IMPLEMENTASI PERJANJIAN PERSAHABATAN DAN KERJASAMA (*TREATY OF AMITY AND COOPERATION*) INDONESIA DAN ASEAN DALAM MENGATASI KEJAHATAN SIBER

SKRIPSI

Diajukan Untuk Memenuhi Syarat
Mendapatkan Gelar Sarjana Hukum

Oleh :

Muhammad Rafi Maulana
NPM : 1806200438

FAKULTAS HUKUM

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

MEDAN

2023

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan
Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

BERITA ACARA
UJIAN MEMPERTAHANKAN SKRIPSI SARJANA
BAGI MAHASISWA PROGRAM STRATA 1

Panitia Ujian Sarjana Strata-I Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dalam sidangnya yang diselenggarakan pada hari Rabu, tanggal 20 Maret 2024, Jam 08.30 WIB sampai dengan selesai, setelah mendengar, melihat, memperhatikan, menimbang:

MENETAPKAN

NAMA	**:**	**MUHAMMAD RAFI MAULANA**
NPM	**:**	**1806200438**
PRODI/BAGIAN	**:**	**HUKUM/ HUKUM INTERNASIONAL**
JUDUL SKRIPSI	**:**	**IMPLEMENTASI PERJANJIAN PERSAHABATAN DAN KERJASAMA (*TREATY OF AMITY AND COOPERATION*) INDONESIA DAN ASEAN DALAM MENGATASI KEJAHATAN SIBER**

Dinyatakan:

(A-) Lulus Yudisium dengan predikat Baik
( ) Lulus Bersyarat, memperbaiki/Ujian Ulang
( ) Tidak Lulus

Setelah lulus, dinyatakan berhak dan berwenang mendapatkan gelar Sarjana Hukum (SH) dalam Bagian Hukum Tinternaisonal.

PANITIA UJIAN

Ketua	**Sekretaris**
Dr. FAISAL, S.H., M.Hum.	**Dr. ZAINUDDIN, S.H., M.H.**
NIDN: 0122087502	**NIDN: 0118047901**

ANGGOTA PENGUJI:

1.MIRSA ASTUTI, S.H., M.H. 1.

2.Dr. M. SYUKRAN YAMIN LUBIS, S.H., CN., M.Kn. 2.

3. MHD. NASIR SITOMPUL, S.H., M.H. 3.

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

بسم الله الرحمن الرحيم

PENDAFTARAN UJIAN SKRIPSI

Pendaftaran Skripsi Sarjana Fakulas Hukum Universitas Muhammadiyah Sumatera Utara Strata I bagi:

NAMA	:	**MUHAMMAD RAFI MAULANA NST**
NPM	:	**1806200438**
PRODI/BAGIAN	:	**HUKUM/ HUKUM INTERNASIONAL**
JUDUL SKRIPSI	:	**IMPLEMENTASI PERJANJIAN PERSAHABATAN DAN KERJASAMA (*TREATY OF AMITY AND COOPERATION*) INDONESIA DAN ASEAN DALAM MENGATASI KEJAHATAN SIBER**
PENDAFTARAN	:	**Tanggal 20 Februari 2024**

Dengan diterimanya skripsi ini, sesudah lulus dari Ujian Komprehensif, penulis berhak memakai gelar:

SARJANA HUKUM (S.H.)

Diketahui	**Pembimbing**
Dekan Fakultas Hukum	
Dr. FAISAL, S.H., M.Hum.	**MHD. NASIR SITOMPUL, S.H., M.H**
NIDN: 0122087502	**NIDN. 0118097203**

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

LEMBAR PERSETUJUAN PEMBIMBING

NAMA	:	**MUHAMMAD RAFI MAULANA NST**
NPM	:	**1806200438**
PRODI/BAGIAN	:	**HUKUM/ HUKUM INTERNASIONAL**
JUDUL SKRIPSI	:	**IMPLEMENTASI PERJANJIAN PERSAHABATAN DAN KERJASAMA (*TREATY OF AMITY AND COOPERATION*) INDONESIA DAN ASEAN DALAM MENGATASI KEJAHATAN SIBER**

Disetujui Untuk Disampaikan Kepada
Panitia Ujian Skripsi

Medan, 20 Februari 2024

Pembimbing

MHD. NASIR SITOMPUL, S.H., M.H.
NIDN. 0118097203

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred-PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

بسم الله الرحمن الرحيم

KARTU BIMBINGAN SKRIPSI MAHASISWA

NAMA : **MUHAMMAD RAFI MAULANA**
NPM : **1806200438**
PRODI/BAGIAN : **ILMU HUKUM/ HUKUM INTERNASIONAL**
JUDUL SKRIPSI : **IMPLEMENTASI PERJANJIAN PERSAHABATAN DAN KERJASAMA (TREATY OF AMITY AND COOPERATION) INDONESIA DAN ASEAN DALAM MENGATASI KEJAHATAN CYBER**

Pembimbing : **MUHAMMAD NASIR SITOMPUL, S.H., M.H**

TANGGAL	MATERI BIMBINGAN	TANDA TANGAN
13-09-2023	Abstrak dan kata kunci	
14-09-2023	Daftar isi Penutup dirapih. kesimpulan	
15-09-2023	UU dimasukkan ke pembahasan	
16-09-2023	Rumusan masalah	
18-09-2023	tinjauan Pustaka	
19-09-2023	Cara mengutip kutipan	
19-09-2023	Pembahasan isi Elemen	
20-09-2023	kesimpulan dan Saran	
21-09-2023	ACC utk Disidangkan	

Diketahui
DEKAN FAKULTAS HUKUM

(Dr. FAISAL, S.H., M.Hum.)

