Aliansi : Jurnal Hukum, Pendidikan dan Sosial Humaniora
Volume. 2, Nomor. 5 September 2025
e- ISSN: 3031-9706; p- ISSN: 3031-9684, Hal 122-141
DOI: https://doi.org/10.62383/aliansi.v2i5.1204
Available online at: https://journal.appihi.or.id/index.php/Aliansi

Penegakan Hukum Internasional terhadap Serangan Siber pada Infrastruktur Kritis Penting di Indonesia

Anny Susilowati
STMIK PPKIA Tarakanita Rahmawati, Tarakan, Indonesia

Alamat: Oval Ladang IV, Jl. Halmahera No.99, Kec. Tarakan Tengah, Kota Tarakan, Kalimantan Utara
Korespondensi penulis: anny.susilowati@gmail.com

Abstract. *Cyberattacks on critical infrastructure are one of the serious threats in the era of global digitalization because they can disrupt social, economic, and national security stability. Critical infrastructure such as the energy, banking, transportation, telecommunications, and public services sectors are particularly vulnerable to planned and systematic attacks. This research focuses on the application of international law in dealing with cyberattacks on critical infrastructure in Indonesia, with the formulation of issues including how to apply international law in these contexts, the obstacles faced by Indonesia, and efforts to overcome obstacles in international law enforcement. The research method used is a normative legal approach by examining international legal instruments, national laws and regulations, and literature related to cyberattacks. The results of the study indicate that the current international legal framework is not fully able to anticipate the complexity of cyberattacks, due to the lack of clarity of norms, non-uniform definitions of cyberattacks, and limitations of international sanctions mechanisms. In addition, the cyber sovereignty aspect is a major challenge because each country has different interests and regulations. Indonesia, although it has participated in international forums such as the Budapest Convention, does not yet have a national legal framework that is fully aligned with global standards. The ITE Act and national cybersecurity regulations are still ineffective in addressing cross-border threats. To overcome these challenges, domestic policy reform with the harmonization of international law is needed, increased bilateral and multilateral cooperation, and strengthening national capacity in terms of technology and human resources. This strategy must be accompanied by increasing public awareness and collaboration between the government, the private sector, and the community in strengthening cyber resilience. With these measures, it is hoped that law enforcement against cyber attacks on critical infrastructure can become more effective, responsive, and in line with the development of global threats.*

Keywords: *Cyber, Enforcement, Infrastructure, International, Law.*

Abstrak. Serangan siber terhadap infrastruktur kritis merupakan salah satu ancaman serius di era digitalisasi global karena dapat mengganggu stabilitas sosial, ekonomi, dan keamanan nasional. Infrastruktur kritis seperti sektor energi, perbankan, transportasi, telekomunikasi, dan layanan publik sangat rentan terhadap serangan yang terencana dan sistematis. Penelitian ini berfokus pada penerapan hukum internasional dalam menangani serangan siber terhadap infrastruktur kritis di Indonesia, dengan rumusan masalah meliputi bagaimana penerapan hukum internasional dalam konteks tersebut, kendala yang dihadapi Indonesia, serta upaya untuk mengatasi hambatan dalam penegakan hukum internasional. Metode penelitian yang digunakan adalah pendekatan hukum normatif dengan menelaah instrumen hukum internasional, peraturan perundang-undangan nasional, serta literatur terkait serangan siber. Hasil penelitian mengindikasikan bahwa kerangka hukum internasional saat ini belum sepenuhnya mampu mengantisipasi kompleksitas serangan siber, karena masih adanya ketidakjelasan norma, definisi serangan siber yang tidak seragam, serta keterbatasan mekanisme sanksi internasional. Selain itu, aspek kedaulatan siber menjadi tantangan utama karena setiap negara memiliki kepentingan dan regulasi berbeda. Indonesia, walaupun telah berpartisipasi dalam forum internasional seperti Konvensi Budapest, belum memiliki kerangka hukum nasional yang sepenuhnya selaras dengan standar global. Undang-Undang ITE dan regulasi keamanan siber nasional masih kurang efektif untuk menangani ancaman lintas batas. Untuk mengatasi tantangan tersebut, diperlukan pembaruan kebijakan domestik dengan harmonisasi hukum internasional, peningkatan kerja sama bilateral dan multilateral, serta penguatan kapasitas nasional dalam hal teknologi dan sumber daya manusia. Strategi ini harus diiringi dengan peningkatan kesadaran publik serta kolaborasi antara pemerintah, sektor swasta, dan masyarakat dalam memperkuat ketahanan siber. Dengan langkah-langkah ini, diharapkan penegakan hukum terhadap serangan siber terhadap infrastruktur kritis dapat menjadi lebih efektif, responsif, dan sesuai dengan perkembangan ancaman global.

Kata kunci: Hukum, Infrastruktur, Internasional, Penegakan, Siber.

Received: Juni 28, 2025; Revised: Juli 12, 2025; Accepted: Juli 26, 2025; Online Available: Juli 28, 2025

1. LATAR BELAKANG

Kemajuan teknologi dalam perekonomian nasional ditingkatkan untuk mencapai kesejahteraan rakyat demi mewujudkan kehidupan perekonomian yang lebih baik. Seiring dengan perkembangan era globalisasi dewasa ini, segala macam aktivitas masyarakat tidak terlepas dari bantuan teknologi. Begitu pula pada sektor keuangan yang kini mulai terintegrasi dengan *platform* sistem elektronik. Perkembangan teknologi dan internet membawa dampak besar bagi kehidupan manusia. Kemajuan teknologi adalah sesuatu yang tidak bisa kita hindari dalam kehidupan ini, karena kemajuan teknologi akan berjalan sesuai dengan kemajuan ilmu pengetahuan. Teknologi yang sebenarnya merupakan alat bantu/ekstensi kemampuan diri manusia. Dewasa ini, telah menjadi sebuah kekuatan yang justru membelenggu perilaku dan gaya hidup kita sendiri. Dengan daya pengaruhnya yang sangat besar, karena ditopang pula oleh sistem sosial yang kuat, dan dalam kecepatan yang makin tinggi, teknologi telah menjadi pengarah hidup manusia.

Masalah kejahatan siber adalah kejahatan dimana tindakan kriminal hanya dapat dilakukan dengan menggunakan teknologi siber dan terjadi di dunia siber. Masalah-masalah kejahatan siber selalu menjadi masalah yang menarik karena beberapa alasan, antara lain; karena permasalahan tersebut masih tergolong baru, berkaitan dengan teknologi yang hanya sebagian orang mampu melakukannya, terbatasnya jangkauan hukum untuk mengantisipasi dan lain sebagainya.

Kejahatan yang terjadi di dunia maya lahir akibat dampak negatif dari perkembangan teknologi, kejahatan yang terjadi dari berbagai bentuk dan jenisnya tersebut membawa konsekuensi terhadap perlindungan hukum penggunanya hal ini penting mengingat bahwa setiap manusia harus dilindungi sesuai dengan harkat dan martabatnya sebagai manusia. Salah satu bentuk wujud tanggung jawab negara atas perlindungan terhadap warga negaranya adalah dengan memberikan jaminan hukum dan tindakan nyata yang melindungi masyarakatnya dari segala bentuk kejahatan atau perbuatan-perbuatan menyimpang lainnya yang mungkin dialami oleh masyarakat baik di dunia nyata ataupun di dunia maya.

Indonesia adalah negara hukum seperti yang tertuang dalam konstitusi, sebagai sebuah negara hukum tentunya negara wajib melindungi setiap warga negaranya dari setiap perbuatan yang dapat merugikan apalagi perbuatan tersebut dapat merusak tatanan kehidupan berbangsa dan bernegara. Seperti halnya kejahatan yang terjadi di dunia maya atau biasa disebut dengan *cybercrime.* Kejahatan yang tidak mengenal ruang dan waktu ini mengalami perkembangan yang pesat akhir-akhir ini, kecanggihan teknologi yang disalahgunakan oleh oknum yang tidak bertanggung jawab demi keuntungan pribadi yang menyebabkan negara-negara berkembang

kesulitan untuk menindak pelaku kejahatan komputer khususnya pihak kepolisian, disamping dibutuhkan suatu perangkat aturan yang mengatur tentang penyalahgunaan informasi ini juga dibutuhkan sumber daya manusia dan sarana dan prasarana yang mendukung.

