e-ISSN : 2621-4105

UPAYA REGULASI TEKNOLOGI INFORMASI DALAM MENGHADAPI SERANGAN SIBER GUNA MENJAGA KEDAULATAN NEGARA KESATUAN REPUBLIK INDONESIA

Wahyu Beny Mukti Setiyawan[1], Erifendi Churniawan[2], Femmy Silaswaty Faried[3]
[1´3]Fakultas Hukum Universitas Islam Batik Surakarta
[2]Politeknik Perkeretaapian Indonesia
[1]muktibeny@gmail.com

Abstrak

Penelitian ini bertujuan untuk menganalisis keberadaan UU ITE dan Upaya Regulasi dalam menghadapi Serangan Siber. Saat ini, teknologi berkembang dengan begitu pesat,oleh karena itu, perlunya diadakannya perlindungan terhadap para pengguna IT saat ini agar para pengguna selalu merasa dilindungi oleh Hukum Indonesia. Penelitian ini menggunakan penelitian hukum normatif. Ditinjau dari sifatnya penelitian ini termasuk penelitian hukum yang bersifat deskriptif, Analisis terhadap rumusan masalah dilakukan secara preskriptif dengan menggunakan penafsiran Gramatikal dan penafsiran Sistematis. Pemberlakuan UU ITE merupakan hukum siber pertama di Indonesia yang bertujuan untuk memberikan kepastian hukum bagi masyarakat dan mencegah kejahatan yang ditimbulkan oleh teknologi informasi bagi penggunanya. Undang-undang khusus tentang kejahatan siber merupakan salah satu kebijakan kriminalisasi kejahatan siber yang ideal di Indonesia yang memuat aturan umum yang berlaku untuk semua kejahatan yang berlaku di bidang teknologi informasi dan komunikasi, kejahatan yang terkait dengan kerahasiaan data atau sistem di komputer. Penegakan hukum merupakan aspek penting dalam suatu negara. Dalam hal ini, POLRI sebagai penegak hukum yang memiliki fungsi, tugas dan wewenang untuk mewujudkan keamanan dan ketertiban masyarakat, termasuk mengambil tindakan tegas dalam penegakan hukum terhadap kejahatan siber.

Kata kunci: Teknologi Komunikasi; Hukum Siber; Serangan Siber

e-ISSN : 2621-4105

INFORMATION TECHNOLOGY REGULATORY EFFORTS IN DEALING WITH CYBER ATTACK TO PRESERVE STATE SOVEREIGNTY OF THE REPUBLIC OF INDONESIA

Wahyu Beny Mukti Setiyawan[1], Erifendi Churniawan[2], Femmy Silaswaty Faried[3]
[1´3]Fakultas Hukum Universitas Islam Batik Surakarta
[2]Politeknik Perkeretaapian Indonesia
[1]muktibeny@gmail.com

Abstract

This study aims to analyze the existence of the ITE Law and Regulatory Efforts in the face of cyber attacks. Currently, technology is developing so rapidly, therefore, it is necessary to provide protection for current IT users so that users always feel protected by Indonesian Law. This research uses normative legal research. In terms of its nature, this research includes legal research that is descriptive in nature. Analysis of the formulation of the problem is carried out prescriptively using Grammatical interpretation and systematic interpretation. The enactment of the ITE Law is the first cyber law in Indonesia which aims to provide legal certainty for the community and prevent crimes caused by information technology for its users. The special law on cyber crime is one of the ideal cyber crime criminalization policies in Indonesia which contains general rules that apply to all crimes that apply in the field of information and communication technology, crimes related to the confidentiality of data or computer systems. Law enforcement is an important aspect in a country. In this case, the POLRI as a law enforcer that has the function, duty and authority to realize public security and order, including taking firm action in law enforcement against cyber crimes.

Keyword: Information Technology; Cyber Law; Cyber Attack

e-ISSN : 2621-4105

A. PENDAHULUAN

Globalisasi telah menjadi pendorong terciptanya era perkembangan teknologi informasi. Kecepatan perkembangan teknologi informasi ini telah menyebar di seluruh negara-negara di dunia, mulai dari negara-negara maju seperti di daratan Eropa dan Amerika sampai ke negara-negara berkembang seperti di sebagian daratan Asia, Afrika, serta Amerika Latin telah memacu perkembangan teknologi informasi pada masyarakatnya masing-masing. Teknologi informasi memiliki kedudukan atau peran sangat penting dalam suatu negara, sehingga perkembangan teknologi mendapat tempat yang penting bagi kemajuan dan perkembangan negara yang bersangkutan.

Walaupun demikian perkembangan teknologi informasi ibarat kata seperti pedang bermata dua, di satu sisi membawa dampak positif dan di sisi lain membawa dampak negatif. Perkembangan teknologi informasi telah mengakibatkan perubahan perilaku pada masyarakat. Selain itu, perkembangan teknologi informasi menjadikan dunia seakan tanpa batas (*borderless*).[1] *Cyberspace* juga menjadi salah satu sumber dari berbagai ancaman kedaulatan suatu negara. Ancaman tesebut dapat bersumber dari pemerintahan, individu maupun pengusaha yang bertujuan memperoleh keuntungan sendiri. Dunia saat ini tidak lagi memandang militer sebagai satu-satunya potensi ancaman, melainkan mulai menaruh perhatian terhadap ancaman yang bersifat non-militer, yakni salah satunya ancaman *cyber*. *Cyberspace* dapat menjadi ancaman bagi suatu negara karena dapat digunakan untuk mencuri informasi, propaganda, provokasi, maupun serangan terhadap informasi di berbagai bidang seperti data perbankan, jaringan militer maupun sistem pertahanan negara. Tanpa adanya penguasaan atau pengawasan terhadap *cyberspace* sangat mungkin terjadinya gangguan stabilitas keamanan dan pertahanan suatu negara.