DOSEN PEMBIMBING

(MUHAMMAD NASIR SITOMPUL, S.H., M.H)

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400- 66224567
http://hukum.umsu.ac.id fahum@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

بسم الله الرحمن الرحيم

PERNYATAAN KEASLIAN SKRIPSI

Saya saya bertanda tangan di bawah ini:

Nama	: Muhammad Rafi Maulana
NPM	: 1806200438
Program	: Strata-1
Fakultas	: Hukum
Program Studi	: Ilmu Hukum
Bagian	: Hukum Internasional
Judul Skripsi	: Implementasi Perjanjian Persahabatan Dan Kerjasama (*Treaty Of Amity And Cooperation*) Indonesia Dan Asean Dalam Mengatasi Kejahatan Siber

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis, secara keseluruhan adalah hasil penelitian/karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya.

Dan apabila ternyata dikemudian hari data-data dari skripsi ini merupakan hasil Plagiat atau merupakan hasil karya orang lain, maka dengan ini saya menyatakan bersedia menerima sanksi akademik dari Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.

Medan, Juni 2024
Saya yang menyatakan

Muhammad Rafi Maulana

ABSTRAK

Implementasi Perjanjian Persahabatan Dan Kerjasama (*Treaty Of Amity And Cooperation*) Indonesia Dan Asean Dalam Mengatasi Kejahatan Siber

Muhammad Rafi Maulana

Kejahatan siber menjadi ancaman yang semakin nyata dan kompleks di era globalisasi dan teknologi informasi. Keberadaan internet dan teknologi digital telah membawa manfaat besar bagi masyarakat, namun juga membuka peluang baru bagi pelaku kejahatan untuk melakukan serangan siber yang merugikan. Oleh karena itu, kerjasama internasional menjadi krusial dalam menghadapi tantangan ini.

Penelitian ini bertujuan untuk menganalisis dan mengidentifikasi implementasi Perjanjian Persahabatan dan Kerjasama (Treaty of Amity and Cooperation) Indonesia dan ASEAN dalam mengatasi kejahatan siber. Perjanjian ini merupakan kerangka kerjasama yang kuat di antara negara-negara anggota ASEAN, yang bertujuan untuk mendorong perdamaian, stabilitas, dan kerjasama di kawasan Asia Tenggara. Penelitian ini menggunakan metode yuridis normatif dengan sifat penelitian deskriptif, yang menggunakan data hukum islam dan data sekunder. Data penelitian yang digunakan adalah pendekatan kualitatif dengan analisis deskriptif. Data diperoleh melalui studi kepustakaan dan analisis dokumen terkait perjanjian, kebijakan, dan inisiatif kerjasama terkait kejahatan siber di Indonesia dan ASEAN.

Hasil penelitian menunjukkan bahwa implementasi Perjanjian Persahabatan dan Kerjasama Indonesia dan ASEAN telah menghasilkan beberapa langkah positif dalam mengatasi kejahatan siber di kawasan ini. Kerjasama antarnegara anggota terkait pertukaran informasi, pelatihan, dan pengembangan kapasitas telah meningkatkan kemampuan untuk mendeteksi, mencegah, dan menangani serangan siber.

Kata Kunci: Implementasi, ASEAN, Perjanjian Persahabatan Dan Kerjasama, Kejahatan Siber (*cyber crime)*

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Pertama-tama disampaikan rasa syukur kehadirat Allah SWT yang maha pengasih lagi penyayang atas segala nikmat dan karunia-Nya sehingga skripsi ini dapat diselesaikan. Skripsi merupakan salah satu persyaratan bagi setiap mahasiswa yang ingin menyelesaikan studinya di Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Sehubungan dengan itu, disusun skripsi yang berjudulkan "IMPLEMENTASI PERJANJIAN PERSAHABATAN DAN KERJASAMA (TREATY OF AMITY AND COOPERATION) INDONESIA DAN ASEAN DALAM MENGATASI KEJAHATAN SIBER" .

Dengan selesainya skripsi ini, perkenankanlah diucapkan terima kasih yang sebesar-besarnya kepada: Rektor Universitas Muhammadiyah Sumatera Utara Bapak Prof. Dr. Agussani, M.AP atas kesempatan dan fasilitas yang diberikan kepada kami untuk menyelesaikan program sarjana ini. Dekan Fakultas Hukum Universitas Muhammadiyah Sumatera Utara Bapak Dr. Faisal, S.H., M.Hum atas kesempatan menjadi mahasiswa Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Demikian juga halnya kepada Wakil Dekan I Bapak Dr. Zainuddin, S.H.,M.H dan Wakil Dekan III Ibu Atikah Rahmi, S.H., M.H.

Terima kasih yang tak terhingga dan penghargaan yang setinggi-tingginya diucapkan kepada Bapak Muhammad Nasir Sitompul, S.H., M.H., selaku

Pembimbing, Ibu Miraa Astuti, S.H., selaku Dosen Penguji I, dan bapak Dr. M. Syukran Yamin Lubis, S.H., CN., M.Kn Selaku Dosen Penguji II, yang dengan penuh perhatian telah memberikan dorongan, bimbingan dan arahan sehingga skripsi ini selesai.

Disampaikan juga penghargaan kepada seluruh staf pengajar Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Tak terlupakan disampaikan terima kasih kepada seluruh narasumber yang telah memberikan data selama penelitian berlangsung.

Secara khusus dengan rasa hormat dan penghargaan yang setinggi- tingginya diberikan terima kasih kepada kedua orang tua saya, yaitu Ayahanda Burhanuddin dan Ibunda Yetti Anisah yang telah mengasuh, mendoakan, memberi dukungan dan mendidik saya dengan curahan kasih sayang, juga kepada Adik sepupu saya Muhammad Faris Almunawar, Faza Almunawar, Said Rafa yang telah memberikan saran, dukungan, dan semangat sehingga saya dapat menyelesaikan skripsi ini.

Dan terima kasih kepada Abang angkat dan Kakak angkat saya Muhammad Rony Willy Saputra dan Dewi Harmida. S.PD., serta teman-teman seperjuangan kelas I-1 Internasional yang tidak dapat disebutkan seluruh namanya. Terutama juga terima kasih kepada Nurul Afiah, Muhammad Tamim Noor Harahap, Reki Kawaharai, Alfajri Hasan, Daffa Ikram, Fasya Ramanda Putra, Fadhil Wijaya, Muhammad

Galih, Aidil Syahputra dan sahabat-sahabat saya lainnya yang tidak bisa saya sebutkan satu persatu.

Akhirnya, tiada gading yang tak retak, retaknya gading karena alami, tiada orang yang tak bersalah, kecuali Ilahi Robbi. Mohon maafatas segala kesalahan selama ini, begitupun Saya menyadari bahwa skripsi ini masih memiliki banyak kekurangan dan jauh dari sempurna. Untuk itu diharapkan ada masukan yang membangun semoga kiranya mendapatkan balasan dari Allah SWT. Semoga skripsi ini dapat bermanfaat khususnya bagi penulis dan bagi pembacaumumnya.

Assalamu'alaikum Warahmatullahi Wabarakatuh
Medan,20 maret 2024

Hormat Saya
Penulis,

Muhammad Rafi Maulana
NPM 1806200438

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang

Dunia internasional kini telah mencapai era baru dimana isu nontradisional semakin mendapatkan perhatian dari aktor-aktor hubungan internasional. Semakin berkembangnya isu-isu global tersebut merupakan konsekuensi dari adanya globalisasi dimana tidak adanya batasan pasti dalam penyebaran informasi di dunia. Keadaan tersebut membawa pada perubahan pola interaksi dari aktor-aktor hubungan internasional yang tidak hanya terjadi antara negara dengan negara, namun juga negara dengan aktor nonnegara. Perubahan yang ada diikuti oleh penemuan dan pengembangan teknologi yang semakin maju, salah satunya berupa penemuan internet sebagai media penyebaran informasi dan komunikasi.

Sejak pertama kali muncul, sedikit banyak internet telah membawa perubahan pada berbagai aspek kehidupan manusia. Perubahan tersebut tak hanya memiliki dampak positif seperti dipermudahnya interaksi dan penyebaran informasi antar aktor hubungan internasional yang semula terhambat jarak dan wilayah, tetapi juga memiliki dampak negatif bagi penyebaran informasi itu sendiri di dalam internet. Lebih lanjut, dampak negatif dari internet adalah munculnya kejahatan siber (cyber crime). Kejahatan siber melibatkan jaringan internet yang terhubung dengan hampir seluruh komputer di seluruh dunia. Selain itu, kejahatan ini dapat menyebabkan ketidakamanan data dan dokumen yang dikoneksikan melalui server internet. Sehingga, dalam konteks lebih luas kejahatan ini dapat mengganggu keamanan suatu negara.

Kejahatan siber dapat mengganggu dan menjadi ancaman bagi keamanan nasional suatu negara dikarenakan saat ini banyak negara yang sudah mengkoneksikan data-data dan kontrolnya terhadap beberapa sektor melalui internet atau daring (online). Karena luasnya jenis kejahatan siber yang dapat terjadi di internet, hingga kini belum ada klasifikasi dan pengertian pasti dari kejahatan siber itu. Namun, kejahatan siber saat ini telah mendapatkan perhatian internasional sebagai salah satu kejahatan transnasional. Dapat dilihat dari diidentifikasikannya kejahatan siber sebagai salah satu dari New Emerging Crimes pada Konferensi Anggota PBB tentang Kejahatan Transnasional Terorganisir (Conference of States Parties UNTOC) pada tahun 2010. Senada dengan penetapan oleh PBB tersebut, Julian Droogan menyatakan bahwa kejahatan siber telah berkembang menjadi salah satu ancaman utama dari kesejahteraan masyarakat di seluruh dunia[1]. Dengan demikian, hal ini membuktikan bahwa keamanan yang ditujukan untuk mencegah dan menangani kejahatan siber perlu dikembangkan dan menjadi fokus baru keamanan nasional negara.

Indonesia adalah negara yang penggunaan internetnya termasuk sangat tinggi. Hal tersebut terbukti dari hasil studi yang bekerjasama dengan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2019 yang menunjukkan bahwa dari total 264 juta penduduk Indonesia, terdapat 171,17 juta jiwa atau 64,8 persen masyarakat yang telah terhubung ke internet.[2] Dengan

[1] Droogan, J. (2010). Asian Transnational Security Challenges: Emerging Trends, Regional

[2] Yudha Pratomo. (16 Mei 2019). APJII: Jumlah Pengguna Internet di Indonesia Tembus 171 Juta Jiwa. diakses pada 20 Mei 2020 melalui https://tekno.kompas.com/read/2019/05/16/03260037/apjii-jumlah-pengguna-internet-diindonesia-tembus-171-juta-jiwa

penggunaan internet yang begitu tinggi dari masyarakat, ancaman terjadinya kejahatan siber tentu juga akan sangat tinggi. Oleh karena itu, diperlukan upaya peningkatan keamanan siber oleh Pemerintah Indonesia sebagai bagian dari penjagaan keamanan nasional.

Indonesia merupakan anggota yang aktif dalam berbagai forum PBB, termasuk dalam Konferensi Anggota PBB tentang Kejahatan Transnasional Terorganisir yang telah menetapkan lima kejahatan baru yang harus mendapat perhatian, termasuk kejahatan siber yang dapat terjadi lintas batas negara. Dari sisi Indonesia sendiri, tergolong rentan terhadap kejahatankejahatan tersebut dikarenakan letaknya yang strategis dan masyarakatnya yang banyak dan beragam. Sehingga, Pemerintah Indonesia melakukan upaya pencegahan dengan menaruh perhatian khusus terhadap kejahatan lintas negara baru dan berkembang yang telah ditetapkan, serta mengintensifkan kerjasama internasional untuk melindungi kepentingan dan kedaulatan nasional Indonesia.3 Dalam hal ini, Indonesia mengupayakan peningkatan keamanan siber dengan cara bekerjasama dengan negara lain, baik melalui kerjasama bilateral maupun multilateral.

Jika dilihat dari aspek kejahatan di ranah media sosial, Indonesia masuk peringkat 13 di wilayah Asia Pasifik dan Jepang, dan sebanyak 72,87 persen dari penipuan dalam ranah media sosial tersebut, ternyata disebarkan sendiri oleh pengguna tanpa sadar.[3] Sementara, laporan dari Kantor Berita Radio Nasional (KBRN), menyebutkan bahwa pada kuartal kedua 2013, Indonesia adalah negara terbesar pertama sebagai asal serangan siber dunia dan negara

[3] "Indonesia Butuh Badan Cyber Nasional", diakses 12 Maret 2018, http://www.majalahict.com/indonesiabutuh-badan-cyber-nasional/

dengan risiko siber tertinggi (38%), diikuti oleh China di urutan kedua (33%) dan Amerika Serikat di posisi ketiga (6,9%).[4]

Dalam kasus ancaman siber, berdasarkan analisis data sistem monitoring traffic ID-SIRTII (*Indonesia Security Incident Response Team On Internet Infrastructure*) tercatat bahwa insiden serangan di dalam dunia maya di Indonesia mencapai satu juta insiden dan akan cenderung mengalami peningkatan setiap harinya akibat kelemahan sistem dan aplikasi yang tidak diketahui. Dalam hal ini, institusi pemerintah juga tidak luput dari serangan siber di mana dalam kurun waktu 1998 - 2009 sebanyak 2.138 serangan telah dialamatkan terhadap website domain milik pemerintah. Serangan *Distributed Denial of Service* pada sistem *Domain Name Service (DNS) CCTLDID* yaitu domain .id terutama .co.id. Kasus lain juga menyangkut penyebaran malware dan malicious code yang disisipkan di dalam file dan web site serta phising site, spionase industri dan penyanderaan sumber daya informasi kritis, maupun black campaign partai politik atau penistaan keyakinan dan penyebaran kabar bohong (hoax) untuk tujuan provokasi politis serta rekayasa ekonomi. Akibat keterbatasan sumber daya dan akses terkait pemeriksaan oleh penegak hukum Indonesia kepada penyelenggara layanan asing di luar negeri, beberapa kasus tersebut belum dapat diatasi walaupun Undang-Undang ITE telah mengaturnya.[5]

---

[4] CATRA, "Dari Desk Cyberspace Nasional Menuju Badan Cyber Nasional", Majalah Setjen Wantannas, Edisi VI (September 2016):16.

[5] Ahmad Budi Setiawan, "Peran Government Chief Information Officer (GCIO) dalam Tata Kelola Keamanan Informasi Nasional", Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika Indonesia, Volume 2 No. 4 (2011): 395-442.

Sementara dalam konteks global, intensitas serangan siber yang semakin tinggi, bisa dilihat dari serangkaian serangan siber seperti yang dilaporkan dari *The Telegraph UK*, di mana pada bulan Mei 2017 telah terjadi serangan *cyber WanaCrypt0r 2.0* atau yang biasa disebut sebagai virus *WannaCry* menyebar dengan cepat dalam skala masif sepanjang sejarah di tingkat global. Virus tersebut pada awalnya menyebar di Ukraina yang kemudian merembet ke 10 negara lainnya hanya dalam waktu kurang dari dua jam, termasuk Indonesia.[6] Bahkan virus ini kemudian meluas ke 99 negara di dunia.[7] Jika melihat trend global, negara-negara seperti Brazil, Rusia, India, China sudah meningkatkan keamanan *cyber security* mereka. Bahkan perang siber sudah banyak terjadi, sehingga sebagai sebuah negara, termasuk dalam hal ini Indonesia, juga perlu memelihara kedaulatan di ranah siber mengingat bahwa kekerahasiaan, komunikasi antara pejabat publik sekarang pun memasuki dunia digital.[8]

Di Indonesia penerapan pertahanan siber sudah dilaksanakan pada masing-masing institusi atau lembaga nasional maupun swasta untuk melindungi sistem jaringan yang menopang infrastruktur kritis mereka. Namun, perlindungan secara nasional dalam kerangka kebijakan siber nasional belum diamanatkan dalam sebuah regulasi dalam bentuk perundang-undangan. Padahal beberapa negara telah menerapkan undang-undang terkait cyber

---

[6] Sabrina Burhanuddin,"Membangun Strategi Pertahanan Cyber di ASEAN", Majalah Masyarakat ASEAN, Edisi 16 (September 2017):34.

[7] Susetyo Dwi Prihadi, "Dihantam Ransomware, Indonesia Butuh Badan Siber Nasional". CNN Indonesia, diakses 12 Maret 2018, https://www.cnnindonesia. com/teknologi/20170515073309-185-214802/ dihantam-ransomware-indonesia-butuh-badan-sibernasional.

[8] Iris Gera, "LIPI: Dibutuhkan Badan Cyber Nasional Indonesia", VoA Indonesia, diakses 12 Maret 2018, https://www.voaindonesia.com/a/lipi-dibutuhkanbadan-cyber-nasional-di-indonesia-/2591870.html

security mengingat ketergantungan mereka akan teknologi informatika. Meskipun Indonesia telah mengeluarkan regulasi dan kebijakan tentang keamanan informasi melalui Undang-Undang ITE, untuk membangun pertahanan negara melalui *cyber security* tidak cukup dilaksanakan jika hanya berlandaskan pada undang-undang tersebut. Salah satu penyebabnya adalah pembagian fungsional pada masalah kewenangan dan otoritas yang berkewajiban dalam menanggulangi ancaman *cyber* seperti *cybercrime*, *cyberterrorism*, *cyber hacktivism* maupun *cyber warfare* yang masih belum jelas.

Islam dijadikan sebagai standar bagi pemanfaatan IPTEK dalam kehidupan sehari-hari. Sesuai firman Allah SWT dalam Alquran surah Yunus ayat 101:

قُلِ انْظُرُوْا مَاذَا فِى السَّمٰوٰتِ وَالْاَرْضِ ۗوَمَا تُغْنِى الْاٰيٰتُ وَالنُّذُرُ عَنْ قَوْمٍ لَّا يُؤْمِنُوْنَ

Artinya: "Katakanlah: "Perhatikanlah apa yang ada di langit dan di bumi. Tidaklah bermanfaat tanda kekuasaan Allah dan Rasul-rasul yang memberi peringatan bagi orang-orang yang tidak beriman".[9]

Berdasarkan ayat Al-Qur'an di atas menjelaskan bahwa Allah memerinthkan manusia untuk memperhatikan fenomena yang terjadi di langit dan di bumi. Manusia hendaklah merenungkan rahmat Allah tersebut dengan mengadakan penelitian alam, agar menemukan ilmu pengatahuan teknologi. Sehingga dapat memanfaatkan alam untuk kesejahteraan manusia dan mempertebal iman kepada Allah.

[9] Kementrian Agama, *Alquran dan Terjemah Mushaf Aisyah*(Bandung: Penerbit Jabal, 2010), hlm.220.

Indonesia sebagai negara yang telah dikarunia Allah dengan teknologi yang sangat maju, tentunya harus dapat memanfaatkan teknologi tersebut sebaik-baiknya untuk dapat memakmurkan dan mensejahterakan kehidupan bangsa dan negara juga berkewajiban untuk membuat peraturan perundang- undangan nasional berkenaan perlindungan dan pencegahan keamanan siber dalam rangka menjaga keamanan data dari ancaman kejahatan siber, sesuai yang diatur dalam Pasal 30 ayat (1) UU ITE. Dalam hal ini ialah pelaksanaan implementasi perjanjian dan kerjasama indonesia dan asean untuk mengatasi serangan siber. Berdasarkan hal tersebut penulis tertarik untuk melakukan penelitian dan mengkaji lebih dalam serta menuangkannya dalam bentuk skripsi hukum dengan judul:

"Implementasi Perjanjian Persahabatan Dan Kerjasama (*Treaty Of Amity And Cooperation*) Indonesia Dan Asean Dalam Mengatasi Kejahatan Siber"

1. Rumusan Masalah

Berdasarkan uraian latar belakang pertanyaan yang diajukan, penulis merumuskan pernyataan masalah yang dihadapi dalam penelitian ini yaitu :

a. Bagaimana Indonesia Dan ASEAN Dalam Mengatasi Cyber Crime?
b. Bagaimana Implementasi Treaty Of Amity And Cooperation Terhadap Cyber Crime Di Indonesia?
c. Bagaimana Upaya Indonesia Dan ASEAN Dalam Mengatasi Hambatan Implementasi Treaty Of Amity And Cooperation Terhadap Cyber Crime?

2. Faedah Penelitian

Penelitian ini dilakukan dengan harapan mampu memberikan manfaat, baik manfaat teoritis dan manfaat praktis :

a. Manfaat teoritis yakni dalam hasil penelitian ini diharapkan dapat menambah wawasan dan ilmu pengetahuan kepada mahasiswa khususnya dan masyarakan luas pada umumnya dalam bidang hukum Internasional terkhusus bidang hukum informasi, transaksi dan elektronik, yakni pemahaman mengenai bagaimana Indonesia dan ASEAN menerapkan perjanjian persahabatan dan kerjasama dalam mengatasi serangan siber.

b. Manfaat praktis yakni dengan adanya penelitian ini diharapkan dapat menjadi sumber rujukan baru, sekaligus dapat memberikan pemahaman yang lebih mengenai Implementasi Perjanjian Persahabatan Dan Kerjasama (*Treaty Of Amity And Cooperation*) Indonesia Dan Asean Dalam Mengatasi Kejahatan Siber sebagai berikut :

1) Pertukaran Informasi dan Intelijen:

Dalam rangka melawan kejahatan siber, pertukaran informasi dan intelijen yang cepat dan efektif antara negara-negara ASEAN dan Indonesia sangat penting. Melalui Perjanjian Persahabatan dan Kerjasama, negara-negara anggota dapat memperkuat kerjasama dalam berbagi data tentang ancaman keamanan siber, pola serangan, dan taktik yang digunakan oleh pelaku kejahatan siber.

2) Koordinasi Tanggap Darurat:

Kejahatan siber seringkali membutuhkan respons cepat dan terkoordinasi untuk meminimalkan dampaknya. Dengan Perjanjian Persahabatan dan Kerjasama, Indonesia dan negara-negara ASEAN dapat membentuk mekanisme tanggap darurat yang dapat diaktifkan dalam situasi serius seperti serangan siber besar atau bocornya data sensitif. Koordinasi semacam ini dapat membantu menghadapi dan menangani ancaman kejahatan siber dengan lebih efisien.

3) Peningkatan Kapasitas dan Pelatihan:

Perjanjian tersebut juga dapat membuka pintu bagi negara-negara ASEAN untuk berbagi pengetahuan, pengalaman, dan keahlian dalam mengatasi kejahatan siber. Melalui kerjasama ini, Indonesia dan negara-negara ASEAN dapat meningkatkan kapasitas mereka dalam melawan ancaman siber dengan memperkuat infrastruktur keamanan siber, melatih personel keamanan siber, dan membangun sumber daya manusia yang berkualitas.

4) Pengembangan Kebijakan Bersama:

Dalam rangka memerangi kejahatan siber, harmonisasi kebijakan dan peraturan antara negara-negara anggota ASEAN dapat menjadi strategi yang efektif. Perjanjian Persahabatan dan Kerjasama dapat menjadi platform untuk mengembangkan kerangka kerja bersama dan pedoman yang mencakup aspek hukum, peraturan, dan etika dalam penggunaan teknologi informasi dan komunikasi.

5) Perlindungan Data dan Privasi:

Kejahatan siber seringkali terkait dengan pelanggaran data dan privasi. Melalui perjanjian ini, negara-negara ASEAN dapat bekerja sama untuk melindungi data pribadi warga negara dan menjaga privasi online, termasuk kerja sama dalam bidang legislasi dan penegakan hukum terkait perlindungan data.

6) Membentuk Front Bersama:

Dengan kejahatan siber yang sering kali tidak mengenal batas negara, solidaritas dan kerjasama regional sangat penting. Dengan adanya Perjanjian Persahabatan dan Kerjasama, Indonesia dan negara-negara ASEAN dapat membentuk front bersama untuk melawan kejahatan siber yang kompleks dan berkembang pesat.

B. Tujuan Penelitian

Adapun tujuan dari penelitian ini ialah:

1. Menganalisis kebijakan dan kerangka hukum:

   Tujuan penelitian dapat melibatkan analisis kebijakan dan kerangka hukum yang telah ditetapkan oleh Indonesia dan ASEAN dalam mengatasi kejahatan siber. Ini melibatkan penelusuran peraturan yang ada, undang-undang yang berlaku, dan kerangka kerja yang digunakan untuk menghadapi ancaman kejahatan siber.

2. Mempelajari upaya pencegahan:

   Penelitian dapat difokuskan pada langkah-langkah yang telah diambil oleh Indonesia dan ASEAN untuk mencegah kejahatan siber. Ini dapat melibatkan analisis strategi, kebijakan, dan program-program yang telah diterapkan untuk meningkatkan keamanan siber, pelatihan

untuk meningkatkan kesadaran tentang kejahatan siber, dan kerja sama regional dalam menghadapi ancaman kejahatan siber.

3. Mengevaluasi kapasitas penegakan hukum:

   Penelitian juga dapat bertujuan untuk mengevaluasi kapasitas penegakan hukum Indonesia dan ASEAN dalam mengatasi kejahatan siber. Ini melibatkan penilaian terhadap kemampuan aparat penegak hukum untuk mendeteksi, menyelidiki, dan menindak pelaku kejahatan siber, serta kerja sama lintas batas dalam hal pengumpulan bukti dan penegakan hukum.

4. Menganalisis kerjasama regional:

   Penelitian juga dapat memeriksa kerjasama regional antara Indonesia dan negara-negara anggota ASEAN dalam menghadapi kejahatan siber. Hal ini melibatkan evaluasi terhadap keefektifan kerja sama, saling bertukar informasi, dan koordinasi antara negara-negara tersebut dalam menanggapi kejahatan siber.

5. Mengevaluasi dampak dan tantangan:

   Tujuan penelitian juga dapat mencakup evaluasi dampak yang telah dicapai dan tantangan yang dihadapi dalam upaya mengatasi kejahatan siber. Ini melibatkan penilaian terhadap efektivitas langkah-langkah yang telah diambil, kesenjangan yang masih ada, serta faktor-faktor sosial, teknis, dan kebijakan yang mempengaruhi upaya tersebut.

C. Definisi Operasional

Definisi operasional atau kerangka konsep adalah sebuah kerangka yang berisi variabel yang akan menggambarkan hubungan antara definisi-definisi/ konsep-konsep yang akan diteliti. Berhubungan dengan judul yakni, "**Implementasi Perjanjian Persahabatan Dan Kerjasama (*Treaty Of Amity And Cooperation*) Indonesia Dan Asean Dalam Mengatasi Kejahatan Siber**", maka definisi operasionalnya adalah:

1. Implementasi

Suatu kegiatan atau suatu tindakan dari sebuah rencana yang dibuat secara terperinci untuk mencapai suatu tujuan. Implementasi mulai dilakukan apabiila seluruh perencanaan sudah dianggap sempurna. Jadi Implementasi adalah tindakan yang dilakukan setelah suatu kebijakan ditetapkan. Implementasi merupakan cara agar sebuah kebijakan dapat mencapai tujuannya.[10]

2. Perjanjian Persahabatan Dan Kerjasama (*Treaty Of Amity)*

Perjanjian internasional yang bertujuan untuk mempromosikan hubungan persahabatan, kerjasama, dan solidaritas antara negara-negara atau wilayah yang terlibat. Perjanjian semacam ini biasanya dirancang untuk menciptakan iklim yang kondusif bagi perdamaian, stabilitas, dan kemajuan bersama di antara para pihak yang terlibat.[11]

3. Indonesia Dan Asean Dalam Mengatasi Kejahatan Siber

Indonesia Dan Asean Dalam Mengatasi Kejahatan Siber dapat dilihat dalam *ASEAN Regional Forum* (ARF) melalui *ASEAN Political-Security*

[10] Mulyadi,Implementasi kebijakan(Jakarta:Balai Pustaka,2015),halaman 45
[11] Pasal 1 Undang-Undang Nomor 24 Tahun 2000

Community (APSC) dalam Sub Bab B.4.1. Bab tersebut berisi tentang kesepakatan peningkatan kerjasama dalam hal ancaman non tradisional, lebih khususnya lagi menyangkut persoalan kejahatan transnasional dan lintas batas. Sementara pembahasan mengenai kejahatan siber dijelaskan dalam Pasal XVII. Dalam hal ini, pada tahun 2006 ARF membentuk ARF *on cybersecurity initiatives* terkait pembahasan kejahatan siber di ASEAN yang kemudian dituangkan dalam *ASEAN's Cooperation on Cybersecurity and against Cybercrime*.[12]

D. Keaslian Penelitian

Implementasi Perjanjian Persahabatan Dan Kerjasama (Treaty Of Amity And Cooperation) Indonesia Dan Asean Dalam Mengatasi Kejahatan Siber merupakan hal yang layak dikaji. Oleh karenanya, penulis meyakini tidak banyak peneliti-peneliti sebelumnya yang mengangkat tentang hal ini. Namun berdasarkan bahan kepustakaan dari lingkungan Universitas Muhammadiyah Sumatera Utara dan perguruan tinggi lainnya, penulis tidak menemukan penelitian yang sama dengan pokok bahasan yang penulis teliti terkait "Implementasi Perjanjian Persahabatan Dan Kerjasama (Treaty Of Amity And Cooperation) Indonesia Dan Asean Dalam Mengatasi Kejahatan Siber". Namun dari beberapa judul penelitian yang pernah diangkat oleh peneliti sebelumnya, ada 1 (satu) judul yang hampir mendekata sama dengan penelitian dalam penulisan skripsi ini, antara lain :

[12] David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari, "Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui Asean Regional Forum On Cybersecurity Initiatives", *Jurnal Penelitian Politik*, Volume 13 No. 1 (Juni 2016): halaman 4-5

1. Kristiani Virgi Kusuma Putri, Mahasiswi Ilmu Hukum Universitas Brawijaya, 2021, yang berjudul "Kerja Sama Indonesia Dengan Asean Mengenai *Cyber Security* Dan *Cyber Resilience* Dalam Mengatasi *Cyber Cime*". Penelitian ini merupakan penelitian normatif yang lebih menekankan kegiatan tindak kejahatan.

Berdasarkan konstruksi, substansi dan pembahasan terhadap penelitian tersebut diatas berbeda dengan penelitian yang dilakukan oleh penulis saat ini. Dalam kajian topik bahasan yang penulis angkat ke dalam bentuk skripsi ini mengarah kepada aspek kajian secara penelitian yuridis normatif.

E. Metode Penelitian

Metode penelitian adalah tata cara bagaimana melakukan penelitian. Metode penelitian adalah suatu cara untuk memecahkan masalah ataupun cara mengembangkan ilmu pengetahuan dengan menggunakan metode ilmiah.[13]Agar mendapatkan hasil yang maksimal maka metode yang digunakan dalam penelitian ini terdiri dari:

1. Jenis dan Pendekatan Penelitian

Berdasarkan pada konstruksi judul yang diangkat maka jenis penelitian ini adalah penelitian hukum, karena objek penelitian ini mengkaji hukum yang dikonsepkan sebagai norma atau kaidah hukum. Pendekatan penelitian yang digunakan dalam penelitian ini ialah menggunakan pendekatan penelitian yuridis normatif. Penelitian yuridis

[13] Jonaedi Efendi dan Johny Ibrahim. 2018. *Metode Penelitian Hukum Normatif dan Empiris.* Depok: Prenada Media Group,2018. Halaman 2-3

normatif dilakukan dengan studi kepustakaan bukandengan ide yang kosong (*Blank idea),* tetapi serangkaian gambaran kasar mengenai sesuatu yang akan diteliti dengan sejumlah besar bahan hukum yang harus dipilah-pilah, serta buku teks hukum dan jurnal ilmiah di bidang hukum. Penelitian hukum normatif jugabisadisebut sebagai penelitian hukum doktrinal.[14]

2. Sifat Penelitian

Sifat penelitian yang digunakan dalam penelitian ini ialah penelitian deskriptif, dimana penelitian ini bersifat memaparkan dan menggambarkan lengkap tentang keadaan hukum yang terjadi dengan menggunakan pendekatan penelitian hukum secara yuridis normatif. Penelitian ini jugaberbasis kepustakaan yang fokus menganalisis data sekunder yang terdiri dari bahan hukum primer (Undang-Undang dan Peraturan yang Terkait) ,bahan hukum sekunder (buku dan Jurnal terkait) dan bahan hukum tersier (Internet).

3. Sumber Data

Sumber data yang digunakan dalam sebuah penelitian dibagi menjadi 2 (dua) macam yaitu data primer dan sekunder. Dalam penelitian hukum yuridis normatif maka sumber datanya adalah data yang bersumber dari hukum islam dan data sekunder yaitu sebagai berikut:

a. Data yang bersumber dari hukum Islam yaitu Al-Qur'an dan Hadist (Sunnah Rasul). Data yang bersumber dari Hukum Islam tersebut

[14] i*bid,* Halaman 124

lazim disebut pula sebagai data kewahyuan. Data kewahyuan yang menjadi landasan skripsi ini yaitu Q.S.Yunus (10): 101.

b. Data sekunder yaitu data pustaka yang mencakup dokumen-dokumenpublikasi tentang hukum meliputi: buku-buku teks dan jurnal-jurnal hukum.

Data sekunder terdiri dari:

1. Bahan hukum primer yaitu bahan-bahan hukum yang mengikat yakni seperti: Cyber crime diatur dalam Undang-Undang Transaksi Elektronik Nomor 8 Tahun 2011 sebagaimana telah diubah menjadi Undang- Undang Nomor 19 Tahun 2016, ("UU ITE") khususnya pada pasal 27 sampai 30 mengenai perbuatan yang dilarang,

2) Bahan Hukum Sekunder, yaitu bahan-bahan hukum yang memberikan penjelasan mengenai bahan hukum primer, seperti: buku-buku literatur atau bahan-bahan bacaan, hasil karya dari kalangan umum, karya-karya tulisan ilmiah lainnya yang berkaitan dengan permasalahan penelitian.

3) Bahan hukum tersier, yaitu bahan-bahan yang memberi petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, seperti: Ensiklopedia, Kamus Besar Bahasa Indonesia, Kamus Bahasa Inggris, Surat kabar dan sebagainya.

4. Alat Pengumpul Data

Penelitian ini menggunakan alat pengumpul data berupa studi dokumentasi dengan hanya menganalisa bahan hukum tertulis seperti: buku-buku literatur terkait jurnal jurnal yang terkait dan sumber data lainnya. Adapun untuk studi kepustakaanyang dilakukan dengan 2 (dua) cara, yaitu;

a. Offline yaitu menghimpun data studi kepustakaan secara langsung dengan mengunjungi toko-toko buku, perpustakaan guna menghimpun data sekunder yang dibutuhkan dalampenelitian.
b. Online yaitu studi kepustakaan yang dilakukan dengan cara mencari dan mengumpulkan data sekunder yang dibutuhkan dalam penelitian melalui media internet

5. Analisis Data

Analisis data dalam penelitian ini menggunakan analisis kualitatif, yakni data yang diperoleh didapatkan berdasarkan kegiatan analisis atau studi kepustakaan atas bahan hukum yang nantinya akan diuraikan dan dihubungkan sedemikian rupa sehingga disajikan dalam bentuk penulisan yang lebih sistematis untuk mencapai tujuan yang diinginkan yakni Implementasi Perjanjian Persahabatan Dan Kerjasama (Treaty Of Amity And Cooperation) Indonesia Dan Asean Dalam Mengatasi Kejahatan Siber. Pengolahan data dilakukan dengan menggunakan pengolahan data logika deduktif, yakni dengan menarik kesimpulan dari data-data umum menjadi sesuatu yang lebih khusus agar penelitian menjadi lebih terstruktur dan tepat sasaran.

BAB II

TINJAUAN PUSTAKA

A. Implementasi

Implementasi adalah tahap penting dalam siklus perencanaan yang melibatkan penerapan atau pelaksanaan rencana, strategi, atau program dalam situasi nyata. Ini adalah langkah kritis yang menghubungkan konsep teoritis atau ide dengan tindakan konkret di dunia nyata. Proses implementasi mewakili perubahan dari konsep menjadi aksi, dan ini dapat terjadi dalam berbagai konteks, termasuk dalam bisnis, pemerintahan, pendidikan, teknologi, dan banyak bidang lainnya.

1) Pentingnya Implementasi:

Implementasi adalah langkah yang kritis karena meskipun sebuah rencana atau strategi dapat terlihat baik di atas kertas, kenyataannya sering kali berbeda. Proses implementasi menghadirkan tantangan dan kompleksitas sendiri karena melibatkan banyak pihak yang harus berkoordinasi, sumber daya yang harus diatur, dan perubahan yang harus dihadapi. Kegagalan dalam mengimplementasikan rencana dengan baik bisa berarti hasil yang kurang optimal, sumber daya yang terbuang sia-sia, dan bahkan kesempatan yang terlewatkan.

2) Langkah-Langkah dalam Implementasi:

1. Perencanaan Implementasi:

Langkah pertama adalah merumuskan rencana implementasi yang jelas dan terperinci. Ini mencakup menetapkan tujuan yang jelas, mengidentifikasi tindakan yang diperlukan, menentukan waktu dan

sumber daya yang diperlukan, dan merancang langkah-langkah untuk mencapai tujuan tersebut.

2. Pengorganisasian:

   Setelah rencana diatur, langkah selanjutnya adalah mengorganisir tim atau kelompok yang akan bertanggung jawab untuk melaksanakan rencana tersebut. Setiap anggota tim harus memiliki peran dan tanggung jawab yang jelas untuk memastikan bahwa semua bagian dari rencana dapat dijalankan dengan efisien.

3. Pengalokasian Sumber Daya:

   Implementasi sering memerlukan sumber daya seperti uang, tenaga kerja, teknologi, dan infrastruktur. Pengalokasian sumber daya ini harus diatur dengan bijaksana untuk memastikan bahwa mereka tersedia sesuai kebutuhan dan dapat digunakan secara efektif selama implementasi.

4. Komunikasi dan Koordinasi:

   Komunikasi yang efektif adalah kunci dalam proses implementasi. Semua pihak yang terlibat harus diberi tahu tentang rencana, tujuan, dan peran mereka dalam proses ini. Koordinasi yang baik juga diperlukan untuk memastikan bahwa tindakan yang diambil sesuai dengan rencana secara keseluruhan.

5. Monitoring dan Evaluasi:

   Selama implementasi, penting untuk terus memantau