Serangan siber terhadap infrastruktur kritis menjadi tantangan besar dalam era digitalisasi global. Infrastruktur kritis seperti sistem energi, sistem komunikasi, serta fasilitas keuangan dan transportasi memiliki peran penting dalam menjaga kelangsungan kehidupan masyarakat modern. Di Indonesia, peran infrastruktur kritis semakin vital seiring dengan berkembangnya teknologi dan meningkatnya ketergantungan terhadap sistem informasi dan komunikasi yang terhubung secara global. Namun, serangan siber terhadap sektor ini menimbulkan dampak yang luas, tidak hanya bagi individu atau perusahaan yang menjadi korban, tetapi juga terhadap stabilitas negara. Dalam konteks ini, penting untuk mengkaji bagaimana penegakan hukum internasional dapat diterapkan untuk mengatasi serangan siber terhadap infrastruktur kritis di Indonesia. Penegakan hukum internasional terhadap serangan siber ini melibatkan pertimbangan hukum yang kompleks karena serangan siber bersifat transnasional dan seringkali sulit untuk ditentukan pelakunya, serta bagaimana negara bertindak dalam penanggulangannya.

Fenomena serangan siber terhadap infrastruktur kritis sudah menjadi ancaman nyata bagi banyak negara. Di Indonesia, kasus-kasus serangan siber terhadap infrastruktur kritis, baik yang dilakukan oleh individu, kelompok, ataupun negara lain, semakin meningkat. Meskipun negara telah melakukan berbagai langkah mitigasi dan memperbarui kebijakan siber, seperti pembentukan Badan Siber dan Sandi Negara (BSSN), belum ada solusi yang komprehensif dalam penegakan hukum internasional untuk mencegah atau menanggulangi serangan siber semacam ini. Serangan terhadap infrastruktur kritis di Indonesia menambah kerumitan masalah di tingkat internasional, karena serangan ini seringkali melibatkan aktor dari luar negeri, yang sulit untuk ditindak secara hukum sesuai dengan hukum domestik Indonesia. Isu ini menjadi semakin mendesak seiring dengan meningkatnya ketergantungan negara terhadap teknologi dan internet.

Seiring dengan kemajuan teknologi informasi, data mengenai serangan siber terhadap infrastruktur kritis semakin banyak tercatat. Laporan-laporan dari Badan Siber dan Sandi Negara (BSSN) dan lembaga-lembaga internasional lainnya menunjukkan bahwa serangan siber di Indonesia pada tahun-tahun terakhir mengalami peningkatan yang signifikan. Di antaranya, tercatat serangan terhadap sektor energi, layanan perbankan, dan sektor transportasi yang dapat mengancam keberlangsungan hidup masyarakat. Selain itu, banyak serangan yang sulit untuk dilacak pelakunya, baik di dalam negeri maupun di luar negeri.

Salah satu instrumen internasional utama yang mengatur kejahatan siber adalah Konvensi Budapešt (*Council of Europe Convention on Cybercrime*), yang diadopsi pada tahun 2001. Konvensi ini menjadi referensi pertama dalam hal penanggulangan kejahatan siber di tingkat internasional. Meskipun Indonesia bukan negara pihak dalam konvensi ini, prinsip-prinsip yang terkandung di dalamnya memberikan pedoman penting mengenai pengaturan aktivitas siber, termasuk serangan terhadap infrastruktur kritis. Konvensi ini berfokus pada pengaturan mengenai kejahatan komputer, perusakan data, dan akses ilegal ke sistem komputer. Konvensi Budapešt menekankan perlunya kerjasama internasional dalam penanggulangan serangan siber yang bersifat lintas batas.

Selanjutnya pada tingkat Perserikatan Bangsa-Bangsa (PBB), *United Nations Group of Governmental Experts* (UNGGE) telah menghasilkan serangkaian laporan yang mengatur penggunaan teknologi informasi dan komunikasi dalam konteks keamanan internasional. Laporan yang diterbitkan oleh kelompok ini pada tahun 2015 dan 2021, antara lain, menyebutkan bahwa serangan terhadap infrastruktur kritis dapat berisiko mengancam perdamaian dan keamanan internasional. Laporan ini mendorong negara-negara untuk memperkuat kerjasama internasional dalam menghadapi ancaman siber, serta mengembangkan kebijakan nasional yang dapat mencegah dan menanggulangi serangan terhadap infrastruktur kritis. UNGGE juga memberikan pedoman mengenai prinsip-prinsip yang mengatur penerapan hukum internasional dalam dunia maya, serta prinsip tidak adanya serangan terhadap infrastruktur kritis yang harus dipatuhi oleh negara-negara. Indonesia, sebagai anggota PBB, diharapkan dapat mematuhi pedoman ini dalam kebijakan nasionalnya mengenai keamanan siber.

Isu hukum yang muncul dalam penegakan hukum internasional terhadap serangan siber terhadap infrastruktur kritis di Indonesia bahwa di satu sisi, hukum internasional menuntut adanya perlindungan terhadap infrastruktur kritis dan pemberian sanksi terhadap pihak yang melakukan serangan. Namun, di sisi lain, terdapat banyak tantangan dalam penerapannya, termasuk definisi yang kabur mengenai serangan siber dan keterbatasan kewenangan penegakan hukum internasional di wilayah negara berdaulat. Hukum internasional juga menghadapi kesulitan dalam menyelesaikan perselisihan terkait serangan siber, mengingat adanya ketidaksepakatan antar negara mengenai norma, standar, dan kewajiban yang harus dipenuhi oleh negara-negara dalam melindungi infrastruktur kritis mereka.

Penelitian ini memiliki signifikansi yang sangat penting, terutama dalam memberikan kontribusi pemahaman tentang bagaimana hukum internasional dapat diterapkan untuk menanggulangi serangan siber terhadap infrastruktur kritis di Indonesia. Dengan fokus pada

tantangan hukum internasional yang dihadapi Indonesia, penelitian ini diharapkan dapat menawarkan solusi dan rekomendasi terkait peningkatan mekanisme penegakan hukum internasional dalam menghadapi serangan siber, yang memiliki dimensi lintas negara dan memerlukan kerjasama internasional. Penelitian ini sangat urgen mengingat meningkatnya ancaman serangan siber terhadap infrastruktur kritis, yang tidak hanya merugikan sektor swasta tetapi juga dapat mengancam keselamatan nasional dan keamanan negara. Urgensi ini semakin nyata dengan semakin terhubungnya infrastruktur kritis Indonesia ke dalam jaringan global. Selain itu, urgensi ini diperburuk dengan keterbatasan hukum internasional yang ada, yang belum sepenuhnya mencakup serangan siber dan tidak mampu menjamin perlindungan yang memadai bagi negara-negara yang menjadi sasaran.