Penelitian ini terkait dengan penelitian Handrini Ardiyanti (2014) yang berjudul *Cyber-Security* Dan Tantangan Pengembangannya Di Indonesia. Penelitian ini membahas tentang bagaimana kebijakan *cyber-security* yang telah dijalankan di Indonesia selama ini dan bagaimana prospek dan tantangan bagi pengembangan kebijakan *cyber-security* di Indonesia. Secara nasional, terdapat sejumlah permasalah terkait dengan pembangunan cyber-security yang tangguh di antaranya lemahnya

[1]Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (CyberCrime), cet. Ke-2*, PT Raja Grafindo Persada, 2013, Jakarta, hal 2.

e-ISSN : 2621-4105

pemahaman penyelenggara negara atan security terkait dengan dunia *cyber* yang memerlukan pembatasan pengunaan layanan yang servernya berada di luar negeri dan diperlukan adanya pengunaan secured system; belum adanya legalitas yang memadai terhadap penanganan penyerangan di dunia *cyber;* tata kelola kelembagaan *cyber-security* secara nasional yang masih parsial dan tersebar serta tidak adanya koordinasi yang baku dalam penanganan masalah *cyber-security*; masih lemahnya industri kita dalam memproduksi dan mengembangkan perangkat keras atau hardware terkait dengan teknologi informasi.[2]

Agus Subagyo (2015) dalam penelitiannya yang berjudul Sinergi Dalam Menghadapi Ancaman *Cyber Warfare*, menyimpulkan bahwa ancaman *Cyber Warfare* menyadarkan setiap negara di dunia, termasuk Indonesia untuk membentuk tentara *cyber*, karena ancaman *Cyber Warfare* tidak bisa dihadapi dengan jumlah persenjataan, alutsista dan jumlah tentara yang banyak dan canggih, melainkan diperlukan tentara *cyber* yang memahami teknologi informasi, komunikasi, komputer, internet, dan media sosial. Ancaman *Cyber Warfare* sudah saatnya mendorong Indonesia untuk menyusun ulang sistem pertahanan yang berbasis pada *cyber* atau *cyber defence* dan *cyber security*, yang tentunya memerlukan persiapan yang matang dan sistematis dengan dukungan dari berbagai pihak dengan ujung tombak kementerian pertahanan dan TNI. Sinergitas dalam menghadapi ancaman *Cyber Warfare* merupakan sebuah keniscayaan dan keharusan bagi Indonesia. Kementerian pertahanan harus mampu menjadi ujung tombak dalam mempelopori sinergitas antar berbagai komponen bangsa untuk melawan ancaman *Cyber Warfare*. Mekanisme pembangunan jalinan komunikasi, koordinasi, jaringan, dan kerja sama teknis harus digalakkan oleh Kementerian Pertahanan untuk membentuk komunitas pertahanan *cyber* (*cyber defence community*) yang dapat menangkal, mendeteksi, menangkis, dan mencegah secara dini berbagai potensi serangan ancaman *Cyber Warfare*.[3]

Sedangkan penelitian yang dilakukan oleh Iqbal Ramadhan (2019) yang berjudul Strategi Keamanan *Cyber Security* Di Kawasan Asia Tenggara: *Self-Help* Atau Multilateralism?. Penelitian ini lebih fokus membahas membahas strategi seperti apakah

[2]Handrini Ardiyanti, *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*, Jurnal Politica 5 (1), 2014. http://dx.doi.org/10.22212/jp.v5i1.336

[3]Agus Subagyo, *Sinergi Dalam Menghadapi Ancaman Cyber Warfare*, Jurnal Pertahanan 5 (1), 2015. http://dx.doi.org/10.33172/jpbh.v5i1.350

e-ISSN : 2621-4105

yang paling tepat dalam menjaga keamanan *cyber* di kawasan Asia Tenggara. Dalam menjawab *research question*, peneliti menggunakan pendekatan *mainstream* seperti *neorealism* dan *neoliberal*. Pada intinya, negara yang tergabung sebagai anggota ASEAN perlu mengembangkan kemampuan *power* teknologinya tanpa mengesampingkan pentingnya kerja sama antar negara.[4]

Seiring dengan adanya pengaruh perkembangan teknologi informasi, terciptanya suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Indonesia sudah memiliki peraturan perundang-undangan yang mengatur persoalan berkaitan dengan ruang lingkup teknologi informasi, yakni Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, selanjutnya disebut sebagai UU ITE. Namun, peraturan tersebut belum mampu mengatur persoalan yang mencakup aspek *cyberspace* yang begitu luas.[5] UU ITE hanya mengakomodir persoalan kejahatan di dunia maya terbatas pada konten illegal, akses illegal, penyadapan illegal, gangguan data, gangguan sistem, penyalahgunaan perangkat, dan *computer fraud*. Dalam UU ITE belum diatur mengenai serangan-serangan siber yang dapat mengganggu stabilitas keamanan dan pertahanan Indonesia.

Pada tahun 2013 Indonesia menjadi korban penyadapan oleh badan intelijen Australia berdasarkan bocoran dokumen dari seorang mantan anggota *National Security Agency* (NSA) Amerika Serikat, Edward Snowden. Dokumen tersebut berisi sejumlah target penyadapan percakapan telepon oleh Australia, yang salah satunya ialah Presiden Susilo Bambang Yudhoyono beserta Sembilan orang terdekat dalam lingkaran presiden.[6] Kemudian, Lembaga Indonesia *Security Incidents Response Team on Internet Infrastructure* (ID-SIRTII) mencatat bahwa ada sekitar 48,4 juta serangan cyber (*cyber attack*) terhadap Indonesia pada tahun 2014. Selanjutnya, pada tahun 2015 tercatat bahwa ada sejumlah serangan yang ditujukan kepada situs resmi pemerintahan seperti kesad.mil.id, paspampres.mil.id, revolusimental.go.id dan Indonesia menjadi negara terbesar dengan jumlah komputer yang terjangkit *malware* pada tahun yang sama.[7]

---

[4]Iqbal Ramadhan, *Strategi Keamanan Cyber Security Di Kawasan Asia Tenggara: Self-Help Atau Multilateralism?,* Jurnal Asia Pacific Studies 3 (2), 2019. https://doi.org/10.33541/japs.v3i1.1081

[5]David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari, "*Diplomasi Pertahanan Indonesia dalam Pencapaian CyberSecurity Melalui ASEAN Regional Forum On CyberSecurity Initiative",* Jurnal Penelitian Politik 13 (1), 2016, hal 3. DOI: https://doi.org/10.14203/jpp.v13i1.250

[6]*Ibid.*

[7]*Ibid*

e-ISSN : 2621-4105

Persoalan yang juga menjadi masalah dalam kasus-kasus serangan siber terhadap Indonesia tersebut diatas ialah terkait yurisdiksi pemberlakuan hukum pidana nasional Indonesia terhadap kejahatan serangan siber terutama yang dilakukan adalah bersifat lintas negara. Yurisdiksi pemberlakuan hukum pidana nasional ini erat kaitannya dengan antara lain: (1) kedaulatan suatu negara; (2) asas-asas pemberlakuan hukum pidana nasional suatu negara; (3) teori tempat terjadinya tindak pidana (*locus delicti*); dan (4) peng-ratifikasian konvensi Internasional.

