

Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional

Aisyah Putri Nabila¹, Nathania Aurell Manabung², Aquilla Cinta Ramadhansha³
^{1,2,3}Fakultas Hukum, Universitas Pembangunan Nasional, Surabaya, Indonesia

Article Info

Article history:

Received Januari 1, 2024

Revised Januari 2, 2024

Accepted Januari 9, 2024

Keywords:

Kejahatan Cyber,
Hukum Internasional,
Kerja Sama Internasional.

Keywords:

Cyber Crime,
International law,
International Cooperation.

ABSTRAK

Penelitian ini membahas urgensi penanganan kejahatan cyber dalam konteks hukum internasional. Perkembangan pesat teknologi informasi dan komunikasi telah membawa dampak signifikan dalam kehidupan sehari-hari, namun juga membuka pintu bagi kejahatan cyber. Kejahatan ini bersifat transnasional dan memerlukan kerja sama internasional. Instrumen hukum internasional, seperti Konvensi Budapest tentang Kejahatan Cyber serta memiliki peran penting dalam penanggulangan. Meskipun banyak negara telah mengadopsi instrumen ini, terdapat banyak tantangan terutama dalam meningkatkan kapasitas aparat penegak hukum. Penelitian ini menggunakan pendekatan kualitatif dengan fokus pada hukum normatif, menganalisis aspek-aspek kejahatan cyber dan upaya penanganannya melalui studi mendalam terhadap peraturan perundang-undangan dan literatur hukum terkait.

ABSTRACT

This research discusses the urgency of handling cyber crime in the context of international law. The rapid development of information and communication technology has had a significant impact on everyday life, but has also opened the door to cyber crime. This crime is transnational in nature and requires international cooperation. International legal instruments, such as the Budapest Convention on Cyber Crime, also have an important role in prevention. Although many countries have adopted this instrument, there are many challenges, especially in increasing the capacity of law enforcement officials. This research uses a qualitative approach with a focus on normative law, analyzing aspects of cyber crime and efforts to deal with it through in-depth study of legislation and related legal literature.

This is an open access article under the [CC BY](https://creativecommons.org/licenses/by/4.0/) license.



Corresponding Author:

Aisyah Putri Nabila

Fakultas Hukum, Universitas Pembangunan Nasional,
Surabaya, Indonesia

Email: aisyahputrinabila83@gmail.com

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) yang pesat telah membawa perubahan signifikan dalam kehidupan manusia. TIK telah meresap ke dalam setiap aspek kehidupan sehari-hari, memberikan dampak yang luar biasa dalam hal personal, sosial, dan

ekonomi. Namun, seiring dengan manfaatnya, kemajuan ini juga membuka pintu bagi kejahatan baru yang dikenal sebagai kejahatan *cyber* atau *cybercrime*. Kejahatan ini menggunakan teknologi informasi dan komunikasi untuk menyerang, memanipulasi, atau mencuri data dan informasi, menciptakan tantangan yang serius bagi keamanan digital [1]. Kejahatan *cyber* tidak terbatas oleh batas-batas geografis, mengingat pelaku dapat berada di negara yang berbeda dengan korban. Oleh karena itu, penanggulangan kejahatan ini memerlukan pendekatan yang melibatkan kerjasama internasional, dan inilah di mana peran hukum internasional menjadi sangat penting. Hukum internasional dapat menjadi landasan bagi negara-negara untuk bersama-sama mengatasi ancaman kejahatan *cyber* melalui berbagai upaya. Upaya penanggulangan kejahatan *cyber* semakin meningkat, dan salah satu strategi yang diterapkan adalah melalui pengembangan instrumen hukum internasional. Konvensi Budapest tentang Kejahatan *Cyber* (Budapest Convention on *Cybercrime*) menonjol sebagai contoh nyata instrumen hukum internasional yang memainkan peran sentral dalam upaya tersebut. Konvensi ini, yang telah diadopsi oleh lebih dari 60 negara, termasuk Indonesia, mencerminkan kerjasama global untuk mengatasi ancaman kejahatan siber yang semakin kompleks [2].

Dengan menjadi pihak dalam Konvensi Budapest, negara-negara anggota menetapkan dasar hukum bersama untuk menghadapi tantangan kejahatan *cyber*. Instrumen ini memberikan panduan yang sangat dibutuhkan bagi negara-negara tersebut dalam merumuskan dan menyempurnakan kerangka hukum nasional mereka terkait *cybercrime*. Keberadaan konvensi semacam ini membantu menciptakan kerangka hukum yang konsisten dan saling mendukung di tingkat internasional, sehingga memberikan dasar yang lebih kuat untuk kerjasama lintas batas dalam mencegah, menyelidiki, dan menuntut pelaku kejahatan siber. Selain itu, Konvensi Budapest juga memberikan landasan untuk pertukaran informasi internasional yang lebih efektif, memperkuat kerjasama di antara negara-negara anggota dalam menyikapi insiden kejahatan siber. Dengan demikian, instrumen hukum internasional ini tidak hanya menciptakan standar bersama tetapi juga meningkatkan kapasitas negara-negara dalam menangani ancaman yang dapat merugikan masyarakat global. Keberlanjutan dukungan terhadap inisiatif semacam ini menjadi kunci dalam menghadapi dinamika yang terus berkembang dalam ranah kejahatan *cyber* di era globalisasi ini [3]. Kerja sama antar negara menjadi kunci dalam menghadapi kejahatan *cyber* yang sering melibatkan pelaku dari wilayah yang berbeda. Interpol atau International Criminal Police Organization (ICPO) adalah salah satu forum internasional yang memungkinkan negara-negara untuk berkoordinasi dan bekerja sama dalam menanggulangi *cybercrime*. Dalam lingkungan ini, pertukaran informasi dan pengalaman dapat meningkatkan kemampuan bersama dalam mendeteksi, menyelidiki, dan menindaklanjuti kasus-kasus *cybercrime*.