Novelty atau keterbaruan penelitian ini terletak pada kajian mendalam terkait penerapan hukum internasional yang belum sepenuhnya terfokus pada masalah serangan siber terhadap infrastruktur kritis di Indonesia. Penelitian ini akan menyelidiki perbedaan antara teori dan praktik dalam penegakan hukum internasional terkait serangan siber, serta mengusulkan pendekatan baru yang lebih adaptif untuk menangani tantangan ini. Fokus utama adalah mengidentifikasi kesenjangan dalam implementasi hukum internasional di Indonesia dan memberikan rekomendasi yang relevan. Pemilihan judul "Penegakan Hukum Internasional terhadap Serangan Siber terhadap Infrastruktur Kritis di Indonesia" sangat penting, mengingat tantangan yang semakin besar dalam melindungi infrastruktur vital negara dari serangan dunia maya. Serangan siber yang menyasar infrastruktur kritis dapat mengganggu kestabilan ekonomi, sosial, dan politik negara. Oleh karena itu, judul ini relevan untuk memberikan kontribusi terhadap pengembangan teori dan praktik penegakan hukum internasional di ranah keamanan dunia maya, khususnya untuk Indonesia.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif yang berfokus pada kajian terhadap norma-norma hukum yang berlaku, baik yang tercantum dalam peraturan perundang-undangan, doktrin hukum, terkait penegakan hukum internasional terhadap serangan siber terhadap infrastruktur kritis di Indonesia. Untuk menjawab masalah pokok penelitian ini, penulis menggunakan metode penelitian dengan pendekatan kualitatif bertujuan menguraikan secara deskriptif sebagaimana dijelaskan oleh Bogdan dan Taylor yang dikutip Lexy Moleong metodologi kualitatif sebagai prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang diamati pendekatan ini diarahkan pada latar dan individu tersebut secara holistik (utuh).

Metode penelitian deskriptif dalam penelitian digunakan untuk memberikan gambaran secara objektif dan subjektif mengenai sebuah peristiwa ataupun fenomena dengan menghadirkan data yang bernilai fakta yang dimana nantinya menghasilkan kesimpulan yang bersifat mendetail mengenai sebuah isu, peristiwa ataupun fenomena yang diteliti. Dalam tulisan ini, penulis berupaya untuk menjelaskan terkait penegakan hukum internasional terhadap serangan siber terhadap infrastruktur kritis di Indonesia.

3. HASIL DAN PEMBAHASAN

Penerapan Hukum Internasional dalam Menangani Serangan Siber Terhadap Infrastruktur Kritis di Indonesia

Infrastruktur kritis merupakan sektor-sektor vital yang menopang kelangsungan hidup masyarakat dan negara. Di Indonesia, sektor-sektor seperti energi, komunikasi, transportasi, air bersih, dan layanan kesehatan termasuk dalam kategori ini. Ketergantungan pada teknologi informasi yang semakin meningkat menjadikan infrastruktur kritis ini sangat rentan terhadap ancaman siber. Serangan terhadap sektor-sektor ini tidak hanya mengancam keamanan nasional, tetapi juga dapat menimbulkan kerugian ekonomi yang sangat besar. Oleh karena itu, perlindungan terhadap infrastruktur kritis ini menjadi salah satu fokus utama dalam kebijakan keamanan nasional Indonesia.

Serangan siber atau *cyber crime* adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer yang menjadi alat, sasaran atau tempat terjadinya kejahatan. Hukum pada prinsipnya merupakan pengaturan terhadap sikap tindak (perilaku) seseorang dan masyarakat yang terhadap pelanggarnya diberikan sanksi oleh negara. Meskipun dunia *cyber* adalah dunia virtual, hukum tetap diperlukan untuk mengatur sikap tindak masyarakat, setidaknya ada dua hal yakni: Pertama masyarakat yang ada di dunia maya adalah masyarakat yang ada di dunia nyata, masyarakat memiliki nilai dan kepentingan baik secara sendiri-sendiri maupun bersama-sama harus dilindungi. Kedua, walaupun terjadi di dunia maya, transaksi yang dilakukan oleh masyarakat memiliki pengaruh dalam dunia nyata, baik secara ekonomis maupun nonekonomis.

Serangan siber terhadap infrastruktur kritis merujuk pada upaya pihak yang tidak sah untuk mengakses, merusak, atau mengganggu sistem komputer dan jaringan yang mendukung infrastruktur vital negara. Serangan ini dapat berupa perusakan data, pencurian informasi sensitif, hingga pengendalian sistem yang dapat menyebabkan kerusakan fisik atau penghentian operasional infrastruktur kritis. Di Indonesia, meskipun ancaman siber ini semakin

dirasakan, hukum domestik yang ada masih belum sepenuhnya memadai untuk mengatasi masalah ini, sehingga peran hukum internasional menjadi penting dalam penanggulangannya.

Penegakan hukum yaitu suatu keadaan dalam menyerasikan kaidah-kaidah hukum dari nilai-nilai luhur terhadap tindakan yang lahir ditengah-tengah kehidupan bermasyarakat sehingga, dengan keberadaan negara Indonesia sebagai negara hukum dapat membuktikan tujuan akhir dari hukum itu sendiri yaitu suatu bentuk penciptaan ketertiban dan kedamaian hidup dalam bermasyarakat melalui penegakan hukum dan perlindungan hukum.

Kejahatan siber atau *cyber crime* dalam peraturan untuk transaksi elektronik yakni UU ITE, tidak mengatur secara jelas bentuk perlindungan bagi para korban atas kejahatan dalam sebuah transaksi elektronik tersebut. Untuk serangan siber terhadap infrastruktur kritis di Indonesia adalah jenis kejahatan yang dapat mengakibatkan kerugian terhadap korban-korbannya secara materiil, seperti data pribadi. Pada dasarnya, data pribadi dilindungi berdasarkan peraturan perundang-undangan di Indonesia. Oleh karena itu, ketika kerahasiaan terhadap suatu (barang) hak milik tidak lagi sempurna maka membutuhkan perlindungan hukum dalam bentuk perlindungan kepada pihak-pihak yang dirugikan. Karena ketika data pribadi telah diketahui oleh pihak lain dapat mengakibatkan pembobolan terhadap data tersebut, seperti yang marak terjadi yaitu ketertarikan pelaku terhadap data kartu kredit dan/atau nomor rekening sehingga dapat membuat kerugian ekonomi bagi korban.

Akan tetapi, menurut UU ITE bentuk dari pemenuhan hak atas perlindungan bagi para korban dalam sebuah transaksi elektronik atau *cyber crime* ini hanya ditandai dengan adanya bentuk penyelesaian perkara berupa ketentuan pemidanaan atas perbuatan-perbuatan yang dilarang dalam undang-undang ini kepada pelaku tindak pidana dimana hal tersebut tercantum dari Pasal 45 sampai Pasal 52 UU ITE berupa pidana penjara dan/atau pidana denda. Pemidanaan pada pelaku untuk menegakan hukum bagi para korban merupakan langkah yang tepat sehingga kebanyakan bentuk ketentuan pidana yang tercantum dalam UU ITE maupun KUHP, dirangkaikan dengan pemberian sanksi berupa pidana penjara dan pidana denda. Sehingga pada akhirnya, pidana penjara dan pidana denda bagi pelaku tindak pidana dirasa kurang cukup untuk melindungi dan memenuhi hak para korban terlebih khusus bagi korban *cyber crime* untuk mengganti kerugian secara materiil yang tidak sepantasnya ia alami, apalagi bagi korban yang memiliki perekonomian lemah.

Potensi terjadinya tindakan Korban kejahatan ITE merupakan jenis dari risiko operasional. Risiko operasional menurut Pasal 1 Butir 7 Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum merupakan risiko akibat ketidakcukupan dan/atau tidak berfungsinya proses internal, kesalahan manusia,

kegagalan sistem, dan/atau adanya kejadian-kejadian eksternal yang mempengaruhi operasional bank. Michel Crouhy, Dan Gali dan Robert Mark mendefinisikan risiko operasional sebagai risiko yang berkaitan dengan operasional bisnis yang meliputi 2 (dua) komponen risiko. Pertama yaitu kegagalan operasional atau risiko internal yang terdiri dari risiko yang bersumber dari sumber daya manusia, proses dan teknologi. Kedua yaitu risiko strategi operasional atau risiko eksternal yang berasal dari faktor antara lain politik, pajak, regulasi, masyarakat dan kompetisi.Kemudian terdapat perlindungan terhadap korban atas keadaan yang tidak diinginkan di atas yang telah terjadi serta merugikan korban, sehingga perlu adanya upaya dalam menyelesaikan permasalahan tersebut. Perlindungan yang tujuannya menyelesaikan masalah atau sengketa yang timbul dikenal dengan perlindungan represif. Dalam perlindungan hukum terhadap korban *cybercrime* secara mendasar ada dua model pendekatan yang dapat digunakan yaitu: 1) model hak-hak prosedural dalam hal ini korban berperan lebih aktif dan dapat membantu jaksa dalam melakukan penuntutan dan hak hadir dalam setiap tingkat proses peradilan dan 2) model pelayanan dalam hal ini melihat korban sebagai sosok yang harus dilayani oleh Polisi dan aparat penegak hukum yang lainnya, dengan demikian maka korban akan merasa dijamin kembali kepentingannya dalam suasana yang adil. Pemberian bantuan kepada korban kejahatan dunia maya maupun di dunia nyata harus dilakukan pada semua tahap pemeriksaan, mulai dari penyidikan, persidangan dan pasca persidangan.

