JURNAL SAHID DA'WATII
Volume 03 Nomor 02 (Desember 2024)
http://jurnal-inais.id/index.php/JurnalSD

e-ISSN : 2961-9785
p-ISSN: xxxx-xxxx

PERAN HUKUM INTERNASIONAL DALAM MENANGANI KASUS *CYBER CRIME*

[1]Wahyu Rifqi Febrian, Raden Mohammad Rangga Faturrahman, Hannah Syahida Rahmadina [UIN Syarif Hidayatullah Jakarta, Kota Tangerang Selatan, 15412]
[2]Fitra Deni [UIN Syarif Hidayatullah Jakarta, Kota Tangerang Selatan, 15412]

E-mail: rifqi.febrian23@mhs.uinjkt.ac.id, rangga.faturrahman23@mhs.uinjkt.ac.id, hannah.rahmadina23@mhs.uinjkt.ac.id

Abstract

Cybercrime is a crime committed through computer networks as the main tool of the perpetrator in carrying out his actions. This type of cybercrime includes several illegal activities such as hacking, phishing, ransomware, malware, identity theft, and so on. Cybercrime has become a global threat that requires international cooperation to overcome. Cybersecurity is currently a fundamental thing that must be considered by the community or government. A weak cyber security system will become the target of hackers in carrying out their actions. Not only that, the weak law enforcement in handling this case is also a gap for hackers to always do their actions. Therefore, various instruments such as conventions on cyber crime, international law, and international cooperation are the main weapons in dealing with cyber crime. In this article, the author will analyze how the role of international law in dealing with cybercrime cases, including existing mechanisms and instruments as well as the challenges faced and the effectiveness of international cooperation in fighting cybercrime networks. This research aims to find out the role of international law in handling cybercrime cases, challenges in the application of international law, international legal instruments and the effectiveness of international cooperation. This research uses a qualitative approach with document analysis and case studies to explore the effectiveness and weaknesses of international law in dealing with cyber crime. The results found that the role of international law is still not maximized due to various challenges in its implementation, but with Indonesia not ratifying the Budapest Convention, this hampers the role of international legal instruments in tackling cyber crime cases in Indonesia. Despite this, the role of international law is still needed to maximize the opportunities for international cooperation carried out by the authorities in fighting cybercrime cases.

Keywords: *international law, cyber crime, cyber attack, cooperation, harmonization.*

Abstrak

Cybercrime merupakan suatu kejahatan yang dilakukan melalui jaringan komputer sebagai alat utama si pelaku dalam melancarkan aksinya. Jenis kejahatan siber ini mencakup beberapa aktivitas ilegal seperti hacking, phising, ransomware, malware, identity theft, dan lain sebagainya. Cybercrime telah menjadi ancaman global yang memerlukan kerjasama internasional untuk penanggulangannya. Keamanan siber saat ini menjadi hal fundamental yang harus diperhatikan oleh masyarakat ataupun pemerintah. Sistem keamanan siber yang lemah akan menjadi sasaran para hacker dalam melancarkan aksinya. Tidak hanya itu, lemahnya penegakan hukum dalam menangani kasus ini juga menjadi celah bagi para hacker untuk selalu melakukan perbuatannya. Oleh karena itu, berbagai instrumen seperti konvensi tentang cyber crime, hukum internasional, dan kerjasama internasional menjadi senjata utama dalam menangani kejahatan siber. Dalam artikel ini, penulis akan menganalisis bagaimana peran hukum internasional dalam menangani kasus cybercrime, termasuk mekanisme dan instrumen yang ada serta tantangan yang dihadapi dan efektivitas kerjasama internasional dalam melawan jaringan kejahatan siber. Penelitian ini bertujuan untuk mengetahui peran hukum internasional dalam menangani kasus cyber crime, tantangan dalam penerapan hukum internasional, instrumen hukum internasional dan efektivitas kerjasama internasional. Penelitian ini menggunakan pendekatan kualitatif dengan analisis dokumen dan studi kasus untuk mengeksplorasi efektivitas dan kelemahan hukum internasional dalam menghadapi kejahatan siber. Hasil penelitian menemukan bahwa peran hukum internasional masih belum maksimal akibat berbagai tantangan dalam implementasinya, namun dengan Indonesia tidak meratifikasi Konvensi Budapest hal ini menghambat peran instrumen hukum internasional dalam menanggulangi kasus cyber crime di Indonesia. Meskipun seperti itu, peran hukum internasional masih dibutuhkan untuk memaksimalkan peluang kerjasama internasional yang dilakukan oleh pihak berwenang dalam melawan kasus kejahatan siber.