Kedaulatan suatu negara memiliki makna bahwa negara tersebut memiliki kekuasaan tertinggi di dalamnya. Dapat dikatakan bahwa tidak ada kekuasaan yang lebih tinggi dari kekuasaan tertinggi suatu negara yang bersangkutan. Menurut asal katanya, kedaulatan memang berarti kekuasaan tertinggi. Negara berdaulat memang berarti bahwa negara itu tidak mengakui suatu kekuasaan yang lebih tinggi dari pada kekuasaannya sendiri. Walaupun demikian, kekuasaan tertinggi ini memiliki batas-batasnya. Pada konteks masyarakat internasional saat ini, ruang berlaku kekuasaan tertinggi suatu negara dibatasi oleh batas wilayah negara itu sendiri, artinya suatu negara hanya memiliki kekuasaan tertinggi di dalam batas wilayahnya atau dengan kata lain, kedaulatan suatu negara berakhir dimana kekuasaan suatu negara lain mulai.[8]

Penelitian ini melengkapi penelitian sebelumnya yang meneliti mengenai permasalahan serangan siber di Indonesia. Perlu adanya suatu upaya penataan regulasi di bidang teknologi informasi agar dapat mencakup ruang lingkup teknologi informasi (*Cyberspace*) yang sangat luas, terutama fokus terhadap kejahatan serangan siber. Selain itu, dalam upaya penataan regulasi pemberlakuannya harus sekuat mungkin yang dimana hal ini diimbangi dengan memperhatikan dan tetap dalam koridor atau kaidah yang berlaku dalam pemberlakuan hukum nasional suatu negara. Penelitian ini bertujuan untuk menganalisis keberadaan UU ITE dan Upaya Regulasi dalam menghadapi Serangan Siber. Saat ini, teknologi berkembang dengan begitu pesat,oleh karena itu, perlunya diadakannya perlindungan terhadap para pengguna IT saat ini agar para pengguna selalu merasa dilindungi oleh hukum Indonesia.

[8]Mochtar Kusumaatmaja dan Etty R. Agoe, *Pengantar Hukum Internasional, cet, ke-2*, PT. Alumni, 2010, Bandung, hal 17-18.

e-ISSN : 2621-4105

B. PERMASALAHAN

1. Bagaimana regulasi bidang teknologi informasi di Indonesia dalam menghadapi tindak pidana siber?
2. Apa upaya regulasi khusus di bidang teknologi informasi dalam menghadapi serangan siber (*CyberAttack*)?

C. METODE PENELITIAN/LANDASAN TEORITIS

Menurut Marzuki, penelitian hukum (*legal research*) dalam bahasa Belanda disebut *rechtsonderzoek*.[9] Penelitian ini menggunakan penelitian hukum normatif. Penelitian hukum normatif adalah penelitian yang dilakukan dengan cara meneliti berdasarkan data-data sekunder atau data kepustakaan. Ditinjau dari sifatnya penelitian ini termasuk penelitian hukum yang bersifat deskriptif, maksudnya adalah suatu penelitian yang dimaksudkan untuk memberikan data-data yang seteliti mungkin tentang manusia, keadaan atau gejala lainnya. Penelitian ini menggunakan pendekatan kualitatif. Menurut Soerjono Soekanto, pendekatan kualitatif adalah suatu penelitian yang menghasilkan data deskriptif analisis, yaitu apa yang dinyatakan responden secara tertulis atau lisan dan juga perilaku nyata, yang diteliti dan dipelajari sebagai sesuatu yang utuh. Penelitian ini menggunakan teknik studi pustaka yaitu, mempelajari buku-buku, literature, peraturan perundang-undangan, jurnal penelitian, hasil penelitian terdahulu dan bahan kepustakaan lain yang berkaitan dengan masalah yang sedang dikaji.

D. PEMBAHASAN

A. Regulasi Bidang Teknologi Informasi di Indonesia Saat Ini dalam Menghadapi Tindak Pidana Siber

1. Analisis Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Disahkannya UU ITE pada 21 April 2008 merupakan hukum siber pertama di Indonesia yang pembentukannya bertujuan untuk memberikan kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik, mencegah terjadinya kejahatan berbasis teknologi informasi serta melindungi masyarakat pengguna jasa yang menggunakan teknologi informasi dan komunikasi. UU ini terdiri dari 54 pasal yang terbagi menjadi 13 bab. Ketentuan yang mengatur rumusan terkait

[9] Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi*, Prenada Media, Jakarta, 2017, hal 55.

e-ISSN : 2621-4105

kriminalisasi perbuatan yang dikategorisasikan sebagai tindak pidana siber terdapat dalam Bab VII tentang Perbuatan yang Dilarang Pasal 27 – Pasal 37 beserta sanksi pidananya dalam Bab XI tentang Ketentuan Pidana Pasal 45 – Pasal 52. [10] Berdasarkan Pasal 1 angka (1) UU ITE yang termasuk ke dalam informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto *electronic data interchange (EDI),* surat elektronik, telegram, teleks, *telecopy,* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Sementara itu menurut Pasal 1 angka (4) disebutkan yang dimaksud dengan dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makan atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Di dalam Pasal 5 ayat (1), ayat (2), dan ayat (3) menjelaskan penguatan eksistensi alat bukti elektronik ini sebagai alat bukti yang sah, yaitu:

a) Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
b) Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia.
c) Informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam undang-undang ini.