Penerapan hukum internasional dalam menghadapi serangan siber melibatkan berbagai instrumen yang mencakup aspek pengaturan dan penegakan hukum. Salah satu instrumen utama adalah Konvensi Budapešt tentang Kejahatan Siber (*Council of Europe Convention on Cybercrime)*. Konvensi ini bertujuan untuk membekali negara-negara dengan alat hukum yang dapat digunakan untuk menangani kejahatan dunia maya, termasuk yang menyasar infrastruktur kritis. Meskipun Indonesia bukan pihak dalam konvensi ini, banyak prinsip yang terkandung di dalamnya yang dapat menjadi acuan dalam pengembangan kebijakan keamanan siber Indonesia.

Selain Konvensi Budapešt, PBB juga melalui *United Nations Group of Governmental Experts* (UNGGE) mengeluarkan laporan-laporan yang memberikan pedoman mengenai pengaturan serangan siber dalam konteks keamanan internasional. Laporan ini mengakui bahwa serangan terhadap infrastruktur kritis dapat mengancam perdamaian dan keamanan internasional. Meskipun dokumen ini tidak mengikat secara hukum, ia menyediakan dasar untuk kerjasama internasional dalam menghadapi ancaman siber dan menekankan pentingnya perlindungan terhadap infrastruktur kritis.

Secara domestik, Indonesia telah mengembangkan kebijakan untuk menghadapi ancaman siber melalui pembentukan Badan Siber dan Sandi Negara (BSSN) dan penerapan Undang-Undang Informasi dan Transaksi Elektronik (ITE). Kebijakan-kebijakan ini bertujuan untuk memperkuat sistem pertahanan siber Indonesia dan meningkatkan kerjasama antar lembaga negara dalam menghadapi ancaman siber. Namun, kebijakan ini masih terbatas pada regulasi domestik dan tidak cukup untuk mengatasi serangan yang berasal dari luar negeri. Oleh karena itu, penegakan hukum internasional dalam konteks serangan siber terhadap infrastruktur kritis Indonesia tetap diperlukan.

Selain itu berkaitan dengan penegakan hukum terhadap perlindungan korban yang menjadi korban kejahatan siber di Indonesia, dalam hal ini penulis membahas perbandingan penegakan hukum perlindungan hukum terhadap korban kejahatan informasi dan transaksi elektronik yang menyangkut perlindungan data pribadi di Negara Singapura, Amerika Serikat dan Malaysia.

Singapura

Berdasarkan survey Global Cybersecurity Index (GCI) pada tahun 2017, Singapura dinilai sebagai negara terbaik dalam urusan penerapan keamanan siber. Perjalanan Singapura dalam urusan keamanan siber sudah dimulai satu dekade silam sejak disahkannya *cybersecurity* masterplan pada tahun 2005. Rencana induk awal ini dijalankan selama tiga tahun melalui pendekatan *multi stakeholders* dan berfokus kepada perlindungan data perseorangan, publik dan privat. Selain membangun infrastruktur, rencana induk ini juga menegaskan terhadap pembangunan sumber daya manusia lewat program *capacity building* untuk meningkatkan pemahaman dan kewaspadaan terhadap isu keamanan siber.

Kemudian di tahun 2016, Singapura mengeluarkan *Singapore's* Cyber Security *Strategy* yang berfokus pada empat pilar; penguatan infrastruktur kritis, tanggung jawab kolektif keamanan siber, pengembangan ekosistem keamanan siber yang dinamis, dan memperkuat kerjasama keamanan siber internasional. Terkait dengan perlindungan data pribadi, Singapura telah mengundangkan *Personal Data Protection Act* (PDPA) pada tahun 2012, yang merupakan dasar hukum perlindungan data pribadi di Singapura. Dalam undang-undang tersebut diatur secara lengkap mengenai prinsip-prinsip perlindungan data pribadi, pengumpulan, penggunaan, dan pembukaan data pribadi, akses dan koreksi terhadap data pribadi, perawatan data pribadi, serta mekanisme penegakan hukum. Lebih lanjut, UU tersebut juga mengamanatkan pembentukan *Personal Data Protection Commission* (PDPC) sebagai badan yang berwenang dalam pengawasan dan pelaksanaan PDPA. Salah satu kritik yang muncul terhadap PDPA mengatakan bahwa hukum ini tidak berlaku untuk pemerintah

sehingga belum ada batasan yang jelas atas otoritas dan batas pemerintah dalam penggunaan data pribadi pengguna internet di Singapura.

Selain itu, dalam PDPA tersebut tidak terdapat adanya klasifikasi data pribadi seperti yang ada di GDPR Uni Eropa dan UU PIP Korea Selatan sebagaimana dijelaskan di atas. Meskipun begitu, PDPA memiliki peran yang penting dan jelas dalam hal perlindungan data pribadi yang patut dicontoh oleh negara-negara lain di seluruh dunia. Ketatnya regulasi perlindungan data pribadi di Singapura tidak serta merta membuat tindakan penyalahgunaan data pengguna hilang sepenuhnya. Menariknya, PDPC merekapitulasi seluruh dugaan dan tindakan pelanggaran (*breach*) terhadap PDPA di situsnya sehingga data tersebut mudah diakses publik. Hal ini menunjukkan jika PDPC selaku pihak yang berwenang menyikapi seluruh pelanggaran perlindungan data pribadi secara serius terlepas dari besar-kecilnya skala ancaman yang ditimbulkan. Misalnya, PDPC memberikan ultimatum kepada *National University of Singapore* (NUS) dalam 120 hari untuk memberikan pelatihan kepada mahasiswanya dalam hal perlindungan data pribadi.

Tindakan ini diambil setelah PDPC menemukan ratusan data pribadi mahasiswa baru NUS (nama lengkap, nomor HP, preferensi makanan, alamat surel, dan sebagainya.) yang awalnya disimpan dalam layanan komputasi awan *google sheet spreadsheet* akhirnya tersebar ke publik karena kecerobohan salah satu pemilik dokumen yang tidak teridentifikasi untuk mengubah aturan dokumen tersebut agar menjadi dapat diakses publik secara bebas. Selain itu, PDPC juga tidak segan memberi denda sebesar S$10.000 kepada Perusahaan besar seperti JP Pepperdine Group dan Propnex Reality yang lalai menjaga privasi data penggunanya di situs masing-masing sehingga dapat dilihat oleh publik. Akan tetapi, Singapura rupanya juga tidak luput dari skandal Cambridge Analytica. Kasus ini pun saat ini tengah menjadi perhatian dari PDPC dan investigasi mendalam masih dilakukan.

