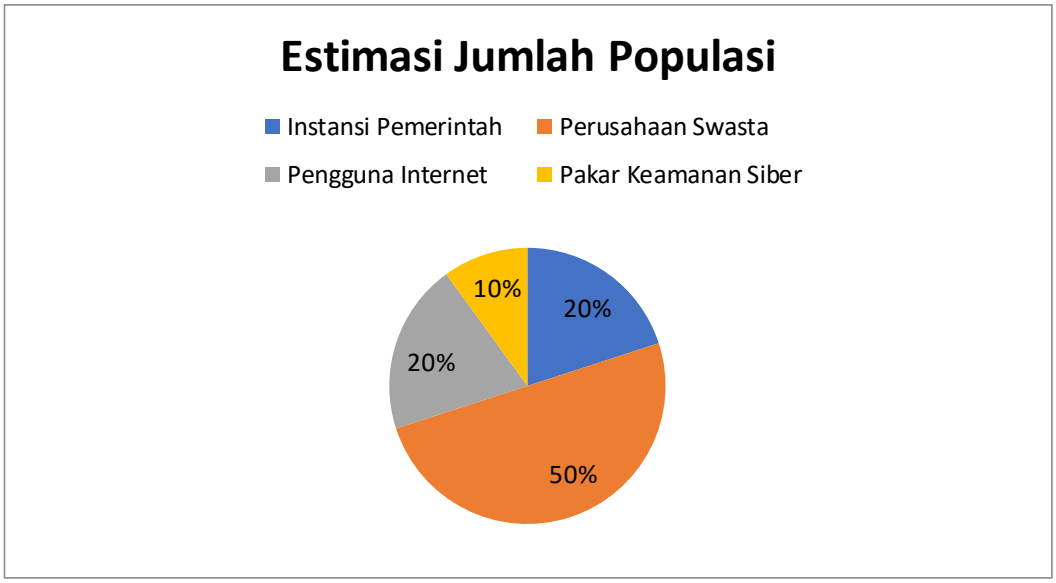
Pada bagian ini, dijelaskan hasil penelitian dan pada saat yang sama diberikan pembahasan yang komprehensif. Hasil dapat disajikan dalam angka, grafik, tabel dan lain-lain yang membuat pembaca memahami dengan mudah. Pembahasan dapat dibuat dalam beberapa sub-bab.

Tabel 1. Estimasi Jumlah Populasi

Kelompok Populasi	Estimasi jumlah populasi	Persentase%
instansi Pemerintah	1000	20%
Perusahaan Swasta	2.500	50%
Pengguna Internet	1000	20%
Pakar Keamanan Siber	500	10%
Total	5000	100%

Sumber: Hasil Penelitian (2024)

Tabel 1 menjelaskan tentang estimasi jumlah populasi.



Sumber: Hasil Penelitian (2024)

Gambar 1. Gambar Diagram Estimasi Jumlah Populasi

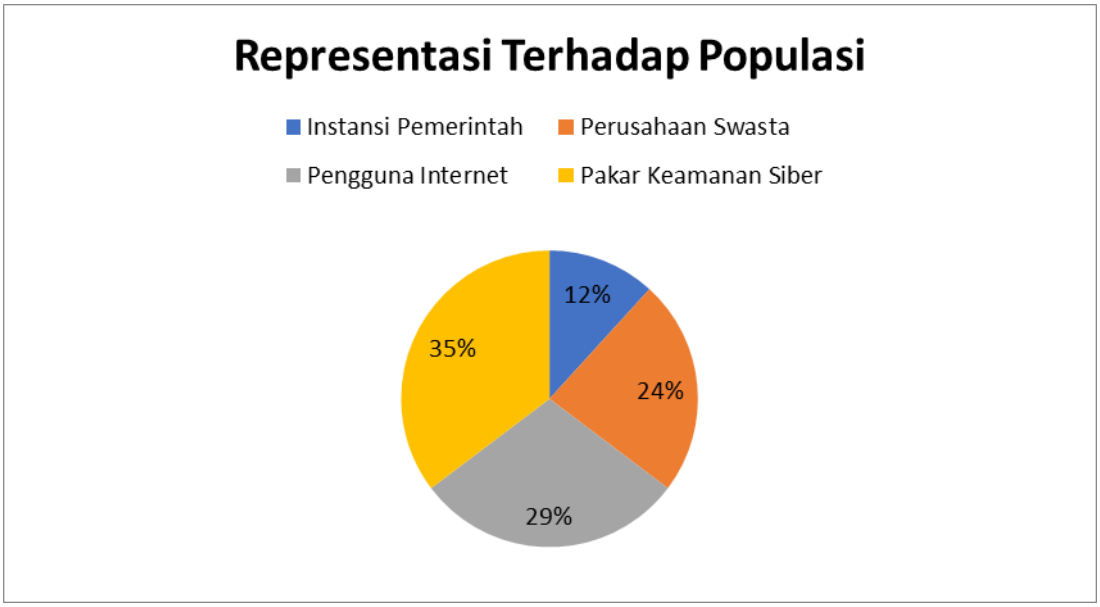
Pada Gambar 1 menunjukkan diagram estimasi jumlah populasi.