Namun, untuk mencapai tingkat efektivitas yang maksimal, peningkatan kapasitas aparat penegak hukum sangat penting. Aparat penegak hukum perlu diberdayakan dengan pengetahuan dan keterampilan yang memadai untuk menangani kasus-kasus *cybercrime* yang semakin kompleks. Pelatihan dan pendidikan menjadi langkah kunci untuk memastikan bahwa aparat penegak hukum memiliki pemahaman mendalam tentang teknologi informasi dan komunikasi serta metode terbaru yang digunakan oleh pelaku kejahatan *cyber* [4]. Dengan demikian, hukum internasional memiliki peran yang sangat penting dalam menanggulangi kejahatan *cyber* yang bersifat transnasional. Melalui pengembangan instrumen hukum internasional, koordinasi dan kerja sama antar negara, serta peningkatan kapasitas aparat

penegak hukum, upaya bersama dapat dilakukan untuk menjaga keamanan dunia digital. Keseluruhan, ini adalah langkah-langkah yang memastikan bahwa perkembangan teknologi informasi dan komunikasi memberikan manfaat maksimal tanpa mengorbankan keamanan dan integritas data.

2. METODE

Penggunaan metode kualitatif, khususnya metode penelitian hukum normatif, menjadi pendekatan yang relevan dalam menyelidiki dan menganalisis fenomena hukum. Metode penelitian hukum normatif menitikberatkan pada kajian terhadap norma-norma hukum yang berlaku, baik itu di tingkat internasional maupun nasional. Dalam konteks penelitian ini, metode tersebut digunakan untuk mengungkap dan memahami substansi normatif yang menjadi dasar bagi peraturan perundang-undangan yang ada [5]. Proses penelitian ini melibatkan pemanfaatan sumber data sekunder, di antaranya adalah peraturan perundang-undangan, literatur hukum, dan putusan pengadilan. Penggunaan sumber data sekunder ini menjadi esensial dalam menggali informasi terkait norma hukum yang dijadikan fokus penelitian. Peraturan perundang-undangan memberikan pandangan terinci terkait norma yang diterapkan dalam suatu konteks hukum, sementara literatur hukum menyediakan wawasan mendalam terhadap pemikiran dan konsep-konsep hukum yang mendasari norma tersebut. Selain itu, putusan pengadilan juga menjadi sumber data kritis yang memberikan gambaran konkret tentang penerapan norma hukum dalam penyelesaian kasus-kasus hukum.

Dengan merangkum dan menganalisis sumber data tersebut, metode penelitian hukum normatif memberikan kontribusi yang berharga dalam membentuk pemahaman yang mendalam terhadap isu hukum yang sedang diteliti. Pendekatan ini membuka ruang untuk menjelajahi konsep-konsep hukum, perkembangan normatif, dan dampak implementasi norma hukum dalam kerangka kebijakan tertentu. Selain itu, metode kualitatif juga memungkinkan peneliti untuk memahami konteks sosial dan historis yang melingkupi norma-norma hukum tersebut, memberikan dimensi tambahan dalam memahami kompleksitas permasalahan hukum yang dihadapi [6]. Pengumpulan data dilakukan melalui studi mendalam terhadap peraturan perundang-undangan, literatur hukum, dan putusan pengadilan yang terkait dengan masalah yang diteliti. Analisis data merupakan tahap penting, di mana peneliti mengkaji dan menginterpretasi informasi yang telah dikumpulkan. Dalam konteks penelitian hukum normatif tentang peran hukum internasional dalam menanggulangi *cyber crime* pada kejahatan transnasional, peneliti dapat memilih asas-asas hukum internasional yang relevan, seperti asas teritorial, asas nasionalitas, dan asas universalitas, sebagai kerangka teori [7].

Dengan demikian, metode penelitian hukum normatif menjadi pilihan yang tepat untuk menggali pemahaman mendalam mengenai peran hukum internasional dalam menanggulangi *cyber crime* pada kejahatan transnasional, asalkan peneliti memiliki pengetahuan yang mendalam tentang hukum.

3. HASIL DAN PEMBAHASAN

3.1 Kejahatan Transnasional

Kejahatan transnasional sebagai fenomena yang melibatkan dua negara atau lebih, memiliki dampak dan konsekuensi yang dirasakan oleh negara-negara yang terlibat. Unsur-unsur utama yang membedakan kejahatan transnasional dari kejahatan biasa adalah keberadaan

unsur lintas negara, transnationality, dan keberadaan kelompok kejahatan yang terorganisir. Keberadaan unsur lintas negara menunjukkan bahwa kejahatan tersebut melibatkan lebih dari satu negara, sedangkan unsur transnationality menekankan bahwa dampak atau konsekuensi dari kejahatan ini dirasakan oleh negara lain. Selain itu, banyak kejahatan transnasional dilakukan oleh kelompok kejahatan terorganisir [8]. Kejahatan transnasional menjadi ancaman serius terhadap keamanan dan kesejahteraan global, mencakup berbagai bentuk seperti kejahatan narkoba, terorisme, perdagangan orang, pencucian uang, korupsi, penyelundupan, serta kejahatan terhadap kehutanan dan satwa liar. Fenomena ini melibatkan jaringan internasional yang terorganisir, memperumit upaya penanggulangan dan menimbulkan dampak yang meluas. Kejahatan narkoba, sebagai salah satu bentuk utama, memberikan tekanan besar pada sistem kesehatan global dan menyebabkan degradasi sosial di banyak negara. Ancaman terorisme, yang bersifat lintas batas, membutuhkan koordinasi keamanan internasional yang erat untuk mencegah dan menanggulangi potensi ancaman terhadap masyarakat global.

