Jurnal Review Pendidikan dan Pengajaran
http://journal.universitaspahlawan.ac.id/index.php/jrpp
Volume 6 Nomor 4, 2023
P-2655-710X e-ISSN 2655-6022

Submitted : 27/10/2023
Reviewed : 08/11/2023
Accepted : 18/11/2023
Published : 22/11/2023

Yustika Citra Mahendra[1]
Ni Komang Desy Setiawati Arya Pinatih[2]

STRATEGI PENANGANAN KEAMANAN SIBER (CYBER SECURITY) DI INDONESIA

Abstrak
Penelitian ini merupakan kelanjutan dari penelitian sebelumnya yang mengeksplorasi isu keamanan siber di Indonesia. Penelitian ini berfokus untuk mengangkat isu tentang cyber security dalam konteks strategi yang dimiliki oleh pemerintah Indonesia. Perkembangan cyber threats di Indonesia dilihat dari sudut pandang cyber security dan pertahanan negara menjadi dasar pada penelitian terdahulu yang kemudian ditindaklanjuti dengan penelitian kali ini yang mengulas strategi penanganannya. Untuk menggambarkan kondisi tersebut penulis menggunakan three perspective model yang memaparkan kondisi cyber space dalam logika lapisan-lapisan. Penulis memulai dengan menjelaskan kondisi netizen di Indonesia dan permasalahannya yang akhirnya kemudian dipersepsikan oleh negara dalam konteks pertahanan negara yang memiliki irisan dengan sektor publik, sektor privat dan konteks internasional.
Kata Kunci: Cyber Security, Strategi Pertahanan Negara, Three Perspective Model

Abstract
This research is a continuation of previous research which explored cyber security issues in Indonesia. This research focuses on raising the issue of cyber security in the context of the strategy of the Indonesian government. The development of cyber threats in Indonesia seen from the perspective of cyber security and national defense was the basis for previous research which was then followed up with this research which reviews strategies for handling them. To describe these conditions the author uses a three perspective model which describes the condition of cyber space in logical layers. The author begins by explaining the condition of netizens in Indonesia and the problems which are ultimately perceived by the state in the context of national defense which has intersections with the public sector, private sector and international context.
Keywords: Cyber Security, National Defense Strategy, Three Perspective Model

PENDAHULUAN

Cyber security atau keamanan siber dalam konteks pertahanan negara menjadi salah satu hal yang tidak dapat terelakan di era modern seperti saat ini. Dimana era digital telah menjadi bagian yang tidak terpisahkan dalam kehidupan bernegara dan keseharian. Mudahnya mobilitas manusia beserta pola komunikasinya menjadi contoh sederhana perubahan perilaku warga negara menuju manusia dengan identitas baru, manusia milenial (Abraham et al., 2015) & (Blain, 2008).

Perubahan perilaku masyarakat tersebut tentu mempengaruhi perilaku negara atau pemerintah. Dalam hal ini negara akan merespon dalam bentuk yang beragam mulai dari munculnya regulasi baru terkait dunia siber hingga dibentuknya badan khusus yang menanganinya yang kesemuanya itu merupakan bentuk adaptasi negara. Sayangnya kemampuan adaptasi setiap negara perihal dunia siber ini berbeda-beda, bahkan bagi negara berkembang dan miskin, dunia cybercrime bukan menjadi isu penting dibanding isu lainnya seperti ekonomi (kesejahteraan) dan stabilitas politik serta keamanan.

Muller (2015: 1-4) dalam ulasannya terdapat beberapa tantangan yang dihadapi oleh negara berkembang. Pertama, kemampuan atau kesiapan negara dalam merespon dunia maya termasuk legal formalnya. Kedua, terkait pengetahuan dan kesadaran akan dunia maya yang dimiliki oleh masyarakatnya. Ketiga, kepemilikan undang-undang baik di level domestik hingga kawasan (studi kasus di Uni Eropa). Keempat, keterjangkauan yakni sejauh mana negara berkembang dapat mandiri