Meski UU ITE telah mengatur jenis-jenis perbuatan yang dapat dikriminalisasi sebagai sebuah tindak pidana, penambahan jenis alat bukti

[10] Akbar Kurnia Putra. (2014). *Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional*, hlm 105.

e-ISSN : 2621-4105

baru, dan imunisasi eksistensi alat bukti elektronik, namun masih terdapat permasalahan hukum dalam menanggulangi tindak pidana siber di Indonesia, yaitu:

a) Permasalahan dalam menentukan tempat terjadinya tindak pidana (*locus delicti*) dan waktu kejadian tindak pidana (*tempus delicti*). Dalam tindak pidana siber, penyidik mengalami kesulitan dalam menentukan lokasi atau tempat yang akurat terjadinya tindak pidana. Karena pelaku dapat menghapus atau mengubah "jejak digital" perangkat yang dipergunakannya untuk melakukan tindak pidana siber maupun mensetting lokasi yang berbeda dengan lokasi yang sebenarnya. Begitu pun halnya dengan dalam menentukan waktu kejadian perkara. Penyidik memiliki kesulitan dalam menentukan secara pasti kapan terjadinya perbuatan tersebut karena biasanya pelaku memililki kemampuan untuk mengubah atau mengacaukan waktu dan tanggal perbuatannya dilakukan.[11]

b) Permasalahan barang bukti juga menjadi promblematik tersendiri bagi aparat penegak hukum. Barang bukti yang dicari adalah terkait dengan segala sesuatu yang dipergunakan untuk mempersiapkan, melakukan dan hasil tindak pidana siber sangat sulit untuk melacaknya karena dibalik kecanggihan sistem jaringannya internet juga memiliki celah bagi orang-orang yang memiliki keahlian untuk menghapus atau memalsukan identitasnya di dunia maya. Di sisi lain, teknologi informasi adalah teknologi dengan sistem yang terbuka yang tidak mustahil untuk dapat dibajak atau dikloning secara ilegal, di mana setiap orang yang memiliki keahlian di bidang tersebut dapat memanipulasi data, mengubah data, seperti menjadikan data palsu (*fake data*) menjadi data yang asli. Sementara itu Asril Sitompul menyampaikan siapa dan bagaimana bentuk kesaksian yang dapat diajukan untuk peristiwa hukum yang terjadi di media internet.

c) Tindak pidana siber ini memiliki karakteristik dilakukan oleh satu orang

[11] Sudarwanto, Al Sentot, *"Cyber Bullying : Kejahatan Dunia Maya yang Terlupakan*., Jurnal Hukum Pro Justitia 27 (1), 2009.

e-ISSN : 2621-4105

dalam ruangan tertutup, sehingga untuk beberapa bentuk tindak pidana siber biasa penyidik sulit untuk mendapatkan saksi yang menyaksikan langsung pelaku saat sedang melakukan tindak pidana siber, sehingga saksi yang dimiliki terbatas pada saksi korban. Dalam hal tindak pidana siber terkait dengan perbankan, bisa saja pihak perbankan cenderung menutupi telah terjadinya serangan tindak pidana siber terhadap mereka, karena hal ini menjadi aib yang dapat menghilangkan kepercayaan masyarakat secara umum dan nasabah penyimpan dana di bank tersebut.

d) Yurisdiksi suatu negara yang diakui hukum internasional dalam pengertian konvensional, didasarkan pada batas-batas geografis, sementara komunikasi multimedia bersifat internasional, multi yurisdiksi, dan tanpa batas, sehingga sampai saat ini belum dapat dipastikan bagaimana yurisdiksi suatu negara dapat diberlakukan terhadap komunikasi multimedia sebagai salah satu pemanfaatan teknologi informasi. Dengan demikian terkait kewenangan hukum (yurisdiksi) dalam penindakannya juga dapat menimbulkan permasalahan yang serius, hal ini disebabkan karena internet tidak mengenal batas wilayah. Sehingga mungkin saja terjadi tarik menarik kewenangan oleh beberapa negara yang merasa dirugikan oleh tindak pidana siber dalam penegakan hukumnya.

e) Terbatasnya kemampuan penegak hukum dalam hal ini penyidik Polri dalam menangani tindak pidana siber ini, keterbatasannya baik dalam hal sumber daya manusianya maupun dalam hal peralatan-peralatannya. Unit kejahatan siber di kepolisian pun baru terbentuk secara khusus di Reskrim Polri di bawah Direktorat Tindak Pidana Siber pada tanggal 3 Februari 2017. Sebelumnya tindak pidana siber ini penanganan berada di Direktorat Tindak Pidana Ekonomi Khusus (DIT TIPPID EKSUS) di Subdirektorat V yang menangani tindak pidana antara lain tindak pidana yang terkait dengan *cyber crime*, tindak pidana informasi dan transaksi elektronik.[12].

[12]Muhammad Prima Ersya, "*Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia",* Journal of Moral and Civil Education 1 (1), 2017, hal 60. https://doi.org/10.24036/8851412020171112

e-ISSN : 2621-4105

2. Regulasi Tindak Pidana Siber di Beberapa Negara

Negara-negara di dunia yang telah memiliki undang-undang yang mengatur tindak pidana siber yang kemudian dimasukkan ke dalam undang-undang nasionalnya juga mengatur tentang yurisdiksi dengan teori dan pendekatan yang berbeda atau prinsip yurisdiksi yang berbeda-beda. Sebagai contoh India. Pengaturan yurisdiksi terhadap tindak pidana siber di India diatur dalam Act No. 21 of 2000 tentang *The Information Technology Act* (IT ACT) tahun 2000. Peraturan tersebut kemudian diamendemen melalui *Information Technology Act* 2008 *Act* No. 10 tahun 2009. Dalam undang-undang ini mengatur yurisdiksi dalam Pasal 1 ayat (2). Rumusan ketentuan Pasal 1 ayat (2) Act India adalah sebagai berikut:

> *"It shall extend to the whole of India and, save otherwise provided in this Act, it applies also to any offense or contravention thereunder comitted outside India by any person"*