Kejahatan perdagangan orang dan pencucian uang juga memiliki konsekuensi serius pada tingkat global. Perdagangan orang merugikan hak asasi manusia dan menciptakan krisis kemanusiaan, sedangkan pencucian uang memfasilitasi keberlanjutan kejahatan dengan menyamarkan jejak finansial. Korupsi, penyelundupan, dan kejahatan terhadap kehutanan serta satwa liar memberikan dampak negatif terhadap lingkungan dan keberlanjutan ekosistem global. Dengan demikian, kejahatan transnasional tidak hanya mengancam keamanan fisik, tetapi juga melibatkan kerusakan sosial, ekonomi, dan lingkungan yang dapat berdampak jangka panjang terhadap kesejahteraan seluruh dunia [9]. Upaya bersama dan kerjasama internasional menjadi kunci dalam menanggulangi kejahatan transnasional ini. Koordinasi antarnegara dalam pertukaran informasi, pengembangan strategi bersama, serta penegakan hukum yang kuat diperlukan untuk merespons dan mencegah bentuk-bentuk kejahatan transnasional ini secara efektif [10]. Penegakan hukum terhadap kejahatan transnasional memerlukan kerja sama antar negara, mengingat kelompok kejahatan terorganisir memiliki jaringan yang luas dan sering kali melibatkan lebih dari satu yurisdiksi. Untuk itu, terdapat instrumen hukum internasional yang mengatur tentang kejahatan transnasional, seperti Konvensi PBB tentang Pemberantasan Kejahatan Transnasional Terorganisir dan Konvensi PBB tentang Pencegahan dan Pemberantasan Kejahatan Genosida [11]. Di tingkat nasional, Indonesia juga telah mengatur pemberantasan kejahatan transnasional dalam berbagai peraturan perundang-undangan, seperti:

1. Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi [12].
2. Undang-Undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang [13].
3. Undang-Undang Nomor 35 Tahun 2009 tentang Narkoba.
4. Undang-Undang Nomor 8 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Dalam konteks analisis, kejahatan transnasional bukan hanya menyebabkan kerugian materil, seperti kerugian ekonomi akibat perdagangan narkoba atau pencucian uang, tetapi juga berdampak secara sosial dan politik. Kejahatan ini dapat menyebabkan ketidakstabilan politik dan keamanan di suatu negara karena sering kali dilakukan oleh kelompok terorganisir yang memiliki jaringan luas [14].

Upaya pencegahan dan penanganan kejahatan transnasional memerlukan strategi yang melibatkan kerja sama antar negara. Pertukaran informasi, kerja sama dalam penegakan hukum, dan kerja sama dalam upaya pencegahan menjadi kunci dalam menghadapi ancaman kejahatan transnasional. Diperlukan kesadaran global dan komitmen bersama untuk menciptakan dunia yang lebih aman dan damai. Seiring dengan itu, penelitian dan analisis yang mendalam terhadap peran hukum internasional dan nasional dalam menanggulangi kejahatan transnasional menjadi penting untuk mengembangkan strategi efektif dalam mengatasi fenomena ini [15].

3.2 Jenis-jenis Kejahatan Terorganisasi Transnasional

Kejahatan terorganisasi transnasional menjadi salah satu bentuk ancaman serius yang menghantui masyarakat dan ekonomi di tingkat global. Dalam konteks ini, kelompok kejahatan yang terstruktur dan terorganisir memainkan peran sentral dalam merencanakan dan melaksanakan berbagai tindakan kejahatan yang melibatkan aktivitas lintas batas negara. Dampak yang dihasilkan oleh kejahatan semacam ini tidak hanya terbatas pada aspek keamanan, tetapi juga melibatkan dimensi ekonomi yang signifikan. Beberapa jenis kejahatan terorganisasi transnasional yang paling umum melibatkan perdagangan narkoba, penyelundupan manusia, pencucian uang, kejahatan siber, dan kejahatan lingkungan. Perdagangan narkoba, misalnya, seringkali melibatkan jaringan yang sangat terorganisir, yang tidak hanya mencakup produksi dan distribusi narkoba, tetapi juga aktivitas pencucian uang yang kompleks. Pencucian uang, dalam konteks kejahatan terorganisasi, menjadi sarana untuk menyamarkan jejak finansial dari kegiatan ilegal mereka. Keberadaan dan aktivitas kejahatan terorganisasi transnasional menekankan perlunya kerjasama internasional yang erat dalam menanggulangi ancaman tersebut. Kolaborasi antarnegara dalam pertukaran intelijen, koordinasi tindakan penegakan hukum, dan pembangunan kerangka hukum bersama menjadi kunci untuk menghadapi tantangan ini. Seiring dengan berkembangnya kompleksitas kejahatan terorganisasi, upaya bersama di tingkat global menjadi semakin penting untuk memastikan keamanan dan kestabilan dunia.