Amerika Serikat

Berdasarkan survei GCI pada tahun 2017, Amerika Serikat menempati posisi kedua setelah Singapura sebagai negara dengan tingkat keamanan siber terbaik. Dalam hal tata kelola *internet*, Amerika Serikat memiliki peran yang vital baik sebagai pelaku maupun regulator. Pada awalnya, internet sendiri diatur oleh Kementerian Pertahanan Amerika Serikat sebelum akhirnya diserahkan ke badan-badan non-negara internasional seperti ICANN, ITU dan sebagainya lewat lobi politik dan kerjasama antar *stakeholders* di seluruh dunia demi mewujudkan tata kelola internet (*internet governance*) yang lebih adil dan transparan. Sebagai negara tempat internet pertama kali dikembangkan, uniknya Amerika Serikat hingga saat ini belum memiliki undang-undang di level federal yang secara khusus mengatur tentang

perlindungan data pribadi. Pada tahun 2008, pemerintah Amerika Serikat di bawah Presiden George W. Bush memperkenalkan *Comprehensive National Cybersecurity Initiative* yang tidak berfungsi sebagai undang-undang melainkan hanya sebagai garis haluan dalam pengembangan kerangka keamanan siber di Amerika Serikat. Selebihnya, Peraturan perlindungan data pribadi di Amerika Serikat yang ada saat ini dikembangkan di negara bagian masing-masing dan sektor publik/pemerintahan tertentu (misalnya di sektor kesehatan dan keuangan). Sistem perundang-undangan yang tidak terintegrasi ini dikhawatirkan memunculkan peraturan yang tumpang tindih dan gagal melaksanakan tugasnya untuk melindungi keamanan data pengguna 28 internet.

Selain itu, Amerika Serikat juga tidak memiliki lembaga khusus yang menangani perlindungan data pribadi. Isu-isu terkait dengan keamanan data kebanyakan dipegang oleh Federal Trade Commission (FTC). Meskipun begitu, Amerika Serikat mendapatkan nilai 1 untuk aspek legal dan 0.96 untuk aspek teknis dalam penilaian GCI 2017. Alasan dibalik tingginya skor Amerika Serikat dalam hal legal ditengarai adanya beberapa tindakan pemerintah pusat yang mampu menghubungkan kebijakan-kebijakan di level sektoral. Misalnya, terbentuknya *Resource Center for State Cybersecurity* sebagai wadah bagi pemangku kepentingan di level negara bagian untuk saling berkoordinasi, memberi informasi dan advokasi kepada negara bagian lainnya dalam menghadapi isu keamanan siber. Selain itu, Amerika Serikat juga memiliki US *Cybersecurity Information Sharing Act* (CISA) 2015. Elemen yang menarik dari aturan ini adalah keleluasaan bagi pihak pemerintah, swasta dan individu untuk bekerjasama dalam berbagi informasi mengenai ancaman keamanan siber.

Malaysia

Malaysia merupakan negara yang menempati peringkat ketiga dalam GCI pada tahun 2017 setelah Singapura dan Amerika Serikat. Upaya pengembangan keamanan siber sudah dimulai bahkan sejak tahun 1997 melalui pendirian Malaysian *Computer Emergency Response Team* (MyCERT) atau yang sekarang dikenal sebagai *Cybersecurity Malaysia*. Lembaga tersebut merupakan organisasi pemerintah di bawah Kementerian Sains, Teknologi dan Inovasi yang bertanggung jawab atas keamanan siber di Malaysia serta mempromosikan keamanan internet di kalangan pengguna internet di Malaysia.

Dalam konteks perlindungan data pribadi, pada tahun 2000, pemerintah Malaysia memperkenalkan Rancangan Undang-Undang Perlindungan Data Pribadi yang perancangannya didasarkan pada Standar Perlindungan Data Eropa, meskipun RUU tersebut pada akhirnya tidak sampai dibahas di Parlemen karena menuai oposisi yang besar dari industri komunikasi dan multimedia. Pembahasan mengenai RUU Perlindungan Data Pribadi di

Malaysia telah melalui perjalanan yang panjang, hingga akhirnya pada tahun 2010, Undang-Undang Perlindungan Data Pribadi (UU PDP 2010) diundangkan. UU PDP 2010 yang terdiri dari 146 Pasal tersebut dapat dibilang cukup spesifik mengatur mengenai perlindungan data pribadi. Beberapa poin penting yang diatur dalam UU tersebut berkaitan dengan klasifikasi data pribadi, prinsip-prinsip perlindungan data pribadi, hak-hak pemilik data, pembentukan badan khusus terkait perlindungan data pribadi, serta prosedur penegakan hukum terkait pelanggaran 37 maupun kejahatan yang terkait dengan data pribadi. UU PDP 2010 berfokus pada pemrosesan data pribadi dalam transaksi komersial dan untuk mencegah penyalahgunaan data pribadi.

Meskipun Malaysia telah memiliki dasar hukum dalam perlindungan data pribadi serta lembaga yang dibentuk khusus untuk melaksanakan UU tersebut, rupanya masih terdapat pula permasalahan dalam implementasinya. Hal ini salah satunya dikarenakan definisi data pribadi sebagaimana diatur dalam UU PDP 2010 tersebut didasarkan pada data terkait dengan transaksi komersial (sehingga tidak bisa mencakup data pribadi di luar transaksi komersial), dan transaksi komersial sendiri didefinisikan secara luas. Bahkan, berdasarkan penelitian yang dilakukan oleh Noriswadi Ismail, seorang akademisi hukum dari Malaysia, definisi transaksi komersial yang luas tersebut menimbulkan ketidakpastian bagi pemegang data (*data users*), mengingat definisi tersebut juga mencakup pengumpulan, perekaman, penyimpanan, bahkan segala tindakan yang berkaitan dengan data pribadi (seperti pengorganisasian data, adaptasi, pembukaan data, dan pengiriman serta pertukaran data). Selain itu, terdapat pula isu mengenai keterlibatan *Cambridge Analytica* dalam pemilu di Malaysia, yang tentunya mengindikasikan adanya penyalahgunaan penggunaan data pribadi masyarakat Malaysia.

Menurut analisis penulis, meskipun ada berbagai instrumen internasional yang relevan, penerapan hukum internasional di Indonesia menghadapi sejumlah tantangan. Salah satu tantangan terbesar yang dihadapi dalam penerapan hukum internasional terhadap serangan siber adalah ketidakjelasan dalam kerangka hukum internasional itu sendiri. Meskipun instrumen internasional seperti Konvensi Budapešt tentang kejahatan siber dan pedoman yang dikeluarkan oleh United Nations Group of Governmental Experts (UNGGE) memberikan dasar hukum, masih terdapat banyak ruang kosong dalam hal penerapan yang konsisten dan mekanisme penegakan yang tegas. Beberapa aspek, seperti definisi serangan siber yang universal dan standar internasional yang mengikat, belum sepenuhnya terwujud. Negara-negara yang menjadi pihak dalam instrumen tersebut seringkali memiliki interpretasi yang berbeda terkait jenis serangan dan dampaknya terhadap keamanan nasional, sehingga penerapan hukum internasional sering kali tidak sejalan dengan kebutuhan praktis.

Penegakan hukum internasional dalam konteks serangan siber terhadap infrastruktur kritis Indonesia sering kali terhalang oleh masalah kedaulatan negara**.** Dalam banyak kasus, serangan siber dilakukan oleh aktor non-negara atau bahkan negara lain yang berada di luar batas yurisdiksi Indonesia. Ini menimbulkan persoalan mengenai hak negara untuk melakukan penegakan hukum di luar wilayahnya**.** Negara yang diserang sering kali mengalami kesulitan dalam menanggapi serangan yang datang dari luar negeri, karena mekanisme hukum internasional tidak selalu memberikan kewenangan yang jelas bagi negara tersebut untuk bertindak secara langsung dan efektif. Selain itu, serangan siber yang terjadi sering kali bersifat tersembunyi, dengan pelaku yang sulit dilacak, baik itu individu, kelompok, atau negara yang berada di luar yurisdiksi hukum Indonesia. Hal ini semakin memperumit upaya untuk menuntut pelaku dan memberikan sanksi yang sesuai. Dalam konteks ini, hukum internasional masih terbatas dalam memberikan solusi konkret untuk memastikan bahwa serangan terhadap infrastruktur kritis dapat dikenakan sanksi yang efektif, terutama ketika pelaku berada di luar batas wilayah hukum nasional.