[1,2]Hubungan Internasional, Fakultas Ilmu sosial dan Ilmu Politik, Universitas Brawijaya
email: masmahe@ub.ac.id

kedepannya. Kelima, tantangan pola hubungan yang dimiliki oleh negara dan sektor privat termasuk edukasinya. Kondisi ini tentu tidak mengherankan jika kita menilik bahwa isu dunia siber dan ancamannya tergolong isu yang baru jika kita mengacu pada era milenium baru. Konsensus antara semua sektor baik privat maupun publik merupakan langkah awal dalam mengatasinya. Kemudian konsensus tersebut ditindaklanjuti dengan pembuatan jejaring komunikasi yang dapat mengklasifikasikan ancaman, pembangunan SDM yang berkelanjutan, pembangunan jejaring informasi, serta dengan pendekatan komperhensif yang melibatkan stakeholder baik dalam maupun luar negeri (Henry & Brantly, 2018: 47-56)

Dikarenakan penelitian ini merupakan penelitian lanjutan dari penelitian sebelumnya yang telah mengulas isu ancaman siber (cyber threats) melalui pemetaannya di Indonesia, terdapat beberapa poin temuan di penelitian terdahulu kami diantaranya adalah pemetaan bentuk ancaman siber di Indonesia yang menunjukkan bahwa Indonesia saat ini (khususnya pemerintah) dapat dikatakan aware terkait isu keamanan siber, hal ini dapat dilihat dari keseriusan pemerintah Indonesia melalui pembentukan lembaga khusus yang menangani isu siber yakni BSSN di tahun 2017. Hanya saja dalam implementasinya di Indonesia masih terdapat kendala baik infrastruktur, yaitu tidak dimilikinya satelit mandiri, dan suprastruktur, terkait edukasi kepada Masyarakat.

Jika menyangkut keamanan suatu negara, diperlukan strategi negara dalam menyikapi tantangan yang timbul dari dunia siber. Setidaknya terdapat dua fokus utama yang dapat dilakukan oleh pemerintah, yaitu membatasi konsekuensi yang timbul akibat ancaman siber terhadap keamanan negara dan menggunakannya dalam konteks yang lebih luas (Kramer, 2014). Pada fokus yang pertama. dilihat bagaimana negara mendesain, meletakkan dan mengoperasikan kapabilitasnya dalam mengantisipasi keamanan siber dengan cara memberikan pelatihan secara spesifik untuk melawan serangan siber, atau bahkan dapat membuat sistem pertahanan yang khusus di masa mendatang, yang kemudian konteks tersebut dapat diluaskan cakupannya khususnya yang terkait sektor privat.

Di sisi lain, isu keamanan siber tidak hanya menyasar negara tetapi juga masyarakat atau individu. Individu atau sektor privat memiliki kerentanan yang lebih dibandingkan negara sehingga tetap diperlukan sinergitas antara pemerintah dan masyarakat. Merujuk pada data yang dikeluarkan oleh hootsuite, Indonesia tercatat tahun 2019 memiliki pengguna internet sebanyak 150 juta bahkan pengguna mobile subscriptions tercatat 355, 5 juta yang itu melebihi dari total penduduk 268 juta. Kondisi ini sekilas menggambarkan bagaimana masyarakat Indonesia hampir sebagian besar saat ini telah terpapar oleh internet. Selain efek positif yang didapat oleh pengguna internet, tentu efek negatif perlu diantisipasi oleh semua pengguna internet, tak terkecuali individu.

Berangkat dari paparan di atas, kiranya perlu melihat bagaimana negara Indonesia memiliki cara spesifik dalam merespon keamanan siber. Maka dari itu, artikel ini memiliki tujuan untuk menggambarkan kesiapan Indonesia dalam isu keamanan siber beserta strategi, hambatan, & tantangan yang dihadapi.

METODE

Bagian ini merupakan bagian kunci dari penelitian, di mana peneliti akan menjelaskan secara detail bagaimana penelitian akan dilakukan, termasuk desain penelitian, teknik pengumpulan data, analisis data, serta alat dan instrumen yang digunakan.

Desain Penelitian

Desain penelitian adalah kerangka dasar yang akan digunakan dalam penelitian Anda. Penelitian ini akan mengadopsi pendekatan campuran yang menggabungkan metode kualitatif dan kuantitatif. Pendekatan kualitatif akan digunakan untuk memahami pandangan subjektif dan analisis kebijakan, sementara pendekatan kuantitatif akan digunakan untuk menganalisis data statistik dan survei.

Jenis penelitian ini adalah penelitian eksploratif dan deskriptif, yang akan membantu dalam pemahaman mendalam tentang isu keamanan siber di Indonesia dan strategi penanganannya. Pendekatan penelitian ini dilakukan secara kombinasi antara pendekatan kualitatif dan kuantitatif akan memungkinkan analisis yang lebih komprehensif.