Perdagangan narkoba, sebagai salah satu kejahatan terorganisasi transnasional yang paling merugikan, melibatkan produksi, distribusi, dan penjualan narkoba secara ilegal. Dampaknya sangat merugikan, mencakup peningkatan kriminalitas, kerusakan kesehatan masyarakat, dan kemiskinan. Sementara itu, penyelundupan manusia melibatkan perpindahan orang secara ilegal untuk tujuan eksploitasi, seringkali melibatkan kekerasan dan ancaman yang mengakibatkan penderitaan fisik dan mental bagi korban [16]. Pencucian uang menjadi kegiatan yang umum dilakukan oleh kelompok terorganisir untuk menyembunyikan asal-usul uang yang diperoleh secara ilegal. Kejahatan siber, dengan menggunakan teknologi informasi dan komunikasi, mencakup berbagai aktivitas seperti penipuan, pembajakan, dan penyebaran malware. Kejahatan lingkungan, yang mencakup perusakan atau pencemaran lingkungan, termasuk perburuan liar, pembalakan ilegal, dan perdagangan ilegal flora dan fauna. Dalam menghadapi kejahatan terorganisasi transnasional, ada berbagai instrumen hukum internasional yang bertujuan untuk menanggulangi kejahatan tersebut. Konvensi PBB Menentang Kejahatan Terorganisasi Transnasional (UNTOC) merupakan salah satu instrumen utama yang mengatur definisi dan standar hukum minimum untuk penanggulangan kejahatan terorganisasi transnasional. Instrumen lainnya mencakup UN Drug Convention, UN Firearms Convention,

dan UN Human Trafficking Convention yang masing-masing mengatasi aspek perdagangan narkoba, senjata api ilegal, dan penyelundupan manusia.

Kejahatan terorganisasi transnasional mengungkapkan bahwa kejahatan ini bukan hanya menimbulkan kerugian materil seperti kerusakan ekonomi atau pencucian uang, tetapi juga mengancam kesejahteraan sosial dan politik. Untuk mengatasi ancaman ini, kerja sama internasional menjadi kunci. Penegakan hukum yang kuat, koordinasi internasional, dan pengembangan kebijakan yang efektif menjadi langkah-langkah strategis yang perlu diambil oleh negara-negara dalam menghadapi kejahatan terorganisasi transnasional. Upaya pencegahan dan penanganan kejahatan terorganisasi transnasional memerlukan kebijakan yang terarah dan komitmen global. Penegakan hukum yang efektif, koordinasi internasional yang kuat, dan pengembangan kebijakan preventif menjadi landasan dalam menjawab tantangan ini. Dengan demikian, kejahatan terorganisasi transnasional dapat diatasi, dan masyarakat global dapat dijaga dari dampak negatif yang ditimbulkannya.

3.3 Kejahatan *Cyber* Dalam Interpretensi Kejahatan Tingkat Internasional

Kejahatan *cyber* sebuah bentuk kejahatan yang menggunakan teknologi informasi dan komunikasi seperti komputer, internet, dan jaringan telekomunikasi, telah menjadi ancaman serius di era globalisasi ini. Kejahatan ini melibatkan berbagai tindakan, termasuk penipuan, pencurian data, peretasan, dan penyerangan siber, yang semuanya dilakukan secara daring. Dalam konteks interpretasi kejahatan tingkat internasional, kejahatan *cyber* secara jelas dapat dikategorikan sebagai kejahatan transnasional [17]. Analisis mendalam terhadap kejahatan *cyber* mengungkapkan beberapa karakteristik khas yang membedakannya dari kejahatan konvensional. Pertama, adalah globalitas kejahatan ini. Kemampuannya untuk dilakukan dari mana saja di dunia membuatnya sulit untuk dilacak dan dihukum. Pelaku kejahatan *cyber* dapat dengan mudah menyusup melintasi batas negara, menciptakan tantangan serius dalam penegakan hukum. Kedua, anonimitas menjadi ciri khas lainnya. Pelaku kejahatan *cyber* dapat menyembunyikan identitas mereka di balik layar dunia maya, menjadikannya sulit diidentifikasi oleh pihak berwenang. Hal ini memberikan mereka keleluasaan untuk beroperasi tanpa takut terkena sanksi hukum, memperumit upaya penindakan. Ketiga, kompleksitas kejahatan *cyber* merupakan hambatan tambahan. Keahlian teknis yang tinggi yang sering diperlukan untuk melancarkan kejahatan ini membuatnya sulit untuk diinvestigasi dan diadili. Keberagaman metode serangan, mulai dari serangan phishing hingga malware, menambah tingkat kesulitan dalam penegakan hukum.

Meskipun belum ada perjanjian internasional yang secara spesifik mengatur kejahatan *cyber*, beberapa instrumen hukum dapat diterapkan. Konvensi Internasional untuk Memerangi Kejahatan Transnasional Terorganisir, Konvensi untuk Memerangi Kejahatan Informasi, dan Konvensi Internasional untuk Mencegah dan Menanggulangi Kejahatan *Cyber* adalah beberapa contoh yang memberikan kerangka hukum untuk menangani kejahatan ini secara global [18]. Di banyak negara, respons terhadap ancaman kejahatan siber tercermin dalam adopsi undang-undang yang dirancang khusus untuk mengatasi fenomena ini. Salah satu contohnya adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, yang memberikan kerangka hukum bagi penanganan tindak kejahatan siber di tingkat nasional. UU ITE ini mencakup berbagai ketentuan yang mengatur keamanan informasi, privasi data, serta sanksi bagi pelanggaran terhadap keamanan dunia maya. Di Amerika Serikat, Computer Fraud and

Abuse Act (CFAA) menjadi instrumen hukum utama dalam menanggulangi kejahatan siber, dengan fokus pada pemakaian ilegal terhadap komputer dan jaringan [19]. Selain itu, sejumlah negara juga telah mengadopsi undang-undang serupa untuk melindungi masyarakat mereka dari ancaman kejahatan siber. Di Inggris, sebagai contoh, Data Protection Act memberikan dasar hukum yang kuat terkait dengan perlindungan data pribadi dan keamanan informasi. Undang-undang semacam itu memberikan landasan hukum yang kokoh untuk penegakan hukum dan menjamin bahwa pelaku kejahatan siber dapat dihadapkan pada konsekuensi hukum yang serius. Meskipun undang-undang tersebut memberikan dasar hukum yang diperlukan, tantangan utama tetap ada pada penegakan hukum dan penanggulangan kejahatan secara efektif. Oleh karena itu, kerjasama internasional dan upaya bersama antarnegara menjadi penting dalam menghadapi ancaman kejahatan siber yang tidak mengenal batas wilayah.