Tabel 2. Representasi Terhadap Populasi

Kelompok Sampel	Jumlah Sampel	Persentase (%) Dari Sampel	Representasi (%) Terhadap Populasi
Instansi Pemerintah	20	10%	12%
Perusahaan Swasta	100	50%	14%
Pengguna Internet	50	25%	15%
Pakar Keamanan Siber	30	15%	16%
Total	200	100%	

Sumber: Hasil Penelitian (2024)

Tabel 2 menjelaskan tentang representasi terhadap populasi.



Sumber: Hasil Penelitian (2024)

Gambar 2. Gambar Diagram Representasi Terhadap Populasi

Pada Gambar 2 menunjukkan diagram representasi terhadap populasi.

3.2. Pembahasan

3.2.1. Populasi:

- Estimasi jumlah populasi dihitung berdasarkan asumsi kontribusi masing-masing kelompok terhadap keamanan siber secara nasional.
- Persentase populasi menggambarkan distribusi mereka dalam penelitian.

3.2.2. Sampel:

- Teknik purposive sampling dipilih untuk memastikan representasi signifikan dari masing-masing kelompok.
- Persentase sampel dihitung berdasarkan relevansi kelompok terhadap fokus penelitian.

Apakah Anda memerlukan penyesuaian atau tambahan data? Sebagai contoh, sampel bisa berupa: Berikut adalah beberapa sumber data terkait populasi pengguna internet di Indonesia:

1. APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) mencatat bahwa pada tahun 2023, jumlah pengguna internet di Indonesia mencapai 215,63 juta orang, dengan tingkat penetrasi sebesar 78,19% dari total populasi 275,77 juta jiwa. Angka ini menunjukkan pertumbuhan dibandingkan tahun sebelumnya, terutama didorong oleh peningkatan kebutuhan internet selama pandemi dan tren kerja jarak jauh yang masih berlanjut.(Andrean W. Finaka, n.d.)
2. Tingkat penetrasi internet di Indonesia pada tahun 2024 diproyeksikan meningkat menjadi 79,5% berdasarkan survei terbaru APJII, dengan dominasi pengguna dari

kalangan milenial. Informasi ini digunakan untuk mendukung pemerintah dalam pengembangan infrastruktur dan kebijakan komunikasi.

3.2.3. Objek Penelitian

Objek penelitian merujuk pada aspek atau elemen spesifik yang menjadi fokus dalam penelitian. Dalam penelitian tentang "Strategi Penanganan Keamanan Siber di Indonesia," objek penelitian dapat mencakup:

- Strategi dan Kebijakan Keamanan Siber: Bagaimana kebijakan keamanan siber dirancang, diimplementasikan, dan dievaluasi di berbagai sektor (pemerintah, swasta, publik).
- Teknologi dan Proses Keamanan: Analisis teknologi yang digunakan untuk mendeteksi dan mencegah serangan siber, serta proses keamanan yang diterapkan di berbagai institusi.
- Kesadaran dan Sikap Pengguna: Pemahaman, sikap, dan perilaku pengguna internet di Indonesia dalam menghadapi ancaman siber.
- Tantangan dan Ancaman dalam Keamanan Siber: Jenis-jenis ancaman siber yang umum di Indonesia, seperti malware, phishing, serangan DDoS, dan lainnya.

3.2.4. Perkembangan Analisis Keamanan Siber

Analisis terkait keamanan dalam studi Hubungan Internasional telah berkembang menjadi topik yang menarik perhatian (Mahendra & Pinatih, 2023) menjelaskan bahwa selama Perang Dingin, kajian keamanan hanya terfokus pada aspek politik dan militer. Namun, seiring berjalannya waktu, ruang lingkup studi keamanan meluas untuk mencakup isu-isu yang berkaitan dengan lingkungan, ekonomi, dan sosial.. Dalam era digital saat ini, sektor keamanan juga mengalami perubahan signifikan. Joseph S. Nye, dalam bukunya "The Future of Power," menyatakan bahwa dimensi kehidupan negara-bangsa, termasuk tatanan sosial di dunia maya, telah menjadi prioritas strategis.