Berdasarkan ketentuan dalam rumusan Pasal 1 ayat (2) undang-undang tersebut memberlakukan yurisdiksi kriminal berdasarkan prinsip teritorial dan ekstrateritorial. Dalam rumusan ini tidak ada penjelasan mengenai prinsip-prinsip yurisdiksi yang digunakan untuk memberlakukan yuridiksi ekstrateritorial sehingga memungkinkan terjadinya penafsiran dengan berdasarkan teori atau prinsip dalam hukum internasional yang berlaku. Singapura juga merupakah salah satu negara yang sudah memilik undang-undang yang mengatur yurisdiksi berlakunya tindak pidana siber. Pengaturan tersebut terdapat dalam *Computer Misuse Act,* amandemen Act No. 42 tahun 2005. Prinsip yuridiksi yang menjadi dasar berlakunya hukum pidana Singapura berdasarkan ketentuan Pasal 11 *Computer Misuse Act* meliputi prinsip teritorial, prinsip nasional aktif, dan prinsip nasional pasif dan prinsip perlindungan. Begitu pun halnya dengan Australia. Tindak pidana siber diatur secara khusus dalam Act No. 161 tahun 2001 tentang *Cybercrime Act* 2001. Penentuan yurisdiksi tindak pidana siber dijelaskan secara rinci dalam Article 476.3 (*geographical jurisdiction)* yang didasarkan pada Section 15.1 *Extended Geographical Jurisdiction - Category A* di *Criminal Code*1995.[13]

[13] Iqbal Ramadhan, *Op. Cit* hlm.188.

e-ISSN : 2621-4105

Begitu pun halnya dengan Australia. Tindak pidana siber diatur secara khusus dalam Act No. 161 tahun 2001 tentang *Cybercrime Act* 2001. Penentuan yurisdiksi tindak pidana siber dijelaskan secara rinci dalam Article 476.3 (*geographical jurisdiction)* yang didasarkan pada Section 15.1 *Extended Geographical Jurisdiction - Category A* di *Criminal Code*1995. Penentuan yurisdiksi tindak pidana siber dijelaskan dalam Article 476.3 (*geographical jurisdiction)* dinyatakan bahwa "Section 15.1 *Extended Geographical Jurisdiction - Category A* diterapkan terhadap tindak pidana yang diatur di dalam Act No. 161 tahun 2001. Berdasarkan ketentuan Article 476.3 *Cybercrime Act 2001* aturan mengenai yurisdiksi terhadap tindak pidana siber berdasarkan atas ketentuan yurisdiksi di *Criminal Code 1995*.[14]

Ketiga negara sebagaimana telah dijelaskan di atas merupakan contoh negara-negara yang sudah memiliki undang-undang khusus tindak pidana siber. Penting adanya peraturan tersebut sebagai payung hukum dalam menyelesaikan perkara tindak pidana siber yang merupakan jenis tindak pidana yang masih terbilang baru yang memungkinkan dapat mengganggu stabilitas keamanan negara. Namun sayangnya, masih banyak negara belum memiliki undang-undang khusus tersebut atau meratifikasi Konvensi Budhapest tentang *Cybercrime* 2001, Indonesia salah satunya.[15]

B. Upaya Regulasi Khusus di Bidang Teknologi Informasi dalam Menghadapi Serangan Cyber (*CyberAttack*)

1. Peratifikasian Konvensi Dewan Eropa Tentang *Convention on Cyber Crime*, Budhapest, Hongaria 2001 oleh Indonesia

Dewan Eropa adalah salah satu organisasi supranasional di Eropa. Pada tahun 1985 dibentuk komite ahli *Europe Committee on Crime Problems* untuk mempertimbangkan berbagai masalah hukum yang ditimbulkan oleh kejahatan komputer. Konvensi Dewan Eropa tahun 2001 saat ini merupakan regulasi pertama yang mengatur tindak pidana siber dan menjadi pedoman dalam regulasi tindak pidana siber dalam hukum nasional. Oleh karena itu,

[14] Maulin Janti Islami,*Tantangan dalam Implemtasi Stratgei Keamanan SIBER Nasional Indonesia ditinjau dari Penilaian Global Cybersecurity* Index,Jurnal Hukum 1 (1) 2017, hlm.142.

[15]Iqbal Ramadhan, *Peran Institusi Internasional dalam Penanggulangan Ancaman Cyber*, Jurnal Populis 2 (4) 2017, hlm.87.

e-ISSN : 2621-4105

Indonesia sebagai negara yang belum meratifikasi konvensi tersebut untuk kedepannya perlu adanya peratifikasian terhadap konvensi Dewan Eropa tahun 2001 ini. Alasannya ialah untuk memperkuat landasan hukum serta memperkuat berlakunya Undang- Undang khusus tindak pidana siber terhadap pelaku kejahatan yang berada di luar negara Indonesia. Tentunya, ratifikasi ini nantinya harus sesuai dengan prosedur yang berlaku baik itu menurut hukum internasional (Konvensi Wina 1969) maupun menurut hukum nasional (pasal 11 UUD NKRI 1945).

2. Pembentukan Undang-Undang Khusus tentang Tindak Pidana Siber

Kebijakan kriminalisasi tindak pidana siber dalam hukum pidana nasional harus dilakukan secara integral sebagai bagian dari sistem hukum pidana substantif Indonesia dengan memperhatikan karakteristik dan kategorisasi tidak pidana siber. Undang-Undang ITE tidak mengatur secara khusus hal-hal yang menyangkut cyber crime, Pemerintah dalam membentuk Undang-Undang ITE ini masih menggunakan pendekatan politis pragmatis, bukan menggunakan pendekatan kebijakan publik yang melibatkan lebih banyak kalangan.[16] UU ITE ini lebih banyak mencermati transaksi elektronik yang dipakai dalam dunia bisnis, tidak lebih. Padahal siapa pun tahu bahwa dunia siber (*cyberword*) lebih luas dari sekedar transaksi elektronik. Ketentuan-ketentuan yang menyangkut tentang pelaksanaan perbuatan jahat atau perbuatan yang dapat dihukum termasuk dalam Undang-Undang ITE seperti kelalaian atau khilaf. Undang-Undang ITE ini juga tidak mengatur kapan kadaluwarsa perbuatan pidana kejahatan hacking.[17] Kebijakan kriminalisasi tidak pidana siber di Indonesia yang ideal adalah dibentuknya Undang-Undang khusus tentang Tindak Pidana Siber. Dalam Undang-Undang Khusus ini dirumuskan aturan umum yang akan berlaku untuk semua tidak pidana di bidang teknologi informasi dan komunikasi, tindak pidana yang berkaitan dengan kerahasiaan, keutuhan, dan ketersediaan data atau sistem komputer/sistem elektronik, pedoman pemidanaan, hukum acara yang

[16] Petrus Reinhart Gollose, "*Perkembangan Cyber Crime Dan Upaya Penanganannya Di Indonesia Oleh Polri*". Buletin Hukum Perbankan. 4 (2), 2006.

