Jurnal Hukum dan Sosial Politik
Vol.2, No.3 Agustus 2024
e-ISSN: 2986-3287; p-ISSN: 2986-4445, Hal 126-135
DOI: https://doi.org/10.59581/jhsp-widyakarya.v2i3.3426

Efektifitas Yurisdiksi Cybercrime Di Tengah Perkembangan Teknologi Informasi

Amanda Fitria Najwa, Aqila Husna
Universitas Tidar
mandafn369@gmail.com, aqilahusna727@gmail.com

Alamat : Jl. Kapten Suparman No.39, Potrobangsan, Kec. Magelang Utara, Kota Magelang, Jawa Tengah 56116
Koresprodensi Penulis : mandafn369@gmail.com

Abstract. *This journal discusses the influence of the development of information technology which cannot be separated from the existence of jurisdiction, which jurisdiction is effective or not in its implementation, so it must be discussed how this jurisdiction can be effective in its implementation, the existence of the ITE Law can pave the way for law enforcement in cyber crime because in the ITE Law, sanctions can be applied to both Indonesian citizens themselves and foreign citizens who commit cyber crime and harm the Indonesian state, however, to carry out legal actions with foreign actors, it must be ensured that the country also has regulations regarding cybercrime, and the ratification of Indonesia's ability to apply for the extradition of perpetrators will be stronger.*

Keyword: *Information technology, Jurisdiction, ITE Law, Ratification*

Abstrak. Jurnal ini membahsa tentang pengaruh adanya perkembangan teknologi informasi yang pasti tidak terlepas dari adanya yurisdiksi, yang dimana yurisdiksi tersebut efektif apa tidak dalam pelaksanaaanya, sehingga harus di lakukannya pembahsasan bagaimana yurisdiksi tersebut dapat efektif dalam pelaksanaanya, adanya UU ITE dapat membuka jalannya penegakan hukum dalam cyber crime karna didalam UU ITE tersebut dapat diberlakukannya sanksi-sanksi baik dari warga negara indonesia itu sendiri ataupun warga negara asing yang melakukan cyber crime dan merugikan negara indonesia, akan tetapi untuk melakukan perbuatan hukum dengan pelaku negara asing maka harus dipastikan negara tersebut juga terdapat peraturan tentang cybercrime, dan adanya ratifikasi untuk indonesia dapat mengajukan ekstradisi terhadap pelaku akan lebih kuat.

Kata kunci : Teknologi informasi, Yurisdiksi, UU ITE, Ratifikasi

PENDAHULUAN

Sesuai dengan berkembangnya zaman dapat diketahui pula bahwa alat alat yang dibuat juga semakin canggih, tidak terkecuali dengan kemajuan teknologi informasi yang dimana sangat berpengaruh dalam kegiatan manusia, seperti kegiatan dalam berinteraksi dengan orang lain dan menyebabkan adanya perubahan sosial di dalam suatu masyarakat, ekonomi, hingga budaya yang secara signifkan. Di zaman sekarang ini dapat diketahui bawha teknologi merupakan suatu hal yang sangat penting dan mengakibatkan banyak dampak yang mempangaruhi baik dampak yang buruk maupaun dampak yang baik. pengaruh yang baik dampak memberikan manfaat bagi orang yang dapat mengelola dengan baik sehingga mendatangkan keuntungan bagi diri nya sendiri, akan tetapi jika teknologi terseut tidak

Received Mei 19, 2024; Accepted Juni 07, 2024; Published Agustus 30, 2024
* *Amanda Fitria Najwa, mandafn369@gmail.com*

digunakan sesuai dengan manfaatnya maka akan merugikan orang banyak tidak hanya dirinya sendiri.

Cyber crime atau kejahatan dunia memang kejahatan yang sudah sering kali terjadi dalam hal dunia teknologi informasi dengan menggunakan internet sebagai media dalam bertindak, akan tetapi kejahatannya mungkin tidak terlihat secara langsung oleh orang sekitar dan tidak menimbulkan luka fisik akan tetapi cyber crime dapat menimbulkan kerugian yang tidak main-main seperti hacker yang bisa mencuri data-data penting yang dapat disalahgunakan, sehingga untuk mencegah hal-hal tersebut perlu adanya peraturan yang dibuat untuk menyelesaikan masalah-masalah cyber crime, yang dimana pelaku cyber crime inni juga tidak dapat dipastikan secara cepat, karna cyber crime itu sendiri dilakukan tanpa adanya kontak fisik anatar pelaku dengan korbannya, sehingga dapat memperlambat jalannya penegakan keadilan yang disebabkan karna tidak taunya pelaku tersebut. Dan cybercrime dapat dilakukan di luar negeri seingga cyber crime merupakan kejahatan yang tidak mengenal batas.