Kata Kunci: *hukum internasional, cyber crime, cyber attack, kerjasama, harmonisasi.*

PENDAHULUAN

Cyber security atau kejahatan siber adalah jenis kejahatan yang memanfaatkan ruang siber atau *cyberspace* dan kemajuan Teknologi Informasi dan Komunikasi dalam melancarkan aksinya (Septasari, 2023). Kejahatan siber merupakan kejahatan yang bersifat lintas batas negara atau *cross-boundaries*, sehingga dalam menangani kejahatan siber dibutuhkan pendekatan yang terpadu dan memiliki koordinasi yang baik antar negara-negara di tingkat internasional. Hukum internasional mengambil posisi yang krusial dalam menangani kasus *cyber crime* dan menjadi kerangka hukum yang menjadi dasar dalam kerja sama antara negara-negara dalam menangani kasus kejahatan ini. Dengan hukum internasional, prinsip-prinsip seperti pencegahan, investigasi, dan penuntutan kejahatan siber dapat dijadikan pijakan bagi tiap negara untuk diikuti dan dijadikan sebuah standar. Sementara itu, hukum internasional dapat menjadi pedoman bagi tiap negara dalam menyelaraskan *national interest* agar tercipta harmonisasi yang berujung pada pendukungan dalam penanganan *cyber crime*. Meskipun seperti itu, upaya harmonisasi merupakan tantangan yang besar karena setiap negara memiliki perspektif yang berbeda-beda yang dipengaruhi faktor sejarah dan budayanya. Bahkan pada tingkat nasional, harmonisasi dapat menemui masalah yang diakibatkan antara pemerintah pusat dengan pemerintah provinsi (Clough, 2015).

Seperti kejahatan siber yang baru-baru ini terjadi, hal ini menimpa Pusat Data Nasional Sementara (PDNS) di Surabaya, Jawa Timur. Hasil pencarian menunjukkan bahwa serangan siber tersebut disebabkan oleh *ransomware brain chiper*, varian dari *ransomware* Lockbit 3.0. *Ransomware* sendiri merupakan jenis malware yang dirancang sedemikian rupa untuk dapat merusak atau menyusup ke sistem komputer dan mengancam korban untuk membayar tebusan. Sementara itu, Lockbit sendiri merupakan sekelompok peretas yang diduga berasal dari Rusia yang sebelumnya bertanggung jawab atas lumpuhnya layanan Bank Syariah Indonesia (BSI) pada Mei 2023 (Indonesia, 2024). Dalam konteks internasional, pada tanggal 30 November 2016, sebuah jaringan kejahatan siber bernama *Avalanche* berhasil ditumpas oleh kerjasama antara Kantor Jaksa Penuntut Umum Verden dan Polisi Lüneburg (Jerman) yang bekerja sama erat dengan Kantor Kejaksaan Amerika Serikat untuk Distrik Barat Pennsylvania, Departemen Kehakiman dan FBI, Europol, Eurojust dan Interpol (‘Avalanche’ Network Dismantled in International Cyber Operation, 2016).