Adapun, sumber data berasal dari data sekunder, seperti laporan keamanan siber, dokumen kebijakan, serta hasil survei dan wawancara. Melalui sumber data tersebut, peneliti menggunakan teknik pengumpulan data pada data sekunder melalui pencarian dan analisis dokumen resmi, sedangkan data primer akan dikumpulkan melalui wawancara dan survei. Instrumen penelitian untuk wawancara dan survei akan dikembangkan berdasarkan kerangka teoretis dan tujuan penelitian.

Populasi dan Sampel

Populasi penelitian ini akan mencakup berbagai pemangku kepentingan, termasuk perwakilan pemerintah, ahli keamanan siber, netizen, serta perwakilan dari sektor publik dan privat yang terkait dengan keamanan siber di Indonesia. Sementara sampel penelitian akan dipilih dengan mempertimbangkan karakteristik masing-masing kelompok pemangku kepentingan. Pengambilan sampel akan menggunakan teknik purposive sampling untuk wawancara dan survei.

Prosedur Penelitian

Riset deskriptif dilakukan menggunakan data sekunder yang akan dianalisis untuk mendapatkan gambaran umum tentang keamanan siber di Indonesia, termasuk tren serangan, kerentanan, dan dampaknya. Analisis kebijakan dilakukan peneliti melalui studi dokumen kebijakan dan regulasi terkait dengan keamanan siber akan dianalisis untuk memahami strategi yang telah diadopsi oleh pemerintah. Wawancara dan survei dilakukan penelitu melalui pemangku kepentingan kunci untuk mendapatkan wawasan mendalam tentang pandangan mereka terhadap keamanan siber. Survei akan dilakukan untuk mengukur persepsi netizen terkait isu keamanan siber. Analisis Tiga Perspektif Model berposisi sebagai kerangka analisis yang ini akan digunakan untuk menggambarkan kondisi keamanan siber dari sudut pandang netizen, pemerintah, dan sektor publik serta privat. Perbandingan dengan Negara Lain digunakan dalam melengkapi tahapan riset ini, di mana akan dilakukan perbandingan strategi keamanan siber Indonesia dengan praktik terbaik di tingkat internasional untuk mengevaluasi keefektifan strategi yang ada.

HASIL DAN PEMBAHASAN

Dinamika Kajian Keamanan Siber

Studi keamanan dalam ilmu Hubungan Internasional menjadi subjek yang menarik. Barry Buzan (1989) mengungkapkan bahwa pada masa Perang Dingin, fokus studi keamanan hanya terbatas pada sektor politik dan militer. Namun, seiring perkembangan waktu, sektor keamanan melibatkan isu-isu lingkungan, ekonomi, dan sosial. Dalam era digital seperti sekarang, sektor keamanan juga terpengaruh, sebagaimana dijelaskan oleh Joseph S. Nye dalam bukunya, "The Future of Power," di mana dimensi kehidupan negara-bangsa, termasuk tatanan sosial dalam dunia maya, menjadi prioritas strategis. Begitu juga dengan keamanan siber, yang, sebagaimana Buzan menyatakan ketidakpastian dalam definisi 'keamanan', juga tidak memiliki definisi tunggal. Roxana Radu (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 post-state, di mana ancaman digital bersifat lintas batas dan tak terlihat, namun memiliki dampak yang signifikan yang tidak dapat diatasi dengan paradigma Westphalia yang mengandalkan instrumen negara, seperti militer.Lalu, bagaimanakah kedudukan keamanan siber dalam konteks relasi antar negara? Nir Kshetri dalam tulisannya yang berjudul Cyber Security and International Relations: The US Engagement with China and Russia mengatakan bahwa keamanan negara tidak hanya di darat, laut, udara dan militer, tetapi juga di dunia maya. Hubungan bilateral antar negara saat ini juga sangat terpengaruh oleh aktifitas yang dilakukan aktor-aktor tersebut di ranah maya. Salah satu contohnya adalah bentuk cyber espionage ataupun pencurian data serta 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. Myriam Dunn Cavelty (2014) menjelaskan ancaman tersebut ke dalam tiga tipologi yakni, cybercrime, cyber war dan cyber terrorism. Kejahatan siber adalah aktifitas kejahatan yang menggunakan teknologi informasi untuk mencapai kepentingan ekonomi yang dilakukan oleh organisasi kriminal. Sedangkan cyber war adalah bentuk perang Von Clausewitz versi digital. Adapun cyber terrorism adalah kegiatan peretasan ataupun pelumpuhan sistem informasi negara-bangsa yang dilakukan oleh kelompok terrorism. Sedangkan Jonathan D. Aronson memberikan tiga tipologi berbeda yaitu intelligence gathering, hacking dan cyber war. Aronson memaparkan tipologi tersebut sebagai ancaman yang melibatkan aksi spionase digital, peretasan sistem informasi dan kemampuan Negara bangsa untuk melumpuhkan sistem pertahanan negara oleh aktor negara lainnya (Aronson, 2005).