Keamanan siber, seperti yang diungkapkan oleh Barry Buzan, tidak memiliki definisi tunggal karena ketidakpastian dalam definisi 'keamanan' (Kremer & Müller, 2014) memandang keamanan siber sebagai kumpulan kebijakan, alat, instrumen, dan manajemen risiko untuk mencegah ancaman dari dunia maya. Sementara itu, Madeline Carr menganggap keamanan siber sebagai permasalahan pasca-negara, di mana ancaman digital bersifat lintas batas dan tak terlihat, namun memiliki dampak signifikan yang tidak dapat diatasi dengan paradigma Westphalia yang mengandalkan instrumen negara, seperti militer.

Dalam konteks hubungan antarnegara, Nir Kshetri dalam tulisannya "Cyber Security and International Relations: The US Engagement with China and Russia" menyatakan bahwa keamanan negara tidak hanya terbatas pada darat, laut, udara, dan militer, tetapi juga mencakup dunia maya. Hubungan bilateral antarnegara saat ini sangat dipengaruhi oleh aktivitas yang dilakukan aktor-aktor di ranah maya, seperti cyber espionage, pencurian data, dan upaya melumpuhkan sistem informasi negara oleh negara lain untuk mendapatkan keuntungan politik atau ekonomi.

Tipologi ancaman terhadap keamanan siber dipandang oleh beberapa ahli secara beragam. (Mahendra & Pinatih, 2023) menjelaskan ancaman tersebut ke dalam tiga kategori: cybercrime, cyber war, dan cyber terrorism. Kejahatan siber adalah aktifitas kejahatan yang menggunakan teknologi informasi untuk mencapai kepentingan ekonomi yang dilakukan oleh organisasi kriminal. Cyber war dapat dipandang sebagai bentuk digital dari perang menurut teori Von Clausewitz, sementara cyber terrorism merujuk pada tindakan peretasan atau pelumpuhan sistem informasi negara oleh kelompok teroris. thurk mengemukakan tiga jenis ancaman dalam dunia maya, yaitu pengumpulan intelijen, peretasan, dan cyber war. Thurk menggambarkan ancaman ini sebagai bentuk spionase digital, peretasan sistem informasi, dan potensi negara untuk mengacaukan sistem pertahanan negara lain (Thurk, 2009)

Ancaman terhadap keamanan siber ini dapat mempengaruhi siapa saja, termasuk negara-negara di Asia Tenggara. Sebagai respons, ASEAN telah mengembangkan ASEAN ICT Masterplan 2012 untuk melindungi sistem informasi dalam menghadapi Masyarakat Ekonomi ASEAN 2015. Inisiatif ini melibatkan pertukaran pengetahuan antarnegara anggota ASEAN guna saling mendukung dalam menjaga keamanan jaringan informasi. Meskipun demikian, tantangan di bidang keamanan siber tetap besar, memberikan dampak yang signifikan terhadap pertumbuhan ekonomi digital di kawasan ini.

Menurut Lembaga E-Trade for All pada tahun 2018, proyeksi untuk tahun 2025 menunjukkan bahwa ekonomi digital dapat berkembang hingga 102 miliar dolar AS, sementara ancaman serangan siber bisa mengganggu sistem informasi dan menghambat perekonomian digital di Asia Tenggara. Walaupun Singapura, yang merupakan pusat teknologi informasi di Asia Tenggara, menjadi sasaran serangan siber, negara ini juga menghadapi masalah kebocoran data kartu kredit pada tahun 2018. Kejadian serupa juga dialami oleh Vietnam dan Malaysia. Laporan Asia Pacific Risk Centre menyatakan bahwa kerugian akibat ancaman siber dapat mencapai 2,1 triliun dolar AS pada tahun 2019. Permasalahan utama terkait ketidakmerataan kemampuan teknologi informasi antar negara di Asia Tenggara, yang menciptakan kerentanannya dalam menghadapi ancaman siber. Meski Singapura menjadi pusat teknologi, ketidakseimbangan ini menjadi beban bagi negara-negara yang kurang berkembang seperti Laos atau Myanmar yang berisiko menghadapi serangan siber. Ancaman siber di kawasan ini memiliki sifat holistik, yang berarti dapat mempengaruhi seluruh negara ASEAN.. Oleh karena itu, penting bagi negara-negara di Asia Tenggara untuk mengembangkan kemampuan teknologi mereka dan membangun kerja sama lintas negara. Dalam menghadapi dilema ini, pendekatan mahzab neorealisme, terutama konsep defensive realism, menekankan kepentingan setiap negara untuk bertahan dalam tatanan politik global. Sebagai alternatif, neo-liberal institusionalisme menekankan pada kerja sama antar negara melalui institusi internasional untuk mengatasi ancaman bersama. Robert Keohane menyoroti pentingnya koordinasi dan kerja sama antar negara sebagai langkah krusial untuk mengatasi risiko ancaman (Adolph, 2016).