[17] Aan Andrew Johanes Pahajow, "*Pembuktian Terhadap Kejahatan Dunia Maya dan Upaya Mengatasinya Menurut Hukum Positif di Indonesia",* Jurnal Lex Crimen 5 (2), 2016, hal 97.

e-ISSN : 2621-4105

mengatur prosedur penyelidikan dan penyidikan di bidang teknologi informasi dan komunikasi, termasuk penggeledahan dan penyitaan alat bukti digital, kerja sama internasional seperti ekstradisi, bantuan hukum timbal balik, dan kerja sama internasional lainya dalam penyelidikan dan penyidikan tindak pidana siber.

a) Ruang Lingkup Berlakunya Undang-Undang Tindak Pidana Siber
   1) Undang-undang ini berlaku terhadap setiap orang yang melakukan tindak pidana siber dan akibat perbuatannya di wilayah negara Republik Indonesia yang mengancam stabilitas keamanan dan pertahanan Republik Indonesia.
   2) Undang-Undang ini juga berlaku terhadap tindak pidana pendanaan Siber yang terjadi di wilayah Negara Kesatuan Republik Indonesia apabila:
      (a) dilakukan oleh warga negara Indonesia atau Warga Negara Asing;
      (b) terkait dengan Tindak Pidana siber terhadap warga negara Indonesia;
      (c) terkait dengan Tindak Pidana siber terhadap fasilitas pemerintah Indonesia;
      (d) terkait dengan Tindak Pidana Siber yang dilakukan sebagai upaya untuk memaksa pemerintah Indonesia melakukan atau tidak melakukan suatu tindakan;
      (e) dilakukan oleh setiap orang yang tidak memiliki kewarganegaraan dan bertempat tinggal di wilayah Negara Kesatuan Republik Indonesia.

b) Jenis-Jenis Kejahatan yang masuk ke dalam Tindak Pidana Siber diantaranya: [18]
   1) *Cyber-Terorism*

      National Police Agency of Japan (NPA) mendefinisikan *Cyber Terrorism* sebagai electronic *attack through computer networks*

[18]Muhammad Prima Ersya, *Op.Cit* hlm 60.

e-ISSN : 2621-4105

againt critical infrastructures that have potential critical effect on social and economic activites of the nation

2) *Cyber-pornography*:Penyebarluasan*obscenematerials* termasuk porno- graphy, indecent exposure, dan childpornography.
3) *Cyber-harassment*: pelecehan seksual melalui e-mail, website, atau chatt program
4) *Cyber-Stalking*: Crimes of stalking melalui penggunaan komputer dan internet.
5) *Cyber Squatting*:diartikan sebagai mendapatkan, memperjualbelikan, atau menggunakan suatu nama domain dengan itikad tidakbaik.
6) *Hacking*: penggunaan *Programming abilities* dengan maksud yang bertentangan denganhukum
7) *Carding* ("*credit-card fraud*"): melibatkan berbagai macam aktivitas yang melibatkan kartu kredit, *Carding* muncul ketika seseorang yang bukan pemilik akun kartu kredit menggunakan kartu krdit tersebut secara melawanhukum
8) *Government and freelance spying* termasuk *corporateespionage*
9) *Organized crime* yaitu menggunakan internet untuk memfasilitasi kegiatan ilegal mereka (smugling, jual beli senjata,narkotika)
10) *Academic cheating* dan *sicentific miscoduct* untuk melakukan tindak pidana plagiarisme

c) Aparat Penegak Undang-Undang Khusus Tindak Pidana Siber

Penegakan hukum merupakan salah satu aspek terpenting dalam suatu negara hukum[19], karena dengan penegakan hukum maka tujuan hukum, yakni keadilan, kepastian hukum dan kemanfaatan akan dapat dirasakan oleh masyarakat. Polri sebagai penegak hukum memiliki fungsi, tugas, dan wewenang untuk mewujudkan keamanan dan ketertiban dalam negeri yang meliputi terpeliharanya keamanan dan ketertiban masyarakat, dan tegaknya hukum,terselenggaranya

[19] Aan Andrew Johanes Pahajow, *Pembuktian Terhadap Kejahatan Dunia Maya dan Upaya Mengatasinya Menurut Hukum Positif di Indonesia*, Lex Crimen 5 (2), 2016, hlm 97.

e-ISSN : 2621-4105

perlindungan, pengayoman dan pelayanan masyarakat, serta terbinanya ketentraman masyarakat dengan menjunjung tinggi hak asasi manusia, termasuk bertindak tegas dalam penegakan hukum terhadap tindak pidana siber ini. Pasal 2 UU No. 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia menjelakan bahwa Fungsi kepolisian adalah salah satu fungsi pemerintahan negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan kepadamasyarakat.[20]

d) Pemberlakuan Regulasi Khusus dalam Menghadapi *Cyber Attack* Terhadap Pelaku Kejahatan yang Berada di Luar Indonesia

Pemberlakuan hukum nasional suatu negara terhadap pelaku kejahatan lintas negara menjadi suatu hal yang penting untuk diperhatikan karena jika tidak cermat dalam hal ini akan terjadi yang disebut sebagai benturan yurisdiksi antara hukum suatu negara dengan negara lain. Terdapat dua hal yang menjadi penentu hukum negara mana yang berlaku untuk menindak pelaku kejahatan lintas negara yaitu (1) Teori tempat terjadinya suatu tindak pidana, dan (2) Asas-Asas pemberlakuan hukum nasional yang dianut suatu negara. Kedua hal ini menurut kami saling menopang satu sama lainnya, teori tempat terjadinya tindak pidana yang cocok dengan tindak pidana siber nantinya akan diperkuat dengan salah satu asas pemberlakuan hukum nasional suatu negara. Jika hal ini disamakan dengan konteks hukum nasional, maka dalam hal ini dicari pengadilan mana yang berwenang secara 'kompetensirelatif'.[21]

Dengan adanya dasar seperti ini, maka regulasi khusus terkait *cyber attack* bukanlah hal yang mustahil untuk ditegakkan terhadap pelaku kejahatan yang berada di luar Indonesia.[22]