Ancaman keamanan siber yang telah diuraikan dapat menimpa pihak manapun, termasuk negara-negara di Asia Tenggara. ASEAN telah merespons hal ini dengan ASEAN ICT Masterplan 2012, yang bertujuan untuk mengamankan sistem informasi dalam menyongsong Masyarakat Ekonomi ASEAN 2015. Upaya ini melibatkan pertukaran pengetahuan antarnegara anggota ASEAN untuk saling mendukung dalam menjaga keamanan jaringan informasi mereka. Namun, tantangan

keamanan siber di kawasan ini masih besar, berdampak signifikan pada pertumbuhan ekonomi digital di ASEAN.

Menurut Lembaga E-Trade for All pada 2018, proyeksi tahun 2025 menunjukkan pertumbuhan ekonomi digital mencapai 102 miliar dolar AS, sementara serangan siber dapat mengakibatkan gangguan pada sistem informasi dan menghambat perekonomian digital di wilayah tersebut. Meskipun Singapura, sebagai pusat teknologi informasi di Asia Tenggara, menjadi target serangan siber, negara ini juga mengalami kebocoran data kartu kredit nasabah pada tahun 2018. Kejadian serupa juga terjadi di Vietnam dan Malaysia. Laporan Asia Pacific Risk Centre menyebutkan bahwa kerugian akibat ancaman siber dapat mencapai 2.1 triliun dolar AS pada tahun 2019.Permasalahan mendasar terletak pada ketidakmerataan kemampuan teknologi informasi di antara negara-negara Asia Tenggara, hal tersebut menciptakan kerentanan dalam keamanan siber. Meskipun Singapura menjadi pusat teknologi, ketidakseimbangan ini menjadi beban saat negara-negara yang kurang berkembang, seperti Laos atau Myanmar, menghadapi potensi serangan siber. Ancaman siber di wilayah ini bersifat holistik, yang memiliki arti mempengaruhi setiap negara di 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 (Cornelia, 2013).

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 (Leonardus et al., 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 mencatat kerugian akibat cybercrime mencapai 1,20% dari tingkat global (Handrini, 2014). 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 (DPR RI, 1999). 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 (Sumantri, 2017: 11). 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 (Mulyadi & Rahayu, 2018: 2). 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 (Maulia, 2017: 141). Lebih lanjut, lembaga pemerintah lainnya, seperti Polri, Kementerian Pertahanan (Kemhan), Badan Intelijen Negara (BIN), dan Tentara Nasional Indonesia, juga menunjukkan ketertarikan terhadap keamanan siber dengan masing-masing peran dan kebijakan di bidang tersebut. Namun, keluputan dalam interpretasi konsep keamanan di Indonesia yang masih bersifat negara dan bukan individu menyebabkan kurangnya strategi keamanan siber yang komprehensif. Perlindungan hak individu di ranah siber diakui sebagai krusial, namun kekurangan regulasi, terutama UU tentang keamanan siber, membuat penegakan keamanan ini menjadi sulit dilakukan.

Kondisi ini ditegaskan oleh pernyataan Deputi Direktur Riset ELSAM, Wahyudi Djafar, yang memandang perlindungan hak- hak individu di ranah cyberspace sangatlah penting dalam penegakan keamanan siber sebuah negara. Karena para pelaku cybercrime sama sekali tidak terikat dengan sebuah lokasi geografis, maka penanganan cyber threats membutuhkan perhatian ekstra (Alia, 2019). Dengan pelaku cybercrime yang tidak terikat oleh batasan geografis, penanganan cyber threat membutuhkan perhatian khusus. Meski prinsip ini diakui oleh pihak-pihak terkait di Indonesia, kekurangan UU khusus tentang keamanan siber menjadi kendala utama dalam upaya penegakan keamanan di era digital ini.