Meskipun sudah ada upaya hukum yang signifikan, tantangan utama yang dihadapi oleh banyak negara tetap terletak pada efektivitas penegakan hukum dan penanggulangan kejahatan *cyber*. Kecepatan perkembangan teknologi dan kompleksitas serangan *cyber* membuat penegakan hukum menjadi tugas yang semakin sulit. Oleh karena itu, negara-negara perlu terus memperbarui kebijakan dan praktik penegakan hukum mereka agar sesuai dengan dinamika yang terus berubah dalam ranah kejahatan siber. Selain peran penegakan hukum, kerjasama internasional juga menjadi faktor kunci dalam menanggulangi kejahatan *cyber* yang melintasi batas negara. Negara-negara tersebut perlu bekerja sama dalam pertukaran informasi, pengembangan teknologi keamanan, dan koordinasi tindakan untuk merespons serangan *cyber*. Melalui inisiatif global ini, diharapkan dapat dibangun fondasi yang kuat untuk menanggapi tantangan keamanan siber yang bersifat transnasional dan menjaga stabilitas dunia maya secara keseluruhan. Kejahatan *cyber* adalah ancaman nyata yang membutuhkan respons serius di tingkat internasional. Kerja sama erat antar negara, peningkatan teknologi keamanan, dan pendidikan masyarakat menjadi kunci dalam melawan kejahatan ini. Dengan menghadapi tantangan ini bersama-sama, masyarakat global dapat menciptakan lingkungan digital yang lebih aman dan terlindungi.

3.4 Kedudukan Kejahatan Cyber Dalam Perkembangan Hukum Internasional Pada Saat Ini

Sebagai manifestasi tindak pidana yang memanfaatkan teknologi informasi dan komunikasi (TIK), kejahatan *cyber* telah mengalami perkembangan pesat dalam beberapa dekade terakhir. Dalam konteks hukum internasional, kejahatan ini merupakan tantangan baru yang menuntut perhatian serius dari komunitas internasional. Dampak yang luas dari kejahatan *cyber*, tidak hanya terbatas pada tingkat individu, melainkan juga mencakup masyarakat, negara, bahkan perdamaian dunia, menjadikannya sebagai fenomena kejahatan internasional kontemporer yang signifikan [20]. Kejahatan *cyber* memiliki sifat lintas batas yang membuat penegakan hukum menjadi sulit dilakukan. Kemampuannya untuk dilakukan dari berbagai sudut dunia dan tanpa batasan geografis memberikan pelaku kejahatan *cyber* kebebasan dan keberanian untuk melanggar hukum tanpa takut terkena sanksi di negara asal atau tempat kejahatan dilakukan. Hal ini menjadikan penegakan hukum internasional terkait kejahatan *cyber* semakin kompleks dan membutuhkan kerja sama yang erat antara negara-negara di seluruh dunia. Kejahatan *cyber* juga memiliki sifat abstrak yang menimbulkan kesulitan dalam definisi dan klasifikasinya. Dinamika dunia maya yang terus berkembang membuat kejahatan

ini sulit untuk didefinisikan dengan tepat, dan seringkali tergantung pada konteksnya. Oleh karena itu, pemahaman bersama tentang apa yang termasuk ke dalam kategori kejahatan *cyber* menjadi penting dalam membentuk dasar hukum yang efektif.

Dampak yang luas dari kejahatan *cyber* terhadap berbagai pihak, mulai dari individu hingga tingkat nasional dan internasional, membuatnya menjadi isu yang kompleks dan mendesak. Pencurian data pribadi, penipuan, penyebaran hoaks, dan serangan siber merupakan beberapa bentuk kejahatan *cyber* yang dapat merugikan secara materiil dan imateriil. Untuk menghadapi tantangan ini, komunitas internasional perlu merancang dasar hukum yang kuat. Seiring dengan meningkatnya ancaman kejahatan *cyber*, komunitas internasional telah merespons dengan mengenalkan berbagai instrumen hukum untuk melawan fenomena ini. Sejumlah perjanjian internasional, seperti Konvensi PBB tentang Kejahatan Siber, Konvensi Amerika tentang Kejahatan Siber, dan Konvensi ASEAN tentang Kejahatan Siber, telah diperkenalkan untuk mengatasi tantangan keamanan siber ini baik di tingkat global maupun regional. Dengan adanya kerangka kerja ini, negara-negara berusaha bersama-sama menanggulangi ancaman serangan siber yang melibatkan kejahatan seperti peretasan data dan serangan terhadap infrastruktur kritis. Di tingkat nasional, Indonesia telah mengadopsi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai respons terhadap kejahatan *cyber* di dalam negeri. Undang-Undang ini memberikan landasan hukum yang diperlukan untuk mengatur berbagai aspek yang terkait dengan keamanan siber dan transaksi elektronik. Dengan demikian, penguatan hukum ini diharapkan dapat memberikan perlindungan lebih baik terhadap masyarakat dan entitas bisnis dari potensi ancaman kejahatan *cyber* yang semakin kompleks dan canggih [21]. Dengan demikian, kejahatan *cyber* berada dalam kedudukan yang menuntut perhatian khusus dalam perkembangan hukum internasional. Tantangan dan kompleksitas yang dihadapinya mendorong komunitas internasional untuk bekerja sama secara lebih erat guna menciptakan dasar hukum yang efektif, memahami sifat abstrak kejahatan ini, dan menjaga keamanan dunia maya. Kesadaran dan kerja sama internasional yang ditingkatkan akan menjadi kunci dalam menanggapi ancaman kejahatan *cyber* dan melindungi kepentingan global.