3.2.5. Implementasi Strategi Keamanan Siber di Indonesia

Perkembangan keamanan siber di Indonesia dimulai pada akhir 1990-an dengan peningkatan akses internet bagi masyarakat. Namun, Indonesia terlambat dalam menetapkan hukum keamanan siber dibandingkan tetangga seperti Malaysia dan Singapura. Pada tahun 1997, Malaysia sudah memiliki undang-undang seperti Computer Crime Act dan Multimedia Act (Nugraha & Putri, 2016) Ancaman keamanan siber di Indonesia meningkat pesat pada abad ke-21, tercatat sebagai negara kedua tertinggi dalam tindakan online fraud pada 2002. Beberapa kasus serius, seperti defacing situs KPU pada Pemilu 2004, mencerminkan kurangnya perhatian pemerintah terhadap keamanan siber. Saat ini, Indonesia mendesak penanganan keamanan siber karena tingkat kejahatan di dunia maya mencapai tahap memprihatinkan, seperti terungkap dalam data CIA yang Menurut (Ardiyanti, 1986), kerugian yang diakibatkan oleh kejahatan siber (cybercrime) diperkirakan mencapai sekitar 1,20% dari tingkat global.Penangganan keamanan siber memerlukan pemikiran komprehensif dalam tataran kebijakan, membedakannya dari penanganan kejahatan konvensional.

Dalam konteks keamanan siber, awal mula hukum Indonesia yang bergerak di bidang keamanan teknologi dan informasi (IT) bisa dilacak dengan diberlakukannya UU Telekomunikasi No.36/1999 dan UU Informasi dan Transaksi Elektronik (ITE) No.11/2008. Kedua UU ini dihitung sebagai bentuk kebijakan dari pemerintah Indonesia mengenai keamanan jalur komunikasi teknologi pada umumnya di Indonesia. Ditandatangani oleh Presiden RI Bacharuddin Jusuf Habibie dan Menteri Sekretaris Negara Muladi, UU Telekomunikasi merupakan salah satu contoh pertama dari dibentuknya sebuah kebijakan khusus tentang kegiatan telekomunikasi di Indonesia (Supartinah, 1989) UU ini membahas semua bentuk komunikasi yang menggunakan teknologi komunikasi pada masanya seperti televisi, radio, telepon, dan lain sebagainya.

Di Indonesia, selain UU Telekomunikasi, UU ITE No.11/2008 menjadi rujukan penting dalam mengamankan jaringan teknologi dan informasi. UU ITE mengakui peran internet sebagai sarana komunikasi dan secara eksplisit membahas informasi elektronik, transaksi elektronik, dan dokumen elektronik. Namun, kritik muncul terkait ketidakcukupan kedua UU tersebut dalam menegakkan keamanan siber. UU Telekomunikasi tidak mencakup jaringan internet sebagai media komunikasi, sulitnya mengatasi kasus hukum berbasis internet. UU ITE, meskipun signifikan, masih memerlukan dukungan beberapa UU lain seperti UU Perlindungan Konsumen, UU Hak Cipta, dan UU Pornografi untuk efektif beroperasi. Kelemahan cakupan definisi dan hukuman terhadap cybercrime di Indonesia menjadi sorotan. Di tengah kurangnya cakupan beberapa UU di Indonesia tentang keamanan siber secara spesifik, pemerintah Indonesia telah melakukan beberapa tindakan untuk menegakkan keamanan siber sejak era 2000-an. Pada tahun 2007, Kementerian Komunikasi dan Informasi (Kemkominfo) memberlakukan Peraturan Menteri Komunikasi dan Informasi No.26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Internet yang

membahas mengenai pembentukan lembaga keamanan yang relevan untuk keamanan siber yaitu Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII).