Pengembangan UU tentang keamanan siber di Indonesia menemui hambatan, terlihat dalam kegagalan kelanjutan RUU Keamanan dan Ketahanan Siber (KKS) pada tahun 2019 (Haryanti, 2019). Menurut Ketua Panitia Khusus RUU Keamanan dan Ketahanan Siber, Bambang Wuryanto, RUU tersebut tidak memenuhi mekanisme tata beracara pembuatan legislasi dan kesepakatan mengenai definisi cybercrime dan konten internet yang dianggap sebagai ancaman. Haryanti menambahkan ketidakhadiran beberapa menteri kunci dalam pembahasan RUU juga jelas menjadi sebuah halangan. Meskipun pemerintah telah berhasil membentuk lembaga seperti BSSN pada tahun 2017 yang dianggap sebagai langkah baru dalam penegakan keamanan siber di Indonesia, tantangan tetap muncul dari aspek legal dan sumber daya. Pembatalan RUU KKS pada tahun 2019 menjadi kendala serius dalam upaya pemerintah untuk memiliki dasar hukum yang komprehensif untuk penegakan keamanan siber di Indonesia.

Tantangan Keamanan Siber di Indonesia

Pengaturan dan penataan lembaga keamanan siber nasional yang kokoh menjadi prasyarat utama bagi keberhasilan keamanan siber yang handal. Penanganan keamanan siber harus terintegrasi secara kuat, melibatkan berbagai lembaga terkait seperti intelijen, penegak hukum, kementerian pertahanan, TNI, serta pemerintah sebagai regulator, diwakili oleh Kominfo, ISSIRTI, dan Lembaga Sandi Negara. Meskipun berbagai lembaga dan undang-undang relevan telah dibentuk untuk menangani keamanan siber di Indonesia, masih terdapat sejumlah tantangan yang menghambat pencapaian keamanan tersebut. Menurut ABC News, pada tahun 2013 Indonesia pernah secara konsisten menjadi sumber serangan siber terbanyak di dunia pada tahun 2013, dengan tindakan hacking yang merugikan berbagai situs web di berbagai lokasi. Meskipun pemerintah telah memprioritaskan isu keamanan siber, keberlanjutan tindakan cybercrime selama beberapa tahun terakhir disebabkan oleh belum adanya lembaga dan undang-undang keamanan siber yang memadai. Dalam menghadapi tingkat kejahatan siber yang mengkhawatirkan ini, salah satu alternatif kebijakan adalah memasukkan keamanan siber ke dalam konteks pertahanan, yang memerlukan pembangunan infrastruktur penunjang, seperti satelit khusus untuk pertahanan, termasuk penanggulangan keamanan siber, mengingat sejumlah penyedia telekomunikasi dimiliki oleh modal asing.

Kendala utama dalam penegakan keamanan siber di Indonesia selama beberapa tahun terakhir melibatkan beberapa faktor krusial. Pertama, tingkat literasi masyarakat Indonesia mengenai keamanan siber masih kurang memadai, sehingga pemahaman mengenai pentingnya keamanan siber bagi pengguna internet masih terbatas (Maulia, 2017). Meskipun Standar Kompetensi Kerja Nasional Indonesia (SKKNI) telah menetapkan Sektor Keamanan Informasi sebagai standar keamanan informasi dalam lingkungan kerja di Indonesia, sosialisasi mengenai hal ini masih minim. Kurangnya promosi yang intensif dan kesulitan dalam memperbarui unit kompetensi dalam SKKNI menghambat jalannya sosialisasi, terutama mengingat laju perkembangan teknologi yang sangat cepat. Kedua, minimnya kebijakan pemerintah yang bersifat spesifik mengenai keamanan informasi menjadi kendala, terutama karena UU ITE tidak menguraikan secara rinci berbagai jenis ancaman siber di era modern. UU No.19/2016 tentang Perubahan Atas UU ITE No.11/2008 hanya memberikan gambaran umum tentang penegakan keamanan siber di Indonesia tanpa memberikan langkah-langkah konkret yang dapat diambil oleh pemerintah. Pembatalan RUU KKS pada tahun 2019 semakin menguatkan ketidakcukupan basis hukum untuk menegakkan keamanan siber. Ketiga, kurangnya alokasi kebijakan dan sumber daya yang memadai oleh pemerintah untuk menegakkan keamanan siber di seluruh Indonesia menjadi masalah serius. Data dari Badan Pusat Statistik (BPS) pada tahun 2017 menunjukkan bahwa pembangunan infrastruktur digital di Indonesia belum merata, dan isu ini menjadi lebih penting karena sebagian besar pengguna internet berada di daerah urban kota-kota besar.