Kerjasama internasional dalam menangani serangan siber sangat penting, mengingat sifat serangan yang sering kali lintas batas negara. Kerjasama antar negara menjadi kunci dalam membangun kapasitas bersama untuk melawan ancaman siber, serta untuk memastikan bahwa negara-negara dapat bekerja bersama dalam menanggulangi serangan terhadap infrastruktur kritis. Indonesia sendiri telah berpartisipasi dalam forum internasional seperti ASEAN *Cybersecurity Cooperation Strategy* dan berkolaborasi dengan negara-negara anggota untuk memperkuat kebijakan dan sistem pertahanan siber. Namun, standarisasi global yang masih terbatas menjadi hambatan dalam menciptakan kerangka kerja yang efektif dalam penanggulangan serangan siber. Setiap negara memiliki kebijakan dan prioritas yang berbeda dalam hal keamanan siber, yang sering kali tidak sejalan. Hal ini menyebabkan ketidaksepakatan mengenai norma dan standar internasional yang harus diterapkan untuk menghadapi serangan siber terhadap infrastruktur kritis. Dalam hal ini, Indonesia harus terus bekerja sama dengan negara-negara lain untuk menciptakan kesepakatan internasional yang lebih seragam dan dapat diterapkan di berbagai negara, termasuk dalam hal penegakan hukum terhadap pelaku serangan siber.

Berdasarkan analisis tersebut, penulis menyimpulkan bahwa penerapan hukum internasional dalam menangani serangan siber terhadap infrastruktur kritis di Indonesia masih menghadapi banyak tantangan, baik dari sisi regulasi yang belum komprehensif, masalah kedaulatan negara, hingga ketidakseragaman standar internasional. Namun, peningkatan kerjasama internasional dan penguatan kebijakan domestik dapat membantu Indonesia dalam

menghadapi ancaman ini secara lebih efektif. Negara-negara di seluruh dunia, termasuk Indonesia, harus terus berinovasi dalam menciptakan kerangka hukum yang dapat memberikan perlindungan yang lebih kuat terhadap infrastruktur kritis, serta memastikan bahwa serangan siber yang mengancam kestabilan internasional dapat ditangani dengan tegas dan efisien.

Kendala yang dihadapi Indonesia dalam Menegakkan Hukum Internasional Terkait Serangan Siber Terhadap Infrastruktur Kritis Serta Upaya dalam Menghadapi Kendala dalam Menegakkan Hukum Internasional Terkait Serangan Siber Terhadap Infrastruktur Kritis di Indonesia

Penegakan hukum internasional terhadap serangan siber terhadap infrastruktur kritis di Indonesia merupakan tantangan besar yang memerlukan pendekatan komprehensif. Serangan siber yang menargetkan sektor-sektor vital seperti energi, komunikasi, dan perbankan dapat merusak stabilitas nasional dan global. Namun, Indonesia menghadapi berbagai kendala dalam menerapkan hukum internasional terkait ancaman tersebut. Kendala ini terkait dengan faktor-faktor hukum domestik, kedaulatan negara, kerjasama internasional, serta keterbatasan teknologi dan sumber daya. Dalam menghadapi tantangan ini, Indonesia perlu mengidentifikasi dan mengatasi kendala-kendala tersebut melalui berbagai upaya yang melibatkan reformasi kebijakan, peningkatan kapasitas domestik, dan memperkuat kerjasama internasional.

Dalam menegakkan hukum siber, terdapat tantangan yang dihadapi penegak hukum dalam menegakkan hukum. Keterbatasan sumber daya dan kapasitas merupakan tantangan utama dalam penegakan hukum siber di Indonesia. Faktanya, menurut survei yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN), kurang dari separuh lembaga pemerintah di Indonesia yang memiliki kebijakan keamanan siber yang memadai, yang menunjukkan kesenjangan serius dalam infrastruktur keamanan digital negara. Hal ini terutama menjadi masalah ketika kita mempertimbangkan kasus-kasus seperti serangan siber terhadap database pemerintah atau kebocoran data yang besar, seperti insiden kebocoran data pengguna platform *e-commerce* besar di Indonesia pada tahun 2020. Lebih lanjut, kesulitan mengidentifikasi pelaku kejahatan siber menjadi semakin rumit dengan adanya teknologi enkripsi dan penggunaan jaringan privat virtual (VPN) oleh pelaku atau *server proxy* yang dapat mempersulit pelacakan dengan menyembunyikan jejak digital mereka. Teknologi enkripsi canggih memungkinkan pelaku untuk mengamankan komunikasi dan data mereka, sehingga sulit untuk diintersepsi atau diakses oleh penegak hukum. VPN dan *server proxy* menambah lapisan kompleksitas lainnya, karena mereka memungkinkan pelaku untuk menyembunyikan lokasi fisik mereka dan membuat jejak digital mereka lebih sulit untuk dilacak. Penggunaan VPN dan server proxy dapat menyulitkan penegak hukum untuk menentukan sumber

sebenarnya dari serangan siber atau aktivitas ilegal lainnya. Pelaku dapat tampak seolah-olah mereka beroperasi dari negara yang berbeda, atau bahkan dari beberapa negara, membuat investigasi menjadi lebih rumit dan sering kali memerlukan kerjasama lintas yurisdiksi.

Dalam era globalisasi, kejahatan siber seringkali juga tidak terbatas pada batas-batas nasional, sehingga memerlukan kerjasama dan kesesuaian dengan standar internasional. Membandingkan regulasi yang ada pada UU ITE dengan regulasi Internasional dapat menjadi tolak ukur efisiensi hukum nasional. Regulasi internasional sering kali mencerminkan praktik terbaik yang telah berkembang melalui konsensus antar negara dan pakar di bidangnya. Mereka menyediakan kerangka kerja untuk menangani berbagai aspek keamanan siber dan perlindungan data yang mungkin belum sepenuhnya tercakup dalam hukum nasional. Selain itu, membandingkan regulasi nasional dengan regulasi Internasional dapat membantu mengindentifikasi celah pada UU ITE untuk kemudian ditindak lanjuti sehingga meningkatkan keamanan siber nasional. Dan ketika regulasi nasional sesuai dengan regulasi Internasional, kerjasama lintas batas kaitannya dalam menangani kejahatan siber dan pertukaran data dalam penanaganan kejahatan lintas negara menjadi lebih mudah. Ketika dibandingkan, ditemukan kesamaan dan perbedaan antara keduanya. Kesamaan dalam regulasi keamanan siber di negara-negara lain dapat dilihat pada beberapa aspek, khususnya dalam hal definisi dan sanksi untuk kejahatan siber. Seperti regulasi di banyak negara, UU ITE turut serta mengatur tentang kejahatan terkait penipuan online, penyebaran virus, dan serangan siber lainnya. Hukum ini juga mengakui perlunya melindungi data pribadi, serupa dengan regulasi di Uni Eropa seperti General Data Protection Regulation (GDPR).