Pendirian ID-SIRTII merupakan langkah awal yang diinisiasi oleh beberapa stakeholder penting di Indonesia, termasuk Kejaksaan Agung Republik Indonesia (KEJAGUNG), Kepolisian Republik Indonesia (POLRI), Asosiasi Penyedia Jasa Internet Indonesia (APJII), Asosiasi Warung Internet Indonesia (AWARI), dan Masyarakat Telematika Indonesia (MASTI). Ini mencerminkan kesadaran akan pentingnya lembaga khusus untuk menangani isu keamanan siber di Indonesia. Tugas dan fungsi ID-SIRTII mencakup pemantauan, pendeteksian dini, peringatan terhadap ancaman jaringan, serta kerja sama dengan pihak dalam dan luar negeri. Secara umum, kerangka hukum keamanan siber di Indonesia dibangun berdasarkan UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah No. 82 Tahun 2012, dan regulasi menteri. Namun, terdapat permasalahan nasional terkait keamanan siber, seperti lemahnya pemahaman pemangku kepentingan terhadap security di dunia siber, kebutuhan legalitas yang memadai dalam menangani serangan cyber, tata kelola kelembagaan yang parsial, serta kelemahan industri dalam mengembangkan perangkat keras terkait teknologi informasi.

Perkembangan keamanan siber di Indonesia pada akhir 1990-an dan dekade 2000-an fokus pada pengembangan UU yang diperlukan untuk mengatasi tantangan keamanan jenis ini. Kesadaran pemerintah Indonesia terhadap keamanan baru muncul pada era 2000-an, dan resmi diwujudkan dalam bentuk UU yang membahas gambaran umum keamanan siber. Namun, langkah-langkah konkret untuk menegakkan keamanan tersebut masih perlu dijabarkan. Memasuki era 2010-an, implementasi penegakan keamanan siber terus dilakukan oleh lembaga pemerintah. Dengan meningkatnya kasus cybercrime, baik di tingkat global maupun di Indonesia, pemerintah telah mencoba merespons masalah ini. Data dari Symantec (2016) mencatat kerugian akibat tindakan cybercrime di Indonesia mencapai sekitar Rp 194.6 miliar pada tahun 2016, memantik urgensi dalam menanggapi ancaman keamanan siber.

Dalam upaya pemerintah Indonesia untuk membangun awareness tentang penegakan keamanan siber, pendidikan tentang keamanan siber secara spesifik juga belum dilaksanakan di Indonesia dengan mencukupi. Meskipun beberapa universitas ternama di Indonesia seperti Universitas Indonesia, Universitas Gunadarma, dan Sekolah Tinggi Sandi Nasional (STSN) menyediakan pendidikan tentang keamanan siber sampai tingkatan tertentu (terutama bagi STSN), tidak banyak sekolah tinggi yang menyediakan pendidikan tentang keamanan siber yang mumpuni dan merata di berbagai daerah di Indonesia. Walaupun begitu, perkembangan sebuah lembaga khusus di bidang keamanan siber di Indonesia pun terus dilanjutkan yang berujung dengan dibentuknya Badan Siber dan Sandi Negara (BSSN) pada tahun 2017.

Peningkatan tindakan cybercrime di Indonesia dapat berupa infeksi malware dan ransomware yang melanda berbagai situs web. Jumlah serangan malware/ransomware meningkat drastis dari 28.430.843 kasus pada 2015 menjadi 135.672.984 kasus pada 2016 (Mahendra & Pinatih, 2023). Selain itu, tindakan phishing dan online fraud juga menjadi

ancaman nyata yang sering kali dilakukan melalui e- mail untuk memperoleh data sensitif. Sebelum tahun 2017, pemerintah Indonesia masih dalam tahap pengembangan lembaga negara khusus untuk menegakkan implementasi keamanan siber, dengan ID- SIRTII berperan sebagai Computer Emergency Response Team (CERT) nasional pada masa itu (Mahendra & Pinatih, 2023). ID-SIRTII tidak hanya menangani permasalahan keamanan siber internal pemerintahan, tetapi juga menjalin kerja sama dengan sektor swasta di Indonesia dalam upaya mengatasi tantangan keamanan siber.