Didalam penerapan hukum untuk pelaku, hukum pidana merupakan peraturan yang menentukan segala perbuatan apapun yang dilarang dan termasuk dalam kategori pidana atau kriminal, serta dalam menentukan sebuah hukuman yang setimpal dan pantas bagi pelaku dengan menganut peraturan perundang-undangan yang sudah berlaku di dalam negara tersebut sehingga hukum pidana merupakan dasar yang pas dalam menegakkan keadilan dan memberikan efek jera bagi pelaku cyber crime tersebut agar tidak menyalahgunakan hal yang sangat besar dampaknya, akan tetapi jika terdapat negara yang tidak mengatur hacker atau semacamnya maka negara yang dirugikan tersebut tidak dpat seenaknya untuk mengambil keputusan hukum, dan harus menjalani hukum internasional karna sudah beda negara terhadap pelakunya.

Salah satu kejahatan yang menggunakan teknologi informasi dan internet adalah penyerangan terhadap jaringan internet KPU, yang dimana jaringan di pusat Tabulasi Komisi Pemilihan Umum sempat down (down) dalam beberapa kali yang dimana KPU meminta bantuan terhadap cybersrime kepolisian, yang dimana terindekasi ada cyber crime dengan cara meretas sebanyak 20 lebih serangan yang di terima, dan penyerang tersebut sudah diblokir alamat IP-nya oleh PT.Telkom Tim TI KPU, kasus tersebut memiliki keinginan untuk mengacaukan proses pemilihan suara di KPK dan termasuk dalam cybercrime sebagai tindak murni kejatahan yang diaman penyerang dengan sengaja melakukan pengacauan pada tampilan halaman tabulasi nasional hasil dari pemilu. yang dimana kasus ini termasuk jenis data forgery, hacking-cracking, sabotage, anda extortion, atau cyber terorism, dan cybercrime ini menyerang

pemerintah (against goverment) dengan adanya kasus tersebut maka perlu adanya cyberlaw yang mengatur**.**

Dan didalam penyelesaian cyber crime maka harus ada kebijakan formulasi/legislasi yang disusun dalam satu kesatuan sistem hukum pidana yang selaras dan terpadukarena pada hakikatnya merupakan bagian dari usaha penegakan hukum sehingga terdapat kefektifatasan yang dapat digunakan dalam menanggulangi cyber crime tersebut dan brtujuan untuk mencapai kesejahteraan masyarakat pada umumnya , dan termasuk dalam kebijakan sosial.

RUMUSAN MASALAH

1. Bagaimana dampak dalam penerapan yurisdiksi yang berlaku terhadap warga negara asing yang melakukan kejahatan siber di Indonesia?
2. Apa strategi dan kebijakan yang dapat diterapkan untuk meningkatkan efektivitas yurisdiksi cybercrime?

METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini menggunakan metode studi literatur dimana penulis mengkaji penelitian dengan berbagai sumber jurnal,artikel,berita untuk memvalidasi temuan dan memastikan keabsahan serta kredibilitas hasil penelitian. Analisis informasi laporan tahunan dari instansi penegak hukum, serta publikasi akademik dan media yang terkait dengan yurisdiksi cybercrime dan perkembangan teknologi informasi. Jenis metode ini dapat memudahkan dalam pembuatan artikel dikarenakan pada metode ini kita dapat melakukan pengamatan mendalam terkait fenomena yang terjadi pada perkembangan teknologi.

PEMBAHASAN

1. Bagaimana dampak dalam penerapan yurisdiksi yang berlaku terhadap warga negara asing yang melakukan cyber crime di Indonesia?

Dapat diketahui bahwa cyber crime bisa dilakukan di lintas negara yang dimana pengaturannya harus sesuai dengan yurisiksi negara dalam hukum international Konsep yurisdiksi berkaitan dengan masalah hukum, kewenangan peradilan atau lembaga, dan undang-undang lain yang berasal dari undang-undang tersebut. sesuai dengan

penerapannya. Dan sejauh mana undang-undang ini dapat dibuat, diberlakukan, dan diterapkan terhadap pihak-pihak yang tidak patuh sangatlah terbatas. Meskipun ada hubungan erat antara yurisdiksi dan lokasi, hal ini tidak mutlak. Pihak lain yang mempunyai kewenangan untuk bertindak atas nama negara lain atau diluar negeri yang dimana juga dapat melakukan hal tersebut.