Aspek lain yang serupa termasuk pemberlakuan hukum terhadap penyebaran konten ilegal dan ujaran kebencian. Selain itu, ada upaya untuk mengatur transaksi elektronik, yang penting dalam ekonomi digital yang berkembang pesat. Sedangkan perbedaan mencolok antara regulasi UU ITE Indonesia dan regulasi keamanan siber di negara lain dapat dilihat pada hal keseimbangan antara keamanan siber dan kebebasan berekspresi. Di beberapa negara, regulasi keamanan siber mereka lebih mengedepankan aspek perlindungan hak asasi manusia, termasuk kebebasan berekspresi. Ini berarti bahwa dalam merancang dan menerapkan hukum siber, negara-negara tersebut memberikan perhatian khusus untuk memastikan bahwa tindakan keamanan siber tidak secara tidak semestinya membatasi hak-hak dasar seperti kebebasan berekspresi, privasi, dan akses informasi. Sedangkan UU ITE sering dikritik karena potensi penyalahgunaannya dalam membatasi kebebasan berekspresi. Selain itu, dalam konteks penanganan data pribadi, UU ITE belum sekomprehensif *General Data Protection Regulatio*n (GDPR), yakni regulasi yang diterapkan oleh Uni Eropa (EU) dalam hal hak individu atas data

mereka. Dalam konteks penegakan hukum, kejahatan siber di Indonesia seringkali terkendala oleh beberapa faktor. Berkaitan dengan kendala yang dihadapi Indonesia dalam menegakkan hukum internasional terkait serangan siber terhadap infrastruktur kritis serta upayanya sesuai pada tabel 1. berikut:

Tabel 1. Kendala dan Upaya dalam Menghadapi Kendala dalam Menegakkan Hukum Internasional Terkait Serangan Siber Terhadap Infrastruktur Kritis di Indonesia

No.	Kendala yang Dihadapi	Upaya Menghadapi Kendala
1	Ketidakjelasan Definisi dan Standar Internasional	- Memperbarui dan menyelaraskan kebijakan domestik dengan standar internasional seperti Konvensi Budapešt dan pedoman UNGGE. - Membentuk forum internasional untuk merumuskan standar seragam mengenai serangan siber dan infrastruktur kritis.
2	Masalah Kedaulatan Negara	- Meningkatkan kerjasama bilateral dan multilateral dengan negara-negara lain dalam hal penanganan serangan siber. - Menguatkan pengawasan dan penegakan hukum siber lintas batas melalui lembaga internasional seperti INTERPOL dan ASEAN.
3	Ketidaksepakatan Antar Negara Mengenai Hukum Siber	- Memfasilitasi dialog dan kesepakatan internasional yang lebih kuat dalam hal regulasi siber dan perlindungan infrastruktur kritis. - Mengusulkan perjanjian internasional yang mengikat terkait penegakan hukum atas serangan siber.
4	Keterbatasan Sumber Daya dan Teknologi di Indonesia	- Meningkatkan investasi dalam teknologi pertahanan siber dan memperkuat kapasitas sumber daya manusia melalui pelatihan dan pendidikan. - Mengoptimalkan peran Badan Siber dan Sandi Negara (BSSN) dalam membangun ekosistem keamanan digital.
5	Kesulitan dalam Melacak dan Menindak Pelaku Serangan Siber	- Meningkatkan kerjasama intelijen dengan negara-negara lain untuk melacak pelaku siber secara lebih efektif. - Menggunakan teknologi canggih untuk mendeteksi dan menanggulangi serangan lebih awal.
6	Regulasi yang Tidak Memadai untuk Penanganan Kejahatan Siber	- Mengembangkan peraturan baru yang lebih spesifik untuk menangani serangan siber terhadap infrastruktur kritis. - Memperbarui Undang-Undang Informasi dan Transaksi Elektronik (ITE) untuk mencakup aspek perlindungan infrastruktur kritis.

Berdasarkan tabel di atas, dapat dilihat bahwa Indonesia menghadapi berbagai kendala dalam menegakkan hukum internasional terkait serangan siber terhadap infrastruktur kritis, termasuk ketidakjelasan definisi dan standar internasional, masalah kedaulatan negara, ketidaksepakatan antar negara, keterbatasan sumber daya dan teknologi, serta kesulitan dalam

melacak pelaku. Upaya untuk mengatasi kendala-kendala ini melibatkan penguatan kerjasama internasional, peningkatan kapasitas teknologi dan sumber daya domestik, serta pembaruan regulasi yang lebih relevan dan komprehensif. Dengan langkah-langkah tersebut, Indonesia dapat lebih efektif dalam melindungi infrastruktur kritisnya dari ancaman serangan siber dan memastikan penegakan hukum internasional yang lebih tegas dan efisien.

Penulis menganalisis bahwa pertukaran informasi tentang ancaman siber antarlembaga memainkan peran penting dalam memperkuat keamanan siber secara kolektif. Ketika lembaga-lembaga berbagi data tentang serangan terbaru, taktik penipuan, atau kerentanan keamanan yang teridentifikasi, setiap entitas menjadi lebih siap dan responsif terhadap ancaman yang muncul. Proses pertukaran informasi ini memungkinkan lembaga-lembaga untuk belajar dari pengalaman satu sama lain dan secara proaktif mengadaptasi strategi keamanan mereka. Misalnya, jika satu lembaga mengidentifikasi sebuah metode serangan siber baru, informasi ini dapat dibagikan dengan cepat, memungkinkan lembaga lain untuk segera mengimplementasikan langkahlangkah pertahanan atau mitigasi yang diperlukan. Pengembangan standar keamanan bersama oleh berbagai lembaga merupakan langkah penting dalam menciptakan kerangka kerja yang konsisten untuk melindungi aset digital. Dengan adanya standar keamanan yang disepakati dan diterapkan secara luas, lembaga-lembaga dapat memastikan bahwa tingkat perlindungan terhadap aset digital mereka adalah seragam dan memadai. pengembangan standar keamanan bersama oleh berbagai lembaga membantu menciptakan kerangka kerja yang konsisten untuk melindungi aset digital. Ini termasuk pembuatan kebijakan yang memastikan implementasi praktik terbaik dalam keamanan siber di semua lembaga, meningkatkan keseragaman dan efektivitas dalam melawan ancaman siber. Latihan bersama untuk meningkatkan kesiapsiagaan terhadap serangan siber sangat penting. Melalui simulasi serangan siber, lembaga-lembaga ini dapat mengidentifikasi kelemahan dalam sistem mereka dan memperbaikinya sebelum terjadi serangan nyata. Latihan ini juga membantu memperkuat koordinasi dan kerjasama antarlembaga dalam merespon insiden siber.

Kerjasama antar lembaga memungkinkan integrasi berbagai perspektif dan keahlian, yang membantu dalam menciptakan regulasi siber yang lebih konsisten dan komprehensif. Ketika lembaga-lembaga dari berbagai bidang ini bekerja sama, mereka dapat saling melengkapi. Misalnya, lembaga teknologi dan keamanan siber dapat menyediakan wawasan tentang ancaman terkini dan kemajuan teknologi, sedangkan lembaga hukum dan hak asasi manusia dapat memastikan bahwa regulasi yang dikembangkan tidak hanya efektif dalam menangani kejahatan siber, tetapi juga menghormati hak-hak dasar dan kebebasan individu. Karena tiap lembaga akan membawa pemahaman uniknya masing-masing mengenai tanda

tangan dan solusi, sehingga cakupan regulasi menjadi semakin luas dan memfasilitasi berbagai sumber daya dari teknologi, data dan juga keahlian, sehingga kejahatan siber dapat diatasi dengan lebih baik dengan adanya fasilitas yang mendukung ini.

4. KESIMPULAN DAN SARAN

Berdasarkan analisis disimpulkan bahwa penegakan hukum internasional terhadap serangan siber terhadap infrastruktur kritis di Indonesia melalui penerapan hukum internasional dalam menangani serangan siber terhadap infrastruktur kritis menghadapi berbagai tantangan signifikan, baik dari sisi regulasi, masalah kedaulatan negara, maupun ketidakseragaman standar internasional. Meskipun Indonesia telah berpartisipasi dalam berbagai inisiatif internasional seperti Konvensi Budapešt dan United Nations Group of Governmental Experts (UNGGE), mekanisme penegakan hukum internasional masih belum cukup efektif untuk menangani ancaman siber lintas batas, terutama yang melibatkan pelaku di luar yurisdiksi Indonesia. Meskipun hukum domestik Indonesia, seperti Undang-Undang Informasi dan Transaksi Elektronik (ITE), berusaha melindungi data pribadi dan infrastruktur kritis, ketentuan yang ada masih terbatas dalam mengatasi serangan yang berasal dari luar negeri. Oleh karena itu, perlu adanya upaya kolaboratif yang lebih erat antara Indonesia dan negara-negara lain untuk memperkuat kerangka hukum internasional yang lebih seragam dan aplikatif, serta memperbarui kebijakan domestik agar lebih komprehensif dalam menghadapi ancaman siber. Selain itu, penguatan kapasitas hukum domestik dan kerjasama internasional yang lebih terintegrasi sangat diperlukan agar serangan terhadap infrastruktur kritis dapat ditangani dengan lebih efektif, memberikan perlindungan lebih kuat, dan meminimalkan kerugian baik secara materiil maupun non-materiil bagi negara dan masyarakat.