1) Tempat Terjadinya Tindak Pidana (*Locus Delicti*) dalam Hal Serangan Siber (*CyberAttack*)

[20]David Putra Setyawan, *Op. Cit*
[21]Soedarto. 2013, *Hukum Pidana I.* Semarang: Yayasan Soedarto d/a Fakultas Hukum Universitas Diponegoro. hlm. 61.
[22]Kristian Aji Nugroho, *Pengaruh Cyber Attack terhadap kebijakan Cyber Security Amerika Serikat*, Jurnal of International Relations 3 (4), 2018.

e-ISSN : 2621-4105

Pelaksanaan atau pemberlakuan hukum nasional suatu negara erat kaitannya dengan tempat terjadinya tindak pidana (*locus delicti*). *Locus Delicti* menjadi masalah apabila pelaku tindak pidana dan penyelesaian tindak pidana tidak berada dalam satu tempat yang sama, tetapi di dua atau lebih tempat yang berbeda. Dalam tindak pidana siber, tindakan atau perbuatan dapat dilakukan dimanapun karena dilakukan dengan komputer atau internet atau sistem jaringan yang dapat menimbulkan akibat yang bersifat lintas batas.

Penetapan *locus delicti* penting berkaitan dengan:

(a) Menentukan berlakunya hukum pidana nasional berkaitan dengan penerapan asas-asas yurisdiksi kriminal;
(b) Dalam hukum ekstradisi, suatu negara berwenang untuk menolak permintaan ekstradisi berdasarkan alasan bahwa tindak pidana terjadi diwilayahnya;
(c) Menentukan kompetensi relatif; dan
(d) Menentukan apakah perilaku tersebut memenuhi unsur tindak pidana jika disyaratkan unsur tertentu.[23]

KUHP yang berlaku di Indonesia saat ini tidak mengatur terkait *locus delicti*, masalah ini berkembang dalam doktrin ilmu hukum pidana.[24] Sebagaimana telah dijelaskan pada bagian sebelumnya, bahwa terdapat teori *locus delicti* yaitu teori perbuatan materiil, teori alat yang digunakan, dan teori akibat.[25]

2) Berdasarkan ketiga teori tempat terjadinya tindak pidana (*locus* delicti) diatas, menurut penulis regulasi khusus yang nantinya akan dibentuk terkait tindak pidana siber berupa *cyber attack* akan lebih sesuai jika digunakan teori akibat. Teori akibat dipandang yang paling sesuai jika diterapkan pada tindak pidana siber adalah karena tindak pidana siber merupakan delik yang bersifat materiil atau delik yang menitikberatkan pada suatu akibat. Pertimbangan berikutnya

[23]Sigid Suseno, "*Yurisdiksi Tindak Pidana Siber",* PT. Rafika Aditama, 2012, Bandung, hal 76-77.
[24]*Ibid.*
[25] Eddy O.S. Hiariej, "*Prinsip-Prinsip Hukum Pidana."* Cahaya Atma Pustaka, 2014, Yogyakarta, hal 250.

e-ISSN : 2621-4105

ialah terkait untuk memperkuat berlakunya hukum nasional terhadap pelaku tindak pidana siber yang berada di luar negara Indonesia. Hal ini bukanlah tanpa alasan melainkan pelaku kejahatan siber yang berada di luar negara Indonesia bukanlah tidak mungkin melakukan perbuatannya atas perintah dari negara yang bersangkutan. Jika digunakan teori *locus delicti* yang lain (teori pelaku dan teori alat) pelaku kejahatan tersebutakan diuntungkan. Tidak hanya sampai disitu, teori akibat ini harus diperluas tidak hanya berkaitan dengan delik materiil nya saja tetapi juga untuk jenis tindak pidana lain yang menimbulkan pengaruh atau dirasakan oleh suatu negara. Asas-Asas yang Menunjang Berlakunya Regulasi Khusus dalam Menghadapi *Cyber Attack.*[26]

Asas merupakan suatu hal yang sangat penting mengingat asas merupakan landasan berpikir untuk menunjang suatu gagasan atau suatu hal, atau dengan kata lain asas merupakan dasar. Untuk memberlakukan regulasi khusus dalam menghadapi *cyber attack*, terdapat beberapa asas yang dapat menjadi dasar pemberlakuannya, meliputi asas khusus dalam hukum pidana Internasional dan asas yurisdiksi pemberlakuan hukum pidana nasional.[27]

(a) Asas-Asas Khusus dalam Hukum Pidana Internasional

(1) Asas *au dedere au punere*, yang berarti terhadap pelaku tindak pidana internasional dapat dipidana oleh negara tempat terjadinya tindak pidana (*locus delicti*) dalam batas teritorial negara tersebut atau diserahkan atau diekstradisikan kepada negara peminta yang memiliki yurisdiksi untuk mengadili pelaku tersebut.

(2) Asas *au dedere au judicare*, yang berarti setiap negara berkewajiban untuk menuntut dan mengadili pelaku tindak pidana internasional dan berkewajiban untuk melakukan kerja sama dengan negara lain di dalam menangkap,

[26] Erman Rajagukguk. *Peranan Hukum dalam Pembangunan Pada Era Globalisasi*, Jurnal Hukum 11 (6), 1999, hlm 123.
[27] Dian Sinaga, , "*Kejahatan TerhadapBuku dan Perpustakaan*", Jurnal Visi Pustaka 6 (1), 2004, hlm.23.

e-ISSN : 2621-4105

menahan, dan menuntut serta mengadili pelaku tindak pidana internasional.[28]

(b) Asas Teritorial Diperluas dan Asas Nasional Sebagai Dasar Yurisdiksi Pemberlakuan Hukum PidanaNasional

Asas Teritorial, berdasarkan asas berlakunya hukum pidana suatu negara pada umumnya yang dianut oleh semua negara dunia adalah asas teritorial. Menurut Moeljatno, asas ini diartikan hukum pidana suatu negara berlaku bagi semua orang yang melakukan perbuatan di negara tersebut, baik oleh warga negaranya maupun warga negara asing. Dalam konteks hukum pidana nasional, hal ini tercantum jelas dalam pasal 2 KUHP "aturan pidana Indonesia berlaku bagi setiap orang yang melakukan perbuatan pidana di dalam Indonesia".