Selain sumber daya mentah, kekurangan sumber daya manusia (SDM) yang kompeten dan berpengalaman dalam keamanan siber menjadi tantangan serius di Indonesia. Hal ini disebabkan oleh dominasi tenaga profesional di bidang keamanan siber yang berasal dari negara-negara lain,

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 (Leonardus & Dinita, 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 (2014) 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, 2014).

Hambatan Pelaksanaan Keamanan Siber di Indonesia

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.

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) hadir sebagai inisiatif untuk meningkatkan sistem keamanan di lembaga-lembaga strategis. 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 (Global Security Index, 2017).

SIMPULAN

Indonesia masih memiliki banyak pekerjaan rumah dalam strategi penanganan keamanan siber. Meskipun saat ini Indonesia sudah memiliki Lembaga yang secara khusus menaungi permasalahan dunia siber melalui BSSN, hal tersebut masih dirasa belum cukup. Ketiadaan hukum yang secara khusus mengatur perihal keamanan siber menjadi salah satu persoalan mendasar bagaimana Indonesia merespon tantangan dunia siber masih jauh dari harapan. RUU tentang Keamanan dan Ketahanan Siber yang diharapkan menjadi payung hukum terkait dunia siber pun gagal diwujudkan. Alhasil hingga saat ini Indonesia hanya mengandalkan beberapa regulasi seperti UU ITE dalam merespon permasalahan siber dan itu tentu sangatlah kurang.

Disamping kondisi tersebut, faktor edukasi juga memiliki andil dalam penanganan keamanan siber di Indonesia. Tidak bisa dipungkiri pengguna dunia maya di Indonesia hampir setiap tahun mengalami peningkatan, bahkan termasuk 5 besar pengguna internet di dunia dengan catatan 175 juta pengguna internet atau sekitar 64% dari total penduduk. Dari data tersebut seberapa banyak yang aware dalam persoalan ancaman di dunia siber. Mungkin sebagian pengguna internet mengenal beberapa istilah ancaman di dunia siber seperti hacking, jacking, dsb tetapi sayangnya persoalan ancaman siber lebih luas dan bervariasi dari itu. Itulah kenapa diperlukan edukasi lebih mengenai kejahatan di dunia siber dan bagaimana penanggulangannya. Di sisi inilah kemudian peran pemerintah juga diperlukan guna menutupi kekurangan yang dimiliki untuk meningkatkan awareness di masyarakat sebagai pengguna internet.

DAFTAR PUSTAKA

Abraham, R and C. Harrington (2015). Consumption Patterns of the Millenial Generational Cohort. Mod. Econ

Aronso, D. Jonathan. (2005). Causes and consequences of the communication and Internet Revolution dalam John Baylis & Steve Smith (ed), The Globalization of World Politics: An Introduction to International Relations. London: Oxford University Press

Ariffin, Eijas. (2018). Strengthening ASEAN's cybersecurity. Available at https://theaseanpost.com/article/strengthening-aseans-cybersecurity

ABC News (2013). Indonesia overtakes China as top source of cyberattack traffic. Diperoleh dari https://www.abc.net.au/news/2013-10-18/an-indonesia-overtakes-china-as-top-source-of-cyber-attack-traf/5032428, diakses pada 16 Agustus 2020.

Blain, A (2008). The Millenial Tidalwave: Five Elements That Will Change The Workplace of Tomorrow. J. Qual. Assur. Inst

Buzan, Barry dkk. (1998). Security: A New Framework of Analysis. Colorado: Lynne Rienner

Badan Pusat Statistik (2017). Indeks Pembangunan Teknologi Informasi dan Komunikasi (IP-TIK) Indonesia Tahun 2016 Sebesar 4,34 Pada Skala 0-10. Diperoleh dari https://www.bps.go.id/pressrelease/2017/12/15/1310/indeks-pembangunan-teknologi- informasi-

dan-komunikasi--ip-tik--indonesia-tahun-2016-sebesar-4-34-pada-skala-0--- 10-.html, diakses pada 16 Agustus 2020.