Indonesia menghadapi sejumlah kendala signifikan dalam menegakkan hukum internasional terkait serangan siber terhadap infrastruktur kritis, yang meliputi ketidakjelasan definisi dan standar internasional yang mengatur serangan siber, masalah kedaulatan negara yang membatasi yurisdiksi penegakan hukum, ketidaksepakatan antar negara mengenai regulasi siber, keterbatasan sumber daya dan teknologi yang memadai, serta kesulitan dalam melacak dan menindak pelaku yang sering kali beroperasi lintas batas. Untuk menghadapi kendala-kendala tersebut, Indonesia perlu mengembangkan kerjasama internasional yang lebih erat, memperkuat kapasitas domestik dalam hal teknologi dan sumber daya manusia, serta memperbarui regulasi yang ada agar lebih spesifik dan sesuai dengan dinamika ancaman siber yang terus berkembang. Penguatan koordinasi antara sektor publik, swasta, dan lembaga internasional, bersama dengan reformasi kebijakan dan peningkatan infrastruktur siber, akan

menjadi kunci untuk memastikan perlindungan yang lebih efektif terhadap infrastruktur kritis Indonesia dari ancaman siber dan memastikan penegakan hukum internasional yang lebih kuat dan responsif di masa depan.

DAFTAR REFERENSI

Ahmad, J. (2016). Perlindungan nasabah debitur terhadap perjanjian baku yang mengandung klausula eksonerasi pada bank umum di Bandar Lampung. Fiat Justisia Journal of Law, 10(2), 128.

Anugerah, A. S. (2019). Mengenal jenis penelitian deskriptif kualitatif pada sebuah tulisan ilmiah. Ilustrasi Penelitian.

Arafat, M. R., & Wirasto, A. T. E. (2024). Kebijakan kriminal dalam penanganan siber di era digital: Studi kasus di Indonesia. Equality: Journal of Law and Justice, 1(2), 220–241. https://doi.org/10.69836/equality-jlj.v1i2.170

Azmi, I. M. (2007). Personal data protection law: The Malaysian experience. Information & Communications Technology Law, 16(2), 125.

Citra, Y., Desy, N. K., Pinatih, S. A., & Negara, S. P. (2023). Strategi penanganan keamanan siber (cyber security) di Indonesia, 6, 1941–1949.

Cloramidine, F., & Badaruddin, M. (2023). Mengukur keamanan siber Indonesia melalui indikator pilar kerjasama dalam Global Cybersecurity Index (GCI). Populis: Jurnal Sosial dan Humaniora, 8(1), 57–73. https://doi.org/10.47313/pjsh.v8i1.1957

Crouhy, M., Galai, D., & Mark, R. (2014). The essentials of risk management. New York: McGraw Hill Education.

Cybersecurity Malaysia. (2011). Laporan tahunan 2011. Cybersecurity Malaysia.

Czuryk, M. (2023). Cybersecurity and protection of critical infrastructure. Studia Iuridica Lublinensia, 32(5), 43–52. https://doi.org/10.17951/sil.2023.32.5.43-52

Dheny, W. (n.d.). Perlindungan hukum terhadap korban kejahatan cyber crime di Indonesia. Jurnal Ilmu Hukum Fakultas Hukum Universitas Jambi.

DLA Piper. (n.d.). Data protection laws of the world: United States. https://www.dlapiperdataprotection.com/index.html?t=law&c=US

Gramatica, M. d., Massacci, F., Shim, W., Tedeschi, A., & Williams, J. (2015). IT interdependence and the economic fairness of cybersecurity regulations for civil aviation. IEEE Security & Privacy, 13(5), 52–61. https://doi.org/10.1109/msp.2015.98

Hayati, A. N. (2021). Analisis tantangan dan penegakan hukum persaingan usaha pada sektor e-commerce di Indonesia. Jurnal Penelitian Hukum De Jure, 21(1), 109. https://doi.org/10.30641/dejure.2021.v21.109-122

Infocomm Media Development Authority. (2017). Singapore gears up for cyber security. https://www.imda.gov.sg/about/newsroom/archived/ida/mediareleases/2005/20050712110643

Josua, S. (2012). Cyberspace, cybercrime, cyberlaw, tinjauan aspek hukum pidana. Jakarta: PT. Tatanusa.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. Computational Methods in Applied Sciences, 3–42. https://doi.org/10.1007/978-3-030-91293-2_1

Lexy, J. M. (1993). Metodologi penelitian kualitatif. Bandung: Remaja Rosdakarya.

Ministry of Communications and Information. (2016). Singapore's cybersecurity strategy 2016. https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

Mkhwanazi, T. D., & Futcher, L. (2024). National critical information infrastructure protection through cybersecurity: A national government perspective. International Conference on Cyber Warfare and Security, 19(1), 555–564. https://doi.org/10.34190/iccws.19.1.1987

O'Connor, N. (2018). Reforming the US approach to data protection and privacy. Council on Foreign Relations. https://www.cfr.org/report/reforming-us-approach-data-protection

Personal Data Protection Commission Singapore. (n.d.). Who we are. https://www.pdpc.gov.sg/About-Us/Who-We-Are

Ramli, A. M., Dewi, S., Rafianti, L., Ramli, T. S., Putri, S. A., & Lestari, M. A. (2021). Perlindungan rahasia dagang dalam industri jasa telekomunikasi. Jurnal Ilmiah Kebijakan Hukum, 15(2), 215. https://doi.org/10.30641/kebijakan.2021.v15.215-230

Samad, M. Y., & Persadha, P. D. (2022). Memahami perang siber dan peran badan intelijen negara dalam menangkal ancaman di siber. Jurnal Iptekkom Jurnal Ilmu Pengetahuan & Teknologi Informasi, 24(2), 135–146. https://doi.org/10.17933/iptekkom.24.2.2022.135-146

Setiawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). Upaya regulasi teknologi informasi dalam menghadapi serangan siber (cyber attack) guna menjaga kedaulatan Negara Kesatuan Republik Indonesia. Jurnal Usm Law Review, 3(2), 275–295. https://doi.org/10.26623/julr.v3i2.2773

Sholikah, D. I., Putra, T. H., & Hidayat, M. F. (2024). Cyber warfare is the newest challenge to support Indonesian national resilience. Asian Journal of Social and Humanities, 2(9), 2000–2006. https://doi.org/10.59888/ajosh.v2i9.332

Syahrin, M. A. (2020). Konsep keabsahan kontrak elektronik berdasarkan hukum nasional dan UNCITRAL Model Law on Electronic Commerce. Repertorium Jurnal Ilmiah Hukum Kenotariatan, 9(2), 105–122. https://doi.org/10.28946/rpt.v9i2.419

Teoh, C. S., & Mahmood, A. K. (2018). Cybersecurity workforce development for digital economy. The Educational Review, USA, 2(1). https://doi.org/10.26855/er.2018.01.003

Wahyuni, R. A. E. (2019). Implementation of legal protection by the government in order to empowerment of micro small medium enterprise to realize the justice economy (Research study: The Office of Cooperative and Micro Small and Medium Enterprise Province of Central Java). Diponegoro Law Review, 4(1), 389.

Waskita, A. S., & Sidik, H. (2023). Diplomasi siber Indonesia dalam penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019. Padjadjaran Journal of International Relations, 5(2), 142. https://doi.org/10.24198/padjir.v5i2.41337