3.5 Upaya Pencegahan Terhadap Kejahatan Cyber Dalam Hukum Internasional

Kejahatan *cyber* yang terus berkembang dalam era teknologi informasi dan komunikasi (TIK), menjadi tantangan serius di tingkat global. Dalam upaya pencegahan kejahatan *cyber*, hukum internasional memainkan peran krusial dengan menyusun standar dan aturan yang dapat diadopsi secara universal. Keberhasilan pencegahan ini tergantung pada kerja sama internasional, pengembangan instrumen hukum, dan peningkatan kesadaran masyarakat terhadap ancaman kejahatan *cyber*. Pertama-tama, pengembangan instrumen hukum internasional menjadi langkah penting untuk menciptakan aturan yang jelas dan komprehensif dalam mengatasi kejahatan *cyber*. Konvensi tentang Kejahatan Siber (Convention on Cybercrime) tahun 2001 dan Resolusi Majelis Umum PBB 53/70 tentang Kejahatan Siber (Crimes in Cyberspace) tahun 1998 menjadi landasan hukum yang mengatur berbagai bentuk kejahatan *cyber*. Konvensi tersebut memberikan panduan dalam mengatasi penipuan, pencurian data, perusakan data, dan penyebaran informasi ilegal. Namun, perlu diakui bahwa belum semua negara meratifikasi instrumen hukum ini, dan ini menunjukkan bahwa upaya untuk mengintegrasikan norma dan aturan masih memerlukan waktu.

Kerja sama internasional menjadi elemen kunci dalam penanggulangan kejahatan *cyber*. Kerja sama ini dapat mencakup pertukaran informasi, pelatihan, dan bantuan teknis antar negara. Upaya ini diwujudkan dalam pengembangan instrumen hukum internasional dan membentuk dasar bagi negara-negara untuk saling berkoordinasi. Namun, tantangan masih muncul terutama dari negara-negara berkembang yang seringkali kekurangan sumber daya untuk terlibat dalam upaya penanggulangan kejahatan *cyber*. Oleh karena itu, perlu ada inisiatif global untuk memberikan bantuan dan dukungan teknis kepada negara-negara tersebut. Peningkatan kesadaran masyarakat juga menjadi langkah esensial dalam pencegahan kejahatan *cyber*. Kesadaran akan bahaya kejahatan *cyber* dan upaya melindungi diri dari ancaman tersebut merupakan kunci dalam mengurangi tingkat kerentanannya. Sosialisasi dan edukasi terhadap masyarakat perlu ditingkatkan untuk memastikan bahwa individu memiliki pemahaman yang memadai tentang risiko dan dampak dari kejahatan *cyber*. Meskipun telah dilakukan upaya yang signifikan dalam pencegahan kejahatan *cyber*, analisis menunjukkan bahwa masih ada kekurangan yang perlu diatasi. Salah satu kendala utama adalah belum meratifikasinya semua negara terhadap instrumen hukum internasional yang bertujuan mengatasi kejahatan siber. Sebagian negara mungkin belum sepenuhnya mengadopsi kerangka kerja hukum yang konsisten, sehingga kerja sama internasional dalam menanggulangi kejahatan *cyber* bisa mengalami hambatan.

Kurangnya sumber daya di negara-negara berkembang juga menjadi faktor penghambat dalam upaya pencegahan kejahatan *cyber*. Dalam menghadapi ancaman keamanan siber yang terus berkembang, diperlukan investasi yang cukup dalam hal teknologi, pelatihan personel, dan infrastruktur keamanan informasi. Negara-negara dengan keterbatasan sumber daya mungkin mengalami kesulitan dalam memenuhi standar keamanan siber global, meninggalkan celah bagi pelaku kejahatan *cyber* untuk beroperasi. Selain itu, tingkat kesadaran masyarakat yang masih rendah terhadap risiko kejahatan *cyber* juga menjadi tantangan serius. Pendidikan dan kampanye sosialisasi perlu ditingkatkan untuk meningkatkan pemahaman masyarakat tentang potensi ancaman siber dan langkah-langkah yang dapat diambil untuk melindungi diri secara online. Dengan demikian, perlu adanya upaya yang lebih intensif dan komprehensif yang melibatkan berbagai pihak, termasuk pemerintah, sektor swasta, dan masyarakat, guna mencapai pencegahan kejahatan *cyber* yang optimal. Dasar hukum upaya pencegahan kejahatan *cyber* dalam hukum internasional didasarkan pada prinsip-prinsip dasar seperti prinsip non-intervensi, prinsip kerja sama internasional, dan prinsip tanggung jawab negara. Prinsip ini menciptakan kerangka kerja yang memungkinkan negara-negara untuk bekerja sama dalam menanggulangi kejahatan *cyber* tanpa melanggar kedaulatan negara lain. Upaya pencegahan kejahatan *cyber* dalam hukum internasional memerlukan kolaborasi yang erat antara negara-negara, pengembangan instrumen hukum yang lebih komprehensif, dan peningkatan kesadaran masyarakat. Hanya dengan pendekatan yang terintegrasi dan global, masyarakat dapat terlindungi secara efektif dari ancaman yang semakin kompleks ini.