Penegakan hukum harus terus-menerus menangani masalah utama yurisdiksi hukum, khususnya ketika berhadapan dengan warga negara asing yang melakukan kejahatan. Kejahatan dunia maya juga yurisdiksi memperjelas bahwa penanganan masalah kejahatan dunia maya berada di dalam yurisdiksi hukum internasional.

Di indonesia sendiri dengan upaya pencegahan tindak pidana, ataupun penangan tindak pidana, UU ITE akan menjadi dasar hukum dalam proses penegakan hukum kejahatan-kejahatan dengan sarana elektronik dan komputer, denagan adanya beberapa faktor yang mempengaruhi penegakan hukum terhadap kejahatan siber sangat di pengaruhi oleh faktor hukum.

Karena cyber crime adalah bagian dari anatomi kejahatan transnasional, maka hukum pun demikian yang digunakan adalah hukum nasional, yaitu hukum Indonesia dalam konteks ini. Namun, tidak seluruhnya diatur oleh peraturan perundang-undangan nasional.

Maka dengan demikian yang dapat diberlakukan adalah asas-asas dan ketentuan hukum prinsip- prinsip dan peraturan-peraturan hukum internasional.

Dalam adanya cybercrime sebelum disahkannya UU ITE dengan dilakukannya penafsiran cyber crime ke perundang-undangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi diantaranya:

A. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi
B. Undang-Undang Nomor 14 Tahun 2008 tentang keterbukaan informasi Publik
C. Undang-Undang Nomor 15 Tahun 2003 tentang pemberantasan Tindak Pidana Terorisme
D. Dan lain sebagainya.

Di dalam perkembangnya zaman berkembang pula pengaturan terhadap cyber crime yang dimana diatur di dalam Undang-Undang nomor 11 tahun 2008 tentang

informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagai pelindung hukum yang di berlakukan di indonesia, dan diharapkan agar menjadi pondasi dalam menegakkan ketertiban bagi kegiatan pemanfataan teknologi informasi tidak hanya terbatas pada kegiatan internet akan tetapi suatu kegiatan yang memanfaatkan perangkat komputer, atau instrumen lainnya.

Apabila indonesia sudah meratifikasi tentang cybercrime sehingga dapat menjalin kerjasama dengan negara-negara peserta didalam menangani kasus cybercrime yang merugikan indonesia, dan jika pelaku tersebut berasal dari luar negeri ataupun kejahaatan di luar wilayah indonesia, dengan adanya meratifikasikan konvensi tersebut maka posisi idonesia dalam mengajukan ekstradisi terhadap pelaku akan lebih kuat. Sehingga perjanjian timbal balik antar negara yan dituangkan di dalam suatu undang-undang. Indonesia dapat melakukan perbuatan hukum apabila kedua negara tersebut atau lebih memperbolehakn dan mengatur tentang cybercrime didalam negaranya, apabila negara pelaku tersebut tidak mengatur tentang adanya cybercrime maka indonesia tidak dapat melakukan perbuatan dengan seenaknya menurut hukum yang ada di indonesia itu sendiri. Adanya UU ITE tersebut telah mengatur tentang suatu yurisdiksi yang bersifat ekstrateritorial sebagaimana diatur di dalam pasal 2.

Dengan diketahui bahwa UU ITE memiliki jangkauan yurisdiksi yang tidak hanya dipergunakan dalam perbuatan hukum yang hanya berlaku di wiliyah indonesia ataupun dilakukan oleh warga negara indonesia itu sendiri di luar wilayah negara indonesia, akan tetapi berlaku utuk perbuatan hukum yang dilakukan oleh warga negara asing yang melakukan suatu perbuatan hukum terhadap indonesia yang merugikan dan mengancam negara indonesia yang dapat dilihat bahwa pemanfaatan teknologi bisa dilakukan diberbagai belahan dunia asalkan memadai dengan bahannya dan untuk infomrasi Elektronik dan Transaksi Elektronik dapat bersifat lintas territorial atau universal.