Kemudian tanggung jawab negara terhadap warga negaranya yang melakukan tindak pidana di luar negara yang bersangkutan dapat dijangkau dengan asas nasional. Regulasi khusus tindak pidana siber ini nantinya memberlakukan asas nasional sebagai upaya untuk menegakkan hukum nasional terhadap warga negara Indonesia yang melakukan tindak pidana siber dari luar negara Indonesia yang dapat mengancam keamanan serta pertahanan Indonesia.[29]

E. PENUTUP

Peraturan perundang-undangan di bidang teknologi informasi yang berlaku di Indonesia saat ini belum mengakomodir seluruh tindak pidana siber, sehingga terdapat beberapa kejahatan siber yang saat ini menjadi persoalan terhadap keamanan dan pertahanan (sebagai faktor dalam menjaga kedaulatan negara) belum diatur dalam regulasi nasional. Perlu adanya regulasi khusus terkait tindak pidana siber di Indonesia. Dalam regulasi khusus ini dirumuskan aturan umum yang akan berlaku untuk semua tidak pidana di bidang teknologi informasi dan komunikasi, tindak pidana

[28]Anis Widyawati, "*Hukum Pidana Internasional*", Sinar Grafika, 2014, Jakarta, hal. 24-25.
[29]Supanto, "*Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy*",Jurnal Yustusia 1 (5), 2016, hlm 34.
https://doi.org/10.20961/yustisia.v5i1.8718

e-ISSN : 2621-4105

yang berkaitan dengan kerahasiaan, keutuhan, dan ketersediaan data atau sistem komputer/sistem elektronik, pedoman pemidanaan, hukum acara yang mengatur prosedur penyelidikan dan penyidikan di bidang teknologi informasi dan komunikasi, termasuk penggeledahan dan penyitaan alat bukti digital, kerja sama internasional dalam mengatasi tindak pidana siber. Hal demikian dikarenakan melihat kondisi Indonesia yang rentan akan serangan siber dan terdapat celah hukum dalam menghadapi hal tersebut.

DAFTAR PUSTAKA

Buku

Aan Andrew Johanes Pahajow, *"Pembuktian Terhadap Kejahatan Dunia Maya dan Upaya Mengatasinya Menurut Hukum Positif di Indonesia",* Lex Crimen, Vol V No 2, Bagian Hukum Pidana Fakultas Hukum Universitas Sam Ratulangi, 2016, Manado.

Akbar Kurnia Putra. *Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional*. 2014.

Anis Widyawati, "*Hukum Pidana Internasional*", Sinar Grafika, 2014, Jakarta.

Budi Suhariyanto, "*Tindakan Pidana Teknologi Informasi (Cyber Crime)*", cet. ke-*2*, PT Raja Grafindo Persada, 2013, Jakarta.

Eddy O.S. Hiariej, "*Prinsip-Prinsip Hukum Pidana."* Cahaya Atma Pustaka, Yogyakarta, 2014.

Mahmud Marzuki, "*Penelitian Hukum: Edisi Revisi*", Prenada Media, Jakarta, 2017.

Mochtar Kusumaatmaja dan Etty R. Agoes, "*Pengantar Hukum Internasional*", cet. ke-2, PT. Alumni,Bandung, 2010.

Soedarto, *Hukum Pidana I.* Semarang: Yayasan Soedarto d/a Fakultas Hukum Universitas Diponegoro, 2013.

Sigid Suseno, "*Yurisdiksi Tindak Pidana Siber",* PT. Rafika Aditama, 2012, Bandung.

Ersya, Muhammad Prima. 2017

Jurnal

Aan Andrew Johanes Pahajow, *Pembuktian Terhadap Kejahatan Dunia Maya dan Upaya Mengatasinya Menurut Hukum Positif di Indonesia*, Lex Crimen 5 (2), 2016.

Agus Subagyo, *Sinergi Dalam Menghadapi Ancaman Cyber Warfare*, Jurnal Pertahanan 5 (1), 2015. http://dx.doi.org/10.33172/jpbh.v5i1.350

Erman Rajagukguk. *Peranan Hukum dalam Pembangunan Pada Era Globalisasi*, Jurnal Hukum 11 (6), 1999.

David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari, *"Diplomasi Pertahanan Indonesia dalam Pencapaian CyberSecurity Melalui ASEAN Regional Forum On CyberSecurity Initiatives",* Jurnal Penelitian Politik 13 (1), 2016. DOI: https://doi.org/10.14203/jpp.v13i1.250

e-ISSN : 2621-4105

Dian Sinaga, , "*Kejahatan TerhadapBuku dan Perpustakaan*", Jurnal Visi Pustaka 6 (1), 2004.

Handrini Ardiyanti, *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*, Jurnal Politica 5 (1), 2014. http://dx.doi.org/10.22212/jp.v5i1.336

Iqbal Ramadhan, *Peran Institusi Internasional dalam Penanggulangan Ancaman Cyber* , Jurnal Populis 2 (4), 2017.

_____, *Strategi Keamanan Cyber Security Di Kawasan Asia Tenggara: Self-Help Atau Multilateralism?*, Jurnal Asia Pacific Studies 3 (2), 2019. https://doi.org/10.33541/japs.v3i1.1081

Kristian Aji Nugroho, *Pengaruh Cyber Attack terhadap kebijakan Cyber Security Amerika Serikat*, Jurnal of International Relations 3 (4), 2018.

Maulin Janti Islami,*Tantangan dalam Implemtasi Stratgei Keamanan SIBER Nasional Indonesia ditinjau dari Penilaian Global Cybersecurity* Index,Jurnal Hukum 1 (1) 2017.

Muhammad Prima Ersya, "*Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia",* Journal of Moral and Civil Education 1 (1), 2017. https://doi.org/10.24036/8851412020171112

Petrus Reinhart Gollose, "*Perkembangan Cyber Crime Dan Upaya Penanganannya Di Indonesia Oleh Polri*". Buletin Hukum Perbankan. 4 (2), 2006.

Sudarwanto, Al Sentot, "*Cyber Bullying : Kejahatan Dunia Maya yang Terlupakan.* Jurnal Hukum Pro Justitia 27 (1), 2009.

Supanto, "*Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy*",Jurnal Yustusia 1 (5), 2016, hlm 34. https://doi.org/10.20961/yustisia.v5i1.8718