3.6 Upaya Penanganan Kejahatan Cyber Sebagai Kejahatan Internasional

Semakin meluasnya kejahatan *cyber* dengan memanfaatkan teknologi informasi dan komunikasi, telah menjadi ancaman global yang memerlukan penanganan serius. Kejahatan ini dapat terjadi di mana saja dan kapan saja, menghadirkan tantangan unik dalam penanganannya. Kategorisasi kejahatan *cyber* sebagai kejahatan internasional disebabkan oleh sifatnya yang

dapat melintasi batas negara. Pelaku kejahatan *cyber* dapat berada di negara yang berbeda dengan korbannya, menyulitkan upaya penegakan hukum karena perbedaan yurisdiksi di setiap negara. Upaya penanganan kejahatan *cyber* menunjukkan bahwa ada pendekatan yang dapat dilakukan, baik secara bilateral, regional, maupun multilateral. Pendekatan bilateral melibatkan dua negara yang terkait dengan kejahatan *cyber*, dapat dilakukan melalui perjanjian bilateral atau kerja sama antarlembaga penegak hukum kedua negara tersebut. Pendekatan regional melibatkan beberapa negara di dalam satu kawasan, dapat diwujudkan melalui perjanjian regional atau kerja sama antarlembaga penegak hukum di kawasan tersebut. Pendekatan multilateral melibatkan berbagai negara di seluruh dunia, dapat diatur melalui perjanjian multilateral atau kerja sama antarlembaga penegak hukum di tingkat internasional [22]. Dasar hukum penanganan kejahatan *cyber* di Indonesia diatur oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-Undang ini menjadi payung hukum yang menyeluruh untuk menanggulangi berbagai tindak pidana *cyber* yang berkembang pesat. Di dalamnya termasuk ketentuan terkait dengan penipuan, peretasan, pencurian identitas, dan penyebaran konten ilegal. UU ITE menciptakan landasan hukum yang memadai untuk penegakan hukum di bidang teknologi informasi dan memberikan otoritas kepada aparat penegak hukum untuk mengatasi ancaman kejahatan *cyber* [23].

Selain Undang-Undang ITE, Indonesia juga telah meratifikasi Convention on Cybercrime atau yang dikenal sebagai Konvensi Kejahatan *Cyber* pada tahun 2009. Ratifikasi ini menandakan komitmen Indonesia untuk bersama-sama mengatasi kejahatan *cyber* di tingkat internasional. Konvensi ini memberikan dasar hukum yang lebih luas dan kerangka kerja koordinasi antarnegara dalam menghadapi kejahatan siber. Dengan adopsi Konvensi Kejahatan *Cyber*, Indonesia juga turut berpartisipasi dalam upaya global untuk menyelaraskan hukum dan langkah-langkah pencegahan kejahatan siber. Meskipun telah ada dasar hukum yang kuat, tantangan utama dalam penanganan kejahatan *cyber* tetap melibatkan peningkatan kapasitas, pelatihan personel, dan koordinasi yang efektif antara lembaga penegak hukum serta sektor swasta. Diperlukan pendekatan yang holistik dan terus-menerus agar Indonesia dapat menghadapi dinamika kejahatan siber yang terus berkembang. Penanganan kejahatan *cyber* yang kompleks memerlukan pendekatan yang komprehensif melalui kerja sama bilateral, regional, dan multilateral. Kerjasama antarlembaga penegak hukum, pemerintah, dan masyarakat sangat penting dalam menghadapi ancaman kejahatan *cyber*. Beberapa rekomendasi untuk meningkatkan upaya penanganan kejahatan *cyber* meliputi perkuatan peraturan perundang-undangan yang lebih komprehensif, peningkatan kerja sama internasional melalui perjanjian dan kerja sama antarlembaga, serta peningkatan kesadaran masyarakat akan bahaya kejahatan *cyber*. Dengan langkah-langkah ini, diharapkan masyarakat dapat lebih efektif melindungi diri dari ancaman kejahatan *cyber* yang terus berkembang [24].

4. KESIMPULAN

Urgensi dan kompleksitas penanganan kejahatan *cyber* menjadi sebuah ancaman global. Kejahatan tersebut melibatkan penggunaan teknologi informasi dan komunikasi, menyulitkan penegakan hukum karena sifatnya yang melintasi batas negara. Upaya penanganan dapat dilakukan melalui pendekatan bilateral, regional, dan multilateral. Pendekatan bilateral melibatkan kerja sama antara dua negara terkait dengan kejahatan *cyber*, sementara pendekatan regional melibatkan beberapa negara di suatu kawasan. Pendekatan multilateral melibatkan

berbagai negara di seluruh dunia, dengan tujuan menciptakan kerangka kerja hukum yang bersifat internasional. Dasar hukum penanganan kejahatan *cyber* di Indonesia diatur oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta melalui ratifikasi Convention on Cybercrime (Konvensi Kejahatan *Cyber*) [25].

Perlunya penguatan peraturan perundang-undangan, peningkatan kerja sama internasional, dan peningkatan kesadaran masyarakat. Penguatan peraturan perundang-undangan bertujuan agar regulasi yang ada lebih komprehensif dan efektif. Kerja sama internasional menjadi kunci dalam menghadapi kejahatan *cyber* yang melibatkan pelaku dari berbagai negara. Sementara itu, peningkatan kesadaran masyarakat dianggap penting untuk melibatkan publik dalam upaya melindungi diri dari ancaman kejahatan *cyber* dan melaporkan insiden yang terjadi. Dengan demikian, menekankan perlunya pendekatan holistik dan kerjasama lintas negara dalam menghadapi ancaman kejahatan *cyber*. Hanya dengan upaya bersama yang melibatkan pemerintah, lembaga penegak hukum, dan masyarakat, kita dapat membangun pertahanan yang kuat terhadap kejahatan *cyber* dan menjaga keamanan dunia maya.