2. Apa strategi dan kebijakan yang dapat diterapkan untuk meningkatkan efektivitas yurisdiksi cybercrime?

Zaman era digital saat ini, teknologi informasi dan komunikasi telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari, mendorong perubahan besar di berbagai sektor seperti ekonomi, pendidikan, dan pemerintahan. Meskipun membawa banyak manfaat, kemajuan ini juga menghadirkan tantangan baru berupa kejahatan siber dan serangan siber yang semakin kompleks dan melintasi batas negara. Kejahatan siber, yang meliputi aktivitas ilegal melalui komputer dan jaringan, serta serangan siber yang bertujuan merusak atau mencuri data, memerlukan respons hukum yang efektif dan terkoordinasi secara global.

Kejahatan semakin meningkat seiring dengan perkembangan teknologi internet dibandingkan masa lalu. Di Indonesia, kejahatan siber sulit untuk diidentifikasi atau dikategorikan karena prinsip legalitas. Dalam konteks kejahatan siber yang melibatkan penggunaan internet, posisi Indonesia kini telah menggantikan Ukraina yang sebelumnya menduduki peringkat pertama. Berbagai jenis kejahatan internet yang marak terjadi di Indonesia meliputi penipuan kartu kredit, penipuan perbankan, defacing, cracking, hacking, perjudian online, dan terorisme, dengan korban yang tidak hanya berasal dari dalam negeri tetapi juga dari luar negeri seperti Amerika Serikat, Inggris, Australia, Jerman, Korea, dan Singapura, serta beberapa wilayah di negara ini.

Upaya yang dilakukan oleh kepolisian untuk menanggulangi dan mengoptimalisasi terjadinya *cybercrime* berupa:

1. Membentuk Direktorat Tindak Pidana Siber *(Dittipidsiber)* di bawah Badan Reserse Kriminal *(Bareskrim)* yang khusus menangani kasus-kasus kejahatan siber. Unit ini bertugas mengidentifikasi, menyelidiki, dan menindak berbagai bentuk kejahatan siber yang terjadi di Indonesia. Dengan tim yang terlatih dalam forensik digital dan investigasi siber, unit ini diharapkan mampu merespons secara cepat dan tepat terhadap insiden siber.
2. Menjalin kerjasama dengan berbagai instansi pemerintah, seperti Kementerian Komunikasi dan Informatika (Kominfo), serta sektor swasta seperti penyedia layanan internet dan perusahaan teknologi untuk berbagi informasi dan teknologi.
3. Mengadakan pelatihan dan workshop untuk meningkatkan kapasitas dan keterampilan anggota dalam menangani kejahatan siber. Ini termasuk pelatihan teknis tentang analisis forensik digital, metode investigasi siber, dan penggunaan perangkat lunak khusus untuk melacak dan mengumpulkan bukti digital.

4. Penyesuaian dan harmonisasi regulasi nasional dengan standar internasional sangat penting untuk memperkuat dasar hukum penanganan kejahatan siber. Ini juga memudahkan kerjasama internasional dalam menangani kasus yang melibatkan pelaku dan korban lintas negara.
5. memperluas jaringan kerjasama internasional dengan badan penegak hukum dan organisasi global lainnya. Ini termasuk bergabung dalam forum internasional dan berpartisipasi dalam konvensi global untuk meningkatkan efektivitas penanganan kejahatan siber lintas batas.
6. Rekrutmen dan pengembangan tim ahli di bidang keamanan siber harus menjadi prioritas. Meningkatkan jumlah personel yang memiliki keahlian khusus dalam keamanan informasi, analisis forensik digital, dan pengembangan perangkat lunak keamanan akan memperkuat upaya penanggulangan.

Berdasarkan metode penanggulangan ini, visi kepolisian yang mencakup prediktif, responsibilitas, dan transparansi sudah terpenuhi. Tentu saja, ada beberapa catatan penting yang menunjukkan bahwa profesionalisme harus diterapkan dalam berbagai kasus, tidak hanya pada kasus ini. Penjabaran dari Kepolisian dapat mengoptimalkan upaya dengan mengikuti prosedur teknis dan panduan fisik untuk menanggulangi kasus-kasus seperti ini. Dalam konteks ini penerapan prinsip hukum internasional menjadi sangat penting.