Beberapa instrumen hukum internasional telah dikembangkan untuk menghadapi tantangan kejahatan siber. Salah satunya adalah konvensi Budapest tentang *cyber crime*, yang diadopsi oleh Dewan Eropa pada 23 November 2001 dan ditandatangani oleh 30 negara termasuk empat negara yang bukan anggota Dewan Eropa seperti Jepang, Amerika Serikat, Kanada, dan Afrika Selatan. Konvensi ini merupakan salah satu perjanjian internasional pertama yang berfokus pada kejahatan siber, dengan tujuan untuk mengharmonisasikan undang-undang nasional tiap negara, meningkatkan kerja sama internasional, dan memperkuat kapabilitas penegak hukum. Selain Konvensi Budapest, instrumen-instrumen lainnya seperti Perjanjian Ekonomi Asia-Pasifik (APEC) tentang *cyber crime* dan *cyber security* dan berbagai perjanjian ataupun resolusi yang diadopsi oleh Perserikatan Bangsa-Bangsa (PBB) yang mendukung upaya dunia internasional dalam menanggulani kejahatan siber (Union, 2017). Meskipun dunia internasional saat ini telah mengadopsi berbagai hukum internasional, tetapi dalam penerapannya masih menghadapi tantangan. Perbedaan hukum dan sistem peradilan di berbagai negara menjadi salah satu tantangan terbesar. Setiap negara memiliki kerangka hukum yang berbeda, sehingga perbedaan ini menjadi hambatan dalam penerapan hukum internasional atau kerjasama internasional. Selain itu, kurangnya harmonisasi kebijakan nasional dengan standar internasional juga menjadi masalah. Beberapa negara yang masih belum dapat menyelaraskan undang-undang nasional mereka dengan konvensi internasional menyebabkan kesulitan dalam penegakan hukum lintas batas negara. Tantangan teknis juga tidak kalah penting, dimana pelacakan dan pembuktian kejahatan siber lintas negara sering kali rumit dan memerlukan teknologi yang canggih serta

kerjasama yang erat antara berbagai yurisdiksi (Casey, 2011).

Kerja sama internasional memegang peranan penting dalam menangani kejahatan siber. Efektivitas dari kerja sama dapat dilihat dari kemampuan negara-negara untuk berbagi informasi, sumber daya, dan keahlian dalam menangani kejahatan siber. Misalnya, melalui jaringan kerja sama Interpol dan Europol, negara-negara dapat mengkoordinasikan upaya penegakan hukum dan berbagi intelijen terkait aktivitas kejahatan siber. Selain itu, perjanjian ekstradisi dan bantuan hukum timbal balik sangat penting untuk memastikan bahwa pelaku kejahatan siber dapat dituntut di negara yang memiliki yurisdiksi. Namun, untuk meningkatkan efisiensi kerja sama internasional, ada banyak tantangan yang harus diatasi. Ini termasuk menumbuhkan kepercayaan antar negara dan memastikan bahwa setiap negara memiliki kapasitas yang memadai untuk berpartisipasi dalam upaya global (Brenner, 2012).

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif-analitis. Data dikumpulkan melalui studi literatur dari berbagai sumber seperti buku, jurnal, artikel ilmiah, dan dokumen hukum internasional terkait cybercrime. Analisis data dilakukan dengan mengidentifikasi dan mengevaluasi peran, instrumen, dan tantangan hukum internasional dalam menangani kasus cybercrime.

HASIL DAN PEMBAHASAN

Peran Hukum Internasional

Hukum internasional berperan penting dalam menyediakan kerangka kerja yang komprehensif untuk penanggulangan *cyber crime* melalui berbagai instrumen hukum seperti konvensi, traktat, dan perjanjian bilateral atau multilateral. Kerangka kerja ini menetapkan aturan dan mekanisme yang memungkinkan negara-negara untuk bekerja sama dalam menghadapi ancaman kejahatan siber yang semakin kompleks dan lintas batas. Dengan adanya konvensi dan traktat internasional, negara-negara dapat mengoordinsikan upaya penegakan hukum, berbagi informasi intelijen, dan menyusun kebijakan keamanan siber yang efektif. Salah satu contoh utama dari instrumen ini adalah Konvensi Budapest tentang *cyber crime*, yang diadopsi oleh *Council of Europe* pada tahun 2001 dan telah diratifikasi oleh 75 negara hingga tahun 2024. Konvensi ini menetapkan standar kriminalisasi untuk berbagai jenis kejahatan siber dan mengatur mekanisme kerja sama internasional yang efisien dalam penyelidikan dan penuntutan kejahatan siber. Melalui kerangka hukum internasional ini juga, komunitas global dapat bekerja sama untuk menanggulangi *cyber crim*e secara lebih efektif, memastikan bahwa pelaku kejahatan siber dapat dituntut dan diadili di mana pun mereka berada, serta upaya penegakan hukum yang terkoordinasi di tingkat internasional (Council of Europe, 2001).