BSSN, dibentuk berdasarkan Peraturan Presiden No.53/2017, merupakan lembaga pemerintah non-kementerian yang langsung berada di bawah presiden. Sebagai penerus Lembaga Sandi Negara (LSN), BSSN memiliki tanggung jawab terhadap keamanan sandi Indonesia dan berfungsi untuk melaksanakan kebijakan teknis dalam identifikasi, deteksi, proteksi, penanggulangan, dan pemantauan keamanan siber di Indonesia, seiring dengan peran hampir serupa yang dimiliki oleh ID-SIRTII (Islami, 2018).

menghambat proses alih teknologi yang diperlukan untuk menegakkan keamanan siber secara efektif. Pada tahun 2015, hanya terdapat sekitar 500 orang tenaga profesional keamanan siber di Indonesia yang telah disertifikasi oleh ISO270001, CEH, CISA, dan sertifikasi lainnya (Nugraha & Putri, 2016).Pada tahun 2016, Indonesia juga membutuhkan lebih dari 1000 tenaga ahli keamanan siber di luar technical officers yang harus ditempatkan di berbagai tempat industry (Suhartadi, 2016). Kurangnya data mengenai jumlah tenaga ahli baru yang dilatih dalam beberapa tahun terakhir membuat penilaian terhadap kecukupan atau kekurangan SDM keamanan siber menjadi sulit. Tantangan lainnya dalam pengembangan kebijakan keamanan siber adalah sifat ancaman cyber yang multidimensional, memerlukan keterlibatan lebih dari TNI, Polri, Kemhan, dan Kemenkominfo. Strategi yang dapat diambil sebagai contoh adalah pendekatan yang dilakukan oleh pemerintah Amerika Serikat dengan mengembangkan The National Cyber Security Division (NCSD), divisi khusus yang bekerja sama dengan sektor swasta dan masyarakat untuk membangun dan menjaga sistem keamanan siber nasional, serta mengimplementasikan program manajemen risiko untuk melindungi infrastruktur telekomunikasi dan siber melalui National Cyber space Response System.

Untuk membangun keamanan siber di Indonesia ke depan, perlu dipenuhi empat pondasi utama yang mendukung perkembangan teknologi informasi. Ini melibatkan pengembangan perangkat lunak (software) seperti sistem dan aplikasi, perkembangan alat keras (hardware), sarana dan prasarana teknologi informasi, manajemen isi (content management), telekomunikasi dan jaringan, serta perkembangan internet dan perdagangan online. Selain itu, menurut (Ardiyanti, 1986) dalam tulisannya ‘Cyber Security dan Tantangan Pengembangannya di Indonesia’, langkah penting lainnya adalah pengorganisasian terkait dengan penggunaan sistem teknologi informasi, dengan mempertimbangkan aspek sistem informasi, kompetisi organisasi, pengambilan keputusan organisasi, dan penggunaan sistem informasi dalam organisasi. Oleh karena itu, penataan keamanan siber ke depan harus

dibangun atas lima bidang dasar, mencakup kepastian hukum dalam undang-undang cybercrime, tindakan teknis dan prosedural untuk pengguna akhir, bisnis, penyedia layanan, dan perusahaan perangkat lunak. Selain itu, struktur organisasi yang berkembang dengan menghindari tumpang tindih, capacity building dan pendidikan pengguna melalui kampanye publik dan komunikasi terbuka mengenai ancaman terbaru dari cybercrime, serta kerjasama internasional, termasuk kerjasama timbal balik untuk mengatasi ancaman siber (Ardiyanti, 1986). Hambatan Pelaksanaan Keamanan Siber di Indonesia

Pilar keempat dalam kerangka keamanan siber adalah kerjasama internasional. Di Indonesia, Computer Emergency Response Team (IDCERT) mendapat perhatian sebagai tim CERT pertama yang berdiri pada tahun 1998. Ini merupakan tim koordinasi teknis berbasis komunitas yang independen dan berfungsi untuk mengkoordinasikan penanganan insiden melibatkan pihak Indonesia dan luar negeri. Namun, kendalanya terletak pada karakter sukarela (volunteer) dari ID-CERT yang bersifat sementara. Selain itu, Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) didirikan sebagai upaya untuk memperkuat keamanan pada institusi-institusi penting. Meskipun ada upaya dalam menyatukan sektor swasta, pemerintah, masyarakat, dan lembaga internasional dalam mencegah dan menangani kejahatan siber, kolaborasi dengan pemangku kepentingan seperti aplikasi atau perangkat lunak, contohnya Twitter atau Facebook, yang digunakan sebagai media kejahatan, memerlukan koordinasi lintas negara. Pilar kelima, yaitu tindakan teknis dan prosedural, dihadapkan pada tantangan seperti perkembangan teknologi Machine-to-Machine (M2M), Internet of Things (IoT), dan Cloud Computing yang diikuti dengan semakin kompleksnya serangan siber dan malware. Hambatan kedua terletak pada hasil penilaian indeks KAMI pada tahun 2012, di mana hanya 3% dari 41 organisasi pemerintah yang memenuhi standar, sementara sisanya masih berfokus pada area teknologi tanpa memperhatikan aspek lainnya (Aptika dan IKP et al., 2017).