Carr, Madeline. (2015). Crossed Wires: International Cooperation on Cyber Security dalam Interstate Journal of International Affairs, 2015/2016, Issue II

Cavelty, Myriam Dunn. (2014). Cyber Threats dalam Victor Mauer & Myriam Dunn Cavelty (ed), The Routledge Handbook of Security Studies. New York: Routledge

DPR RI (1999). Undang-undang Republik Indonesia Nomor 36 Tahun 1999 Tentang Telekomunikasi. Jakarta, Indonesia: DPR RI.

E-Trade for All. (2018). ASEAN: E-commerce set to dominate the region in 2019. Available at https://etradeforall.org/asean-e-commerce-set-to-dominate-the-region-in-2019/.

Henry, Shawn, and Brantly (2018). Countering the Cyber Threat. Cyber Def. Rev, vol. 3, No. 1 (SPRING), pp47-56

Handrini Ardiyanti: Cyber security dan Tantangan Pengembangannya di Indonesia, Politica Vol. 5 No. 1 Juni 2014.

ID-SIRTII (2018). Sejarah ID-SIRTII/CC. Diperoleh dari https://idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html, diakses pada 15 Agustus 2020.

Islami, Maulia J. (2017). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index. Jurnal Masyarakat Telematika dan Informasi, Vol. 8, No. 2 (Oktober-Desember 2017). Jakarta Pusat, Indonesia: Kemenkominfo, hal. 141.

Kramer, FD (2014). Cyber Security: An Integrated Governmental Strategy for Progress.

Kshetri, Nir. (2014). Cybersecurity and International Relations: The U.S. Engagement with China and Russia. Diambil dari Prosiding FLACSO-ISA 2014, University of Buenos Aires, School of Economics, Buenos Aires, Argentina

Kr-Asia. (2018). Singapore is the most vulnerable to cyberattacks in Southeast Asia: Report https://kr-asia.com/singapore-is-the-most-vulnerable-to-cyber-attacks-in- southeastasiareport.

Kementerian Pertahanan Republik Indonesia (2014). Pedoman Pertahanan Siber. Diperoleh dari https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82- Tahun-2014-tentang-Pertahanan-Siber.pdf, diakses pada 15 Agustus 2020.

Karunian, Alia Y. (2019). Mendiskusikan Kebijakan Keamanan Siber di Indonesia. Diperoleh dari https://elsam.or.id/mendiskusikan-kebijakan-keamanan-siber-di- indonesia/, diakses pada 16 Agustus 2020.

Muler, L (2015). Cyber Security Capacity Building in Developing Countries. No. 21, pp 1- 4

Mulyadi dan Rahayu, D. (2018). Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency (BSSN). CITSM 2018, hal. 2.

Nugraha, Leonardus K. dan Putri, Dinita A. (2016). Mapping the Cyber Policy Landscape: Indonesia. London, England: Global Partners Digital, hal. 17.

Navari, Cornelia. (2013). Liberalism dalam Paul Williams (ed), Security Studies: An Introduction (2nd Edition). New York: Routledge

Radu, Roxana. (2014). Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace dalam Jan Frederik Kremer & Benedikt Muller (ed), Cyberspace and International Relations: Theory, Prospect and Challenges. Bonn: Springer

Ramadhan, Iqbal. (2017). Peran Institusi Internasional dalam Penanggulangan Ancaman Cyber. Jurnal Populis Vol 2 (4) 2017. ISSN: 2640-4208

Symantec, N. (2016). Norton Cyber Security Insights Report Global Corporation. Symantec Corporation.

Sumantri, I. (2017). Tren Serangan Siber Nasional 2016 dan Prediksi 2017. Jakarta, Indonesia: ID-SIRTII – Kemenkominfo, hal. 11.

Sari, Haryanti P. (2019). RUU Keamanan dan Ketahanan Siber Dibatalkan, Ini Alasannya. Diperoleh dari https://nasional.kompas.com/read/2019/09/27/18241611/ruu-keamanan- dan-ketahanan-siber-dibatalkan-ini-alasannya, diakses pada 16 Agustus 2020.

Suhartadi, I. (2016). Indonesia Kekurangan Bakat Cyber Security. Diperoleh dari https://www.beritasatu.com/iptek/406490-indonesia-kekurangan-bakat-cyber- security.html, diakses pada 17 Agustus 2020.