Instrumen Hukum Internasional

Salah satu instrumen hukum internasional yang ada dalam menangani kejahatan siber adalah *Convention on Cybercrime* atau yang dikenal sebagai Konvensi Budapest. Konvensi Budapest diadopsi oleh Dewan Eropa pada tanggal 23 November 2001 dan diratifikasi oleh banyak negara pada saat itu. Konvensi ini mencakup banyak aspek yang membahas tentang kebijakan kriminal, dengan tujuan melindungi masyarakat dunia dari kejahatan siber. Ada beberapa pertimbangan mengapa Konvensi Budapest dibentuk, antara lain adalah masyarakat internasional telah sadar bahwa diperlukan adanya kerjasama antar negara dan lembaga terkait untuk memerangi kejahatan siber dan melindungi kepentingan yang ada didalam suatu negara, diperlukan adanya kepastian hukum dalam proses penyelidikan dan penuntutan baik di dalam negeri maupun di luar negeri melalui mekanisme kerjasama internasional yang cepat dan mudah diakses, dan semakin jelas bahwa ada kebutuhan untuk menjamin bahwa penegakkan Hukum Asasi Manusia (HAM) sesuai dengan Konvensi PBB tahun 1996 tentang hak politik dan sipil, yang melindungi kebebasan berpendapat, termasuk kebebasan untuk mendapatkan, menerima, dan berbagi informasi (Fadhillah et al., 2023).

Konvensi tersebut mengklasifikasikan pelanggaran menjadi lima kategori: *Pertama*, mencakup pemalsuan kerahasiaan, integritas, dan ketersediaan data. *Kedua*, terkait dengan

pelanggaran dalam menggunakan Teknologi Informasi dan Komunikasi (TIK). *Ketiga*, mencakup pelanggaran seperti produksi dan distribusi pornografi anak. Keempat, pelanggaran terkait hak cipta dan kelima, mencakup tanggung jawab seperti tanggung jawab perusahaan atas pelanggaran atas nama badan hukum. Konvensi ini telah diratifikasi oleh negara-negara di Uni Eropa, negara di luar Uni Eropa, seperti Amerika Serikat. Konvensi Budapest membuat negara-negara yang meratifikasi memiliki kepentingan untuk melindungi keamanan dunia siber dari *cyber crime* (Fadhillah et al., 2023).

Selain Konvensi Budapest, dalam konteks hukum yang mengatur ruang siber atau *cyberspace*. Diperlukan sebuah landasan hukum yang mengatur tentang hal itu, hukum itu biasa disebut *cyber law*. *Cyber law* adalah hukum yang mengatur berbagai aspek terkait entitas hukum yang memanfaatkan teknologi internet. Di Indonesia sendiri, tindakan-tindakan yang menyalahi aturan dalam dunia siber sudah diatur dalam Undang-Undang Nomor 19 Tahun 2016 yang merupakan perubahan dari Undang-Undang Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-Undang tersebut mengatur tentang penggunaan komputer dan sarana elektoronik lainnya. Tetapi kejahatan siber merupakan kejahatan lintas batas negara (*cross boundaries*). Oleh karena itu, jika hukum nasional masih belum dapat digunakan dalam menangani kasus kejahatan seperti ini, maka prinsip-prinsip hukum internasional akan digunakan sebagai acuan (Septasari, 2023).

Tantangan dalam Penerapan Hukum Internasional

Salah satu tantangan yang ada dalam penerapan hukum internasional adalah perbedaan hukum dan sistem peradilan di berbagai negara. Setiap negara memiliki hukum dan sistem peradilannya masing-masing, tidak terkecuali Indonesia dan Amerika Serikat, hal ini membuat mengadili kejahatan siber lintas negara menjadi rumit untuk penyelesaiannya, oleh karena itu kita harus memahami apa perbedaan hukum di berbagai negara, pada bagian ini kami membandingkan hukum dan sistem peradilan Indonesia dan Amerika Serikat.

Sistem hukum peradilan pidana di Indonesia menggunakan sistem akusator sebagaimana tertuang pada Undang-undang No 8 Tahun 1981 tentang Kitab Undang-undang Hukum Acara Pidana, sistem akusator adalah sistem pembuktian permasalahan pidana sesuai kepada pembuktian nyata serta ilmiah lalu sistem peradilan di Indonesia juga terpengaruh oleh due proses model, yaitu: pelaksanaan hukum yang adil dan layak serta penetapan hak-hak tersangka/terdakwa (Soediro, 2019). Indonesia menggunakan KUHAP yang di mana menggunakan asas *Presumption of Innocent*, asas yang sering dipakai pada Model due process model, jadi Indonesia tidak menggunakan asas *Presumption of Guilty*, yang sering digunakan pada model *crime control model* (Soediro, 2019).