Keamanan siber merupakan suatu ekosistem yang melibatkan aspek legal, organisasi, keterampilan, kerjasama, dan implementasi teknik secara bersinergi untuk mencapai hasil yang efektif. Tantangan dalam implementasi strategi nasional keamanan siber melibatkan sumber daya manusia, prosedur, dan kebijakan pencegahan serta keamanan yang memerlukan koordinasi di seluruh pemangku kebijakan, baik dari sektor swasta, pemerintah, masyarakat, maupun institusi luar negeri yang merupakan pengembang aplikasi yang seringkali digunakan sebagai media kejahatan siber. Selain itu, teknologi juga harus terus dikembangkan seiring dengan meningkatnya jenis serangan siber. Hambatan pelaksanaan keamanan siber di Indonesia, berdasarkan pilar-pilar Global Cybersecurity Index (2017), terlihat pada yang pertama pilar capacity building, di mana sosialisasi keamanan informasi, promosi SKKNI bidang Keamanan Informasi dan Auditor TI masih terbatas. Proses pembaharuan unit kompetensi dalam SKKNI memerlukan waktu yang lama, sementara perkembangan teknologi informasi dan jenis ancaman siber terus berlangsung pesat. Edukasi publik, khususnya dalam hal sosialisasi konten berkualitas, keamanan siber, pemahaman kebhinekaan, dan anti terorisme, belum

diterapkan secara sistematis, terutama pada usia dini, padahal pengguna internet di Indonesia usia 9 hingga 15 tahun cukup tinggi, mencapai 27.5%.

Pilar kedua dalam konteks keamanan siber, yaitu legal, menghadapi beberapa hambatan. Jumlah kebijakan dan regulasi untuk keamanan siber belum sepenuhnya mampu mengakomodasi berbagai bentuk ancaman siber, sementara kecepatan perkembangan Teknologi Informasi dan Komunikasi (TIK) terus meningkat seiring dengan peningkatan kejahatan siber. Urgensi pengesahan RUU Perlindungan Data dan Informasi Pribadi menjadi krusial untuk memberikan kepastian hukum terkait perlindungan data pribadi. Pilar ketiga, yakni struktur organisasi, juga mengalami hambatan seperti ketidakjelasan tenggat waktu peralihan penggabungan fungsi Direktorat Keamanan Informasi dan Lembaga Sandi Negara menjadi Badan Siber dan Sandi Negara (BSSN) sebagai organisasi baru. Diperlukan urgensi dalam membangun ekosistem ranah siber Indonesia yang tahan dan aman, serta inisiasi peta jalan dan pedoman penanganan keamanan siber. Seperti di negara-negara maju seperti Inggris, masyarakat membutuhkan pusat keamanan siber nasional (National Cyber Security Centre) sebagai rujukan utama yang mapan dan jelas untuk menanggapi tantangan di bidang keamanan siber.

4. Kesimpulan

Indonesia masih menghadapi berbagai tantangan dalam merumuskan strategi yang komprehensif untuk menangani isu keamanan siber. Walaupun Badan Siber dan Sandi Negara (BSSN) telah didirikan sebagai lembaga yang bertanggung jawab dalam mengelola masalah di dunia maya, efektivitas dari upaya tersebut masih dianggap belum maksimal. Salah satu hambatan utama adalah ketidakadaan kerangka hukum yang secara jelas mengatur aspek keamanan siber, sehingga respons Indonesia terhadap ancaman di dunia maya belum sepenuhnya terkoordinasi. Rancangan Undang-Undang (RUU) Keamanan dan Ketahanan Siber, yang diharapkan dapat menjadi dasar hukum yang kuat dalam menghadapi isu ini, hingga kini masih belum berhasil disahkan. Alhasil, Indonesia masih mengandalkan peraturan yang ada, seperti UU Informasi dan Transaksi Elektronik (UU ITE), yang dianggap belum cukup untuk mengatasi ancaman siber yang semakin berkembang.