REFERENSI

- [1] Ketaren, E. (2016). Cybercrime, cyber space, dan cyber law. *Jurnal Times*, 5(2), 35-42.
- [2] Maskun, S. H., LM, L., Maskun, S. H., LM, L., Achmad, S. H., MH, A. S., ... & Lubis, S. N. (2020). Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional.
- [3] Nasution, A. R. (2018, October). Penegakan Hukum Terhadap Tindakan Terorisme sebagai 'Extraordinary Crime' dalam Perspektif Hukum Internasional dan Nasional. In *Talenta Conference Series: Local Wisdom, Social, and Arts (LWSA)* (Vol. 1, No. 1, pp. 008-014).
- [4] Rosana, A. S. (2010). Kemajuan Teknologi Informasi dan Komunikasi dalam Industri Media di Indonesia. *Gema Eksos*, 5(2), 218225.
- [5] Barus, Z. (2013). Analisis filosofis tentang peta konseptual penelitian hukum normatif dan penelitian hukum sosiologis. *Jurnal Dinamika Hukum*, 13(2), 307-318.
- [6] Tan, D. (2021). Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, 8(8), 2463-2478.
- [7] Idik Saeful Bahri, S. H. (2020). *Cyber Crime Dalam Sorotan Hukum Pidana* (Vol. 159). Bahasa Rakyat
- [8] Amrullah, M. A. (2003). Pencucian Uang dan Kejahatan Terorganisir. *Jurnal Hukum IUS QUIA IUSTUM*, 10(22), 130-146.
- [9] Gagola, E. D. (2018). Tindak Pidana Perdagangan Orang Sesuai Konvensi Palermo Menentang Kejahatan Transnasional Terorganisasi Menurut UU No. 21 Tahun 2007. *Lex Crimen*, 7(3).
- [10] Ak, S., & Fidelia, F. (2019). Kerjasama Internasional Dalam Upaya Pemberantasan 'Illicit Arms Trafficking' di Kawasan Asia Tenggara. *Simbur Cahaya*, 25(1), 114-133.
- [11] Hasan, M. I. (2018). Kejahatan Transnasional Dan Implementasi Hukum Pidana Indonesia. *Lex Crimen*, 7(7).
- [12] Indonesia, P. R. (2001). Undang-Undang Republik Indonesia Nomor 20 Tahun 2001 Tentang Perubahan Atas Undang-Undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi.
- [13] Monita, Y. (2013). Perlindungan Hukum Bagi Korban Tindak Pidana Perdagangan Orang Dalam Perspektif Undang-Undang Nomor 21 Tahun 2007. *INOVATIF| Jurnal Ilmu*

- Hukum, 6(2).
- [14] Naseh, M., Ikhwanuddin, I., Ramadhani, F., Kusprabandaru, A., & Bathara, B. (2019). Karakteristik Pelaku Kejahatan Transnasional Terorganisasi Di Indonesia Dan Eropa. *Jurnal Hubungan Internasional*, 8(1), 48-60.
 - [15] Banjarani, D. R. (2020). Illegal Fishing Dalam Kajian Hukum Nasional Dan Hukum Internasional: Kaitannya Dengan Kejahatan Transnasional. *Jurnal Kertha Patrika*, 42(2).
 - [16] Silvia, E. M. (2020). Upaya Penanggulangan Kasus Perdagangan dan Penyelundupan Manusia Sebagai Kejahatan Transnasional Terorganisir. *INICIO LEGIS*, 1(1).
 - [17] Saragih, Y. M., & Azis, D. A. (2020). Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal Di Era Globalisasi. *Soumatera Law Review*, 3(2), 265-279
 - [18] Tabiu, R., Intan, N., & Safiuddin, S. (2023). Globalisasi dan Kejahatan Transnasional Terorganisasi. *Halu Oleo Law Review*, 7(1), 99-110.
 - [19] Sidik, S. (2013). Dampak undang-undang informasi dan transaksi elektronik (UU ITE) terhadap perubahan hukum dan sosial dalam masyarakat. *Jurnal Ilmiah Widya*, 1(1), 1-7.
 - [20] Indriati, N. (2009). Mutual Legal Assistance Treaties (MLATs) Sebagai Instrumen Pemberantasan Kejahatan Internasional. *Jurnal Dinamika Hukum*, 9(2), 125-134.
 - [21] BENI SETIAWAN, B. S. (2019). Penegakan hukum pidana terhadap akses sistem komputer secara ilegal (hacking) dan menimbulkan kerusakan (cracking) dalam kejahatan dunia maya (cybercrime) menurut perspektif undang-undang nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik (Doctoral dissertation, Universitas Batanghari).
 - [22] Simanjuntak, S. Y., & Utomo, T. C. (2016). 13. Analisis Kerja Sama Bilateral Indonesia Dengan Australia Dalam Penanggulangan Terorisme Sebagai Kejahatan Transnasional Terorganisir (2002-2015). *Journal of International Relations*, 2(3), 117-127.
 - [23] Nugraha, R. (2021). Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di Indonesia. *Jurnal Ilmiah Hukum Dirgantara*, 11(2).
 - [24] Putra, A. K. (2014). Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional. *Jurnal Ilmu Hukum Jambi*, 5(2), 43297.
 - [25] Sutrisno, B., & Paksa, F. B. B. (2019). Penegakan Hukum Terhadap Tindak Pidana Pencemaran Nama Baik Menurut Pasal 27 Ayat (3)