Sistem hukum peradilan di Amerika Serikat mempunyai dan melewati beberapa tahap, tahap-tahap tersebut adalah, tahap sebelum pemeriksaan persidangan, tahap ini terdiri dari penahanan, kehadiran di depan hakim, pendengaran pendapat awal, pelaksanaan atau proses juri agung, pemanggilan terdakwa, dan pernyataan bersalah. Setelah melewati tahap tersebut barulah masuk ke tahap berikutnya yaitu, tahap pemeriksaan persidangan yang terdiri dari memilih para juri, pernyataan pembuka, alasan hukum jaksa penuntut, alasan hukum terdakwa/ kuasa hukum, arahan juri, dan hasil putusan juri. Tahap terakhir adalah tahap setelah pemeriksaan sidang, tahap ini terdiri dari keputusan hukuman, permintaan banding, pelaksanaan eksekusi (Soediro, 2019). Dalam pelaksanaan peradilan pidana di Amerika Serikat, mereka memakai dua model dalam prosesnya, yaitu *due process model* dan *crime control model* (Soediro, 2019). Dalam konteks *cyber crime*, Amerika Serikat dan Indonesia masing-masing mempunyai cara penanggulangan mereka sendiri, Amerika Serikat dengan *Computer Crime and Intellectual Property Section* (CCIPS) dan *National Infrastructure Protection Center* (NIPC). Indonesia mempunyai Pasal 362 KUHP, Pasal 282 dan 311 KUHP, lalu Pasal 378 dan 362 (Arifah, 2011).

Kurangnya harmonisasi kebijakan nasional dengan standar internasional juga menjadi tantangan dalam penerapan hukum internasional dalam menanggulangi kejahatan siber. Dalam dunia internasional sudah terdapat banyak organisasi dan konvensi atau perjanjian internasional mengenai *cyber crime* ini, salah satunya adalah Konvensi Budapest. Pada Konvensi Budapest sudah terdapat banyak hukum serta cara untuk mengatasi *cyber crime*, tetapi jika ingin memberlakukan hal tersebut suatu negara harus meratifikasi Konvensi Budapest, sayangnya Indonesia tidak meratifikasi Konvensi Budapest, jika Indonesia meratifikasi Konvensi Budapest, maka bisa terciptanya harmonisasi hukum. Penyatuan atau harmonisasi antara hukum nasional dengan internasional harus dilakukan untuk menciptakan solusi dalam mengatasi permasalahan antar negara yang muncul dikarenakan adanya interaksi antar negara. Upaya penyatuan dan harmonisasi hukum ini dapat dilakukan melalui penyesuaian aspek-aspek tatanan hukum nasional yang meliputi substansi hukum, struktur hukum, dan budaya hukum degan sistem hukum internasional (Chalim, 2018).

Dalam mengatasi kejahatan siber lintas negara, terdapat beberapa tantangan yaitu, kurangya batas yuridiksi teritorial, karena internet adalah tempat ekstrateritorial, dan pelaku kejahatan siber tidak lagi terbatas pada peretas individu saja, tantangan berikutnya adalah kurangnya kerangka regulasi kejahatan dunia maya yang sejenis, harus ada kerangka struktur dan regulasi dengan peraturan yang sejemis untuk mengatasi kejahatan siber, tantangan terakhir adalah evolusi kejahatan pada dunia maya atau internet, karena upaya legislatif untuk memerangi kejahatan siber tidak terlalu efisien dikarenakan pembuatan undang-undang kalah cepat dengan taktik kriminal yang dinamis serta evolusi cepat dari dunia maya (Iu & Wong, 2022).

Efektivitas Kerjasama Internasional dengan Studi Kasus Avalanche

Jika bicara tentang kerja sama internasional dalam menangani kasus kejahatan siber, dunia internasional telah banyak melakukan upaya untuk melakukan pencegahan atas tindakan kejahatan siber. Seperti diantaranya adalah Konvensi Budapest yang diresmikan oleh Dewan Eropa pada 23 November 2001 dan forum internasional seperti Interpol atau *International Criminal Police Organization* (ICPO). Tetapi upaya-upaya tersebut tidak selamanya berjalan sebagaimana mestinya karena masih terdapat banyak tantangan dalam implementasi hukum yang melibatkan banyak negara atau lintas batas negara (*cross-boundaries)*. Hal itu disebabkan tiap-tiap negara memiliki perspektif budaya, sejarah dan hukum yang berbeda-beda (Clough, 2015). Meski begitu, masih terdapat upaya-upaya yang berhasil dalam menumpas kejahatan siber yang melibatkan banyak pihak atau operasi bersama. Upaya tersebut adalah operasi *Avalanche* pada tahun 2016.