Selain itu, edukasi masyarakat terkait keamanan siber juga menjadi faktor penting yang perlu mendapatkan perhatian lebih. Dengan jumlah pengguna internet yang terus meningkat setiap tahun, di mana Indonesia termasuk dalam lima besar negara dengan jumlah pengguna internet terbesar di dunia, yakni sekitar 175 juta pengguna atau 64% dari total populasi, kesadaran masyarakat terhadap ancaman siber masih sangat rendah. Walaupun sebagian pengguna internet mungkin telah mengenal istilah seperti hacking atau jacking, ancaman siber sebenarnya jauh lebih kompleks dan beragam daripada itu. Oleh karena itu, edukasi yang lebih luas dan mendalam sangat diperlukan untuk meningkatkan pemahaman masyarakat tentang kejahatan siber dan cara-cara pencegahannya.

Peran pemerintah sangat penting dalam menutup celah ini, baik melalui regulasi yang lebih kuat maupun dengan meningkatkan kesadaran masyarakat terhadap ancaman-ancaman siber. Tanpa kerangka hukum yang jelas dan edukasi yang masif, upaya menangani keamanan siber di Indonesia akan terus tertinggal, terutama mengingat meningkatnya skala ancaman global dan kebutuhan untuk melindungi infrastruktur penting negara dari serangan siber, Beberapa masalah terbaru yang dihadapi Indonesia dalam keamanan siber meliputi:

- Serangan ransomware dan pencurian data pribadi yang semakin marak, terutama di sektor publik dan layanan kesehatan.
- Kurangnya tenaga ahli di bidang keamanan siber yang berpengalaman, yang menghambat implementasi strategi keamanan siber yang efektif.
- Rendahnya kesadaran siber di sektor bisnis dan individu, terutama dalam menerapkan praktik-praktik keamanan siber dasar seperti penggunaan kata sandi yang kuat, pengamanan data, dan pembaruan perangkat lunak.

Ancaman terhadap infrastruktur penting seperti perbankan, transportasi, dan energi, yang menjadi target utama para pelaku serangan siber di tingkat global.

Daftar Pustaka

Abraham, R., & Harrington, C. (2015). Consumption Patterns of the Millenial Generational Cohort. *Modern Economy*, *06*(01), 51–64. https://doi.org/10.4236/me.2015.61005

Adolph, R. (2016). *済無No Title No Title No Title*.

Andrean W. Finaka. (n.d.). *Orang Indonesia Makin Melek Internet*. https://indonesiabaik.id/infografis/orang-indonesia-makin-melek-internet

Aptika dan IKP, P., Litbang SDM, B., & Jl Medan Merdeka Barat No, K. (2017). TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX Maulia Jayantina Islami TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX Challenges in The Implementation of National Cybersecurity Strategy of Indonesia from The Global Cybersecurity Index Point of View Maulia Jayantina Islami. *Jurnal Masyarakat Telematika Dan Informasi*, *8*(2), 137–144.

Ardiyanti, H. (1986). *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*. 95–110.

Islami, M. J. (2018). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *8*(2), 137. https://doi.org/10.17933/mti.v8i2.108

Kremer, J. F., & Müller, B. (2014). Cyberspace and international relations: Theory, prospects and challenges. In *Cyberspace and International Relations: Theory, Prospects and Challenges* (Vol. 9783642374814, Issue February). https://doi.org/10.1007/978-3-642-

37481-4

Mahendra, Y. C., & Pinatih, N. K. D. S. A. (2023). Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia. *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, *6*(4), 1941–1949. http://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/20659

Möckel, M., Searle, J., Hamm, C., Slagman, A., Blankenberg, S., Huber, K., Katus, H., Liebetrau, C., Müller, C., Muller, R., Peitsmeyer, P., Von Recum, J., Tajsic, M., Vollert, J. O., & Giannitsis, E. (2015). Early discharge using single cardiac troponin and copeptin testing in patients with suspected acute coronary syndrome (ACS): A randomized, controlled clinical process study. *European Heart Journal*, *36*(6), 369–376. https://doi.org/10.1093/eurheartj/ehu178

Nugraha, L. K., & Putri, D. A. (2016). Mapping the Cyber Policy Landscape: Indonesia. *No. November*, *November*.

Suhartadi, I. (2016). *indonesia kekurangan bakat cyber security*. Berita Satu.

Supartinah. (1989). No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析Title. *NBER Working Paper Series*, *58*(58), 99–104. https://www.unhcr.org/publications/manuals/4d9352319/unhcr-protection-training-manual-european-border-entry-officials-2-legal.html?query=excom 1989

Thurk, J. (2009). *International Intellectual Property Rights : A Quantitative Assessment*. 1–32.