Prinsip kedaulatan negara merupakan landasan fundamental dalam hukum internasional, yang menyatakan bahwa setiap negara memiliki hak eksklusif untuk mengatur urusan dalam negerinya tanpa campur tangan dari pihak luar. Dalam konteks penanganan kejahatan siber, prinsip ini berarti bahwa setiap negara berhak untuk mengatur dan menegakkan hukum terhadap aktivitas siber yang terjadi di dalam wilayah yurisdiksinya. Negara-negara memiliki kebebasan untuk menetapkan undang-undang siber mereka sendiri, membentuk badan penegak hukum khusus, dan melaksanakan prosedur hukum terhadap pelaku kejahatan siber yang beroperasi di dalam perbatasan mereka. Namun, ketika pelaku kejahatan siber beroperasi melintasi batas negara, penerapan prinsip kedaulatan menghadapi tantangan besar. Misalnya, sebuah serangan siber yang dilancarkan dari satu negara ke negara lain memerlukan kerja sama lintas batas untuk investigasi dan penuntutan. Prinsip non-intervensi juga relevan di sini, menuntut negara untuk tidak campur tangan dalam urusan domestik negara lain.

Berkaitan dengan Konvensi Budapest ini memberikan pedoman bagi negara-negara dalam membentuk undang-undang domestik yang sesuai, serta menetapkan mekanisme untuk kerja sama internasional dalam hal penegakan hukum. Untuk meningkatkan efektivitas yurisdiksi

cybercrime berdasarkan kerjasama internasional, negara-negara perlu memperkuat perjanjian ekstradisi dan bantuan hukum timbal balik *(Mutual Legal Assistance Treaties)*. Perjanjian ini memungkinkan negara untuk meminta dan memberikan bantuan hukum dalam proses penyelidikan dan penuntutan kejahatan siber yang melibatkan lebih dari satu yurisdiksi. Dengan ini negara dapat berbagi bukti dan informasi penting dengan cepat dan efisien, mengatasi hambatan birokrasi yang seringkali memperlambat proses investigasi lintas batas.

Penting bagi negara-negara untuk terlibat dalam konvensi internasional seperti Konvensi Budapest tentang kejahatan Siber. Konvensi ini menyediakan kerangka hukum yang komprehensif untuk memerangi cybercrime dan memfasilitasi kerjasama antara negara-negara anggotanya. Dengan mengikuti standar dan pedoman yang ditetapkan oleh konvensi ini, negara dapat memastikan bahwa hukum domestik mereka selaras dengan norma internasional, sehingga memudahkan koordinasi dan kolaborasi lintas batas.

Kerjasama internasional juga memerlukan pembentukan tim respons siber internasional yang dapat bergerak cepat dalam menanggapi insiden kejahatan siber. Tim ini harus terdiri dari pakar keamanan siber dari berbagai negara yang dapat bekerja bersama dalam melakukan analisis forensik, melacak pelaku, dan menutup celah keamanan yang dimanfaatkan oleh penjahat siber. Dengan adanya tim respons ini, negara-negara dapat segera menanggulangi serangan siber dan meminimalisir dampak yang ditimbulkan. Penting juga untuk mengadakan latihan bersama dan simulasi serangan siber secara berkala. Latihan ini akan membantu meningkatkan kesiapan dan koordinasi antara berbagai lembaga penegak hukum dan badan keamanan siber di berbagai negara. Melalui simulasi ini, negara dapat menguji prosedur respon mereka, mengidentifikasi kelemahan, dan memperbaiki strategi penanggulangan serangan siber secara efektif.

Penerapan prinsip kedaulatan harus disertai dengan penghormatan terhadap kedaulatan negara lain. Intervensi atau serangan siber yang dilancarkan oleh satu negara terhadap infrastruktur kritis negara lain dianggap sebagai pelanggaran kedaulatan dan dapat memicu konflik internasional. Oleh karena itu, penting bagi negara-negara untuk mengembangkan norma dan kesepakatan internasional yang jelas mengenai aktivitas siber yang dapat diterima dan batasan-batasan tertentu untuk mencegah konflik antar negara. Dengan demikian, prinsip kedaulatan negara dalam menangani kejahatan siber dapat diterapkan secara efektif sambil tetap menjaga stabilitas dan keamanan internasional.

KESIMPULAN DAN SARAN

Efektivitas yurisdiksi cybercrime di tengah perkembangan teknologi informasi merupakan tantangan yang kompleks dan membutuhkan pendekatan multi-aspek. Teknologi informasi telah mengubah lanskap kejahatan, dengan serangan siber yang semakin canggih dan bersifat transnasional. Negara-negara harus beradaptasi dengan cepat dan menciptakan kerangka hukum yang mampu mengimbangi laju perkembangan teknologi. Dalam konteks ini, kerjasama internasional menjadi sangat penting untuk mengatasi hambatan yurisdiksi yang sering kali menghambat proses investigasi dan penuntutan kejahatan siber.