Setelah melakukan berbagai penyelidikan yang memakan waktu lebih dari empat tahun, tim gabungan yang terdiri dari polisi Lüneburg dan jaksa penuntut umum Jerman bekerja sama dengan pihak berwenang Amerika Serikat, FBI, Europol, Eurojust dan mitra global lainnya termasuk Interpol, telah berhasil membongkar jaringan kriminal internasional yang dikenal sebagai "*Avalanche*". Operasi yang berlangsung tepat pada 30 November 2016 tersebut berhasil mengkoordinasi aksi dalam satu hari yang melibatkan 30 negara, 800.000 lebih domain disita dan diblokir. Tidak hanya itu, lima orang ditangkap, 37 tempat digeledah dan 39 server disita, dengan 221 server lainnya dinonaktifkan. 180 negara juga diidentifikasi menjadi korban infeksi *malware* yang diakibatkan oleh komunitas ini. Pada hari aksi tersebut, pos komando Europol yang berada di Den Haag, Belanda, menjadi pusat koordinasi. Dari pusat komando tersebut, perwakilan dari negara-negara yang terlibat bekerja sama dengan *Europol's European Cybercrime Centre* (EC3) dan pejabat Eurojust berkumpul untuk memastikan keberhasilan operasi skala besar tersebut ('Avalanche' Network Dismantled in International Cyber Operation, 2016).

Dalam rangka menyiapkan aksi besar ini, Kantor Federal Jerman untuk Keamanan Informasi (BSI) dan *Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie* (FKIE) menganalisis 130 TB

(*TeraByte)* lebih data dan mengindetifikasi server botnet yang memungkinkan ribuan server ditutup, dinonaktifkan dan diruntuhkannya seluruh jaringan kriminal. Hasil investigasi yang dimulai sejak 2012 tersebut menemukan bahwa jaringan *Avalanche* diperkirakan menginfeksi 500.000 komputer di seluruh dunia setiap harinya. Selain itu, kerugian moneter yang diakibatkan dari kejahatan siber *Avalanche* diperkirakan mencapai ratusan juta euro, meski perhitungan pastinya sulit didapatkan karena tingginya jumlah keluarga *malware* yang dikelola oleh platform. European Commissioner for the Security Union, Julian King mengatakan "*Avalanche* menunjukkan bahwa kita hanya bisa berhasil dalam memerangi kejahatan dunia maya ketika kita bekerja sama secara erat, lintas sektor dan lintas batas. Otoritas keamanan siber dan penegak hukum perlu bekerja bahu membahu dengan sektor swasta untuk mengatasi metode kriminal yang terus berkembang. Uni Eropa membantu dengan memastikan bahwa kerangka hukum yang tepat tersedia untuk memungkinkan kerja sama semacam itu setiap hari" ('Avalanche' Network Dismantled in International Cyber Operation, 2016).

Keberhasilan operasi tersebut memang tidak lepas dari adanya kerja sama internasional yang melibatkan aparat penegak hukum lintas batas negara (*cross boundaries)*. Meski begitu, dalam pelaksanaan penguatan keamanan siber semacam itu dibutuhkan beberapa faktor penting agar penguatan keamanan siber dapat lebih maksimal. *Pertama*, meningkatkan kemampuan pengetahuan *cyber*. Langkah meningkatkan pengetahuan dalam hal ini sangat penting dilakukan guna memberikan edukasi bagi setiap orang yang menggunakan *cyber space* dan diperlukan kerjasama dari semua pihak. Dalam sebuah negara, pemerintah memiliki tanggung jawab membangun komunitas keamanan siber dengan tujuan mencegah dan mengetahui potensi serangan siber sejak awal untuk memperkuat *cyber security* negara. *Kedua*, penguatan Undang-Undang dan hukum negara. Dalam konteks Indonesia, Undang-Undang Nomor 8 Tahun 2011 yang saat ini diubah menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Traknsaksi Elektronik (UU ITE) saat ini menjadi landasan hukum yang mengatur segala transaksi dan pelanggaran dalam penggunaan TIK (Teknologi Informasi dan Komunikasi). Selain itu, terdapat beberapa langkah yang dapat diambil untuk menguatkan keamanan siber, diantaranya adalah mengembangkan sistem informasi yang selalu *update* dengan perkembangan zaman, mengembangkan sumber daya manusia yang sadar akan pentingnya *cyber security*, dan turut menjadi agen perubahan dalam meningkatkan kesadaran dan pentingnya penggunaan teknologi yang positif (Septasari, 2023).

KESIMPULAN

Peran hukum internasional dalam menangani kasus *cyber crime* sangat penting meskipun masih menghadapi berbagai tantangan signifikan. Penelitian ini menunjukkan bahwa meskipun instrumen hukum internasional seperti Konvensi Budapest dan perjanjian multilateral lainnya memberikan kerangka kerja yang komprehensif, perbedaan hukum dan sistem peradilan diberbagai negara serta kurangnya harmonisasi kebijakan nasional dengan standar internasional menghambat efektivitas penerapannya. Selain itu, tantangan teknis dalam pelacakan dan pembuktian kejahatan siber lintas negara juga menjadi kendala utama. Namun, kerjasama internasional tetap esensial, dengan organisasi internasional seperti Interpol dan Europol memainkan peran penting dalam memfasilitasi koordinasi penegakan hukum dan berbagi informasi. Meskipun Indonesia belum meratifikasi Konvensi Budapest, hukum internasional masih sangat diperlukan untuk memaksimalkan peluang kerjasama internasional dalam melawan kejahatan siber. Dengan demikian, meskipun ada berbagai hambatan, kerjasama dan hukum internasional tetap memegang peranan kunci dalam upaya global mengatasi tantangan *cyber crime*.

DAFTAR PUSTAKA

Buku

Brenner, S. W. (2012). *Cyber crime and the law: Challenges, issues, and outcomes*. UPNE.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic Press.

Clough, J. (2015). *Principles of cyber crime*. Cambridge University Press.

Council of Europe. (2001). Convention on Cybercrime (ETS no. 185).

Union, I. T. (2017). *Understanding cyber crime: Phenomena, challenges and legal response*. United Nations.

Jurnal

Amalia Arifah, D. (2011). Kasus Cybercrime di Indonesia. *Jurnal Bisnis Dan Ekonomi*, *8*(2), 185–195.

Chalim, M. A. (2017). Harmonization Between The National And International Law On The Usage Settings Of Natural Resources In The Territory Of The Republic Of Indonesia. *Jurnal Pembaharuan Hukum*, 4(2), 191. https://doi.org/10.26532/jph.v4i2.1669

Fadhillah, S. A., Matakupan, M. S. A., & Mingga, B. W. B. (2023). Peran Interpol dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest On Cybercrimes. Journal on Education, 5(4), 16553–16564. https://doi.org/10.31004/joe.v5i4.2822

Iu, K. Y., & Wong, V. M.-Y. (2022). The trans-national cybercrime court: Towards a new harmonisation of cyber law regime in ASEAN. SSRN Electronic Journal, 5. https://doi.org/10.2139/ssrn.4265726

Septasari, D. (2023). The cyber security and the challenge of society 5.0 Era in Indonesia. *Aisyah Journal of Informatics and Electrical Engineering (A.J.I.E.E), 5*(2), 227–233. https://doi.org/10.30604/jti.v5i2.231

Soediro, S. (2019). Perbandingan Sistem Peradilan Pidana Amerika Serikat dengan Peradilan Pidana di Indonesia. *Kosmik Hukum*, *19*(1). https://doi.org/10.30595/kosmikhukum.v19i1.4083

Website

'Avalanche' network dismantled in international cyber operation. (2016, December 1). Europol. https://www.europol.europa.eu/media-press/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

Indonesia, B. N. (2024, June 27). PDNS: Pusat Data Nasional Sementara lumpuh akibat ransomware, mengapa instansi pemerintah masih rentan terhadap serangan siber? BBC News Indonesia. https://www.bbc.com/indonesia/articles/cxee2985jrvo