Penguatan bantuan hukum timbal balik *(MLATs)* adalah langkah krusial dalam memperkuat kerjasama lintas batas. Perjanjian ini memungkinkan negara-negara untuk berbagi informasi dan bukti penting dengan cepat, memudahkan proses investigasi dan penuntutan kejahatan siber yang melibatkan berbagai yurisdiksi. Selain itu, partisipasi aktif dalam konvensi internasional seperti Konvensi Budapest tentang Kejahatan Siber dapat memastikan bahwa hukum domestik sejalan dengan standar internasional, memfasilitasi kolaborasi yang lebih efektif.

Pembentukan tim respons siber internasional juga merupakan strategi penting untuk meningkatkan efektivitas penanganan kejahatan siber. Tim ini dapat bergerak cepat dalam menanggapi insiden siber, melakukan analisis forensik, dan melacak pelaku kejahatan. Latihan bersama dan simulasi serangan siber yang rutin akan meningkatkan kesiapan dan koordinasi antar negara, memungkinkan respons yang lebih cepat dan efisien terhadap ancaman siber.

Pentingnya pengembangan dan pembagian teknologi canggih tidak bisa diabaikan. Negara-negara maju dalam bidang teknologi informasi dapat membantu negara-negara lain dengan menyediakan alat dan teknologi yang diperlukan untuk meningkatkan kapabilitas dalam menghadapi serangan siber. Akses ke teknologi terbaru sangat penting untuk semua negara dalam upaya melawan kejahatan siber yang terus berkembang.

Untuk meningkatkan efektivitas yurisdiksi cybercrime, negara-negara perlu memperkuat kerjasama internasional dengan memperbarui dan memperluas perjanjian ekstradisi serta bantuan hukum timbal balik *(MLATs)*. Selain itu, partisipasi aktif dalam konvensi internasional seperti Konvensi Budapest sangat disarankan untuk memastikan keselarasan hukum domestik dengan standar internasional. Negara-negara juga harus membentuk tim respons siber internasional yang dapat bergerak cepat dan efektif dalam menanggapi insiden siber. Latihan bersama dan simulasi serangan siber harus dilakukan secara berkala untuk meningkatkan kesiapan dan koordinasi antara berbagai lembaga penegak hukum dan badan keamanan siber.

Pengembangan dan pembagian teknologi canggih harus menjadi prioritas dalam kerjasama internasional. Negara-negara maju harus mendukung negara-negara lain dengan menyediakan teknologi terbaru yang diperlukan untuk menghadapi ancaman siber yang semakin canggih. Pembentukan forum internasional untuk diskusi dan pertukaran informasi mengenai ancaman siber terbaru sangat disarankan. Forum ini akan menjadi platform bagi negara-negara untuk berbagi pengetahuan, pengalaman, dan membangun jaringan kerjasama yang kuat dalam menghadapi tantangan siber global.

DAFTAR PUSTAKA

Nugraha, R. (2021). PERSPEKTIF HUKUM INDONESIA (CYBERLAW) PENANGANAN KASUS CYBER DI INDONESIA. *Jurnal Ilmiah Hukum Dirgantara*, Vol.*11*(2).

Pangestika, E. Q., & suningrat, N. (2024). PENERAPAN PRINSIP HUKUM INTERNASIONAL DALAM PENEGAKAN HUKUM TERHADAP KEJAHATAN SIBER DAN SERANGAN SIBER. *Jurnal Review Pendidikan dan Pengajaran*, *Vol.7*(2), 4-5.

Purnama, P., & nuarta. (2023). PENGUATAN PENEGAKAN HUKUM POLRI DALAM RANGKA OPTIMALISASI PENANGGULANGAN CYBERCRIME DI INDONESIA. *Journal of Multi Disciplinary Sciences*, *Vol.2*(1), 21-23.

Sari, U. I. P. (2021). KEBIJAKAN PENEGAKAN HUKUM DALAM UPAYA PENANGANAN CYBER CRIME YANG DILAKUKAN OLEH VIRTUAL POLICE DI INDONESIA. *Mimbar Jurnal Hukum*, Vol.*2*(1), 58-77.

Siahaan, A. P. U. (2018). PELANGGARAN CYBERCRIME DAN KEKUATAN YURISDIKSI DI INDONESIA. *Jurnal Teknik dan Informatika*, Vol.*5*(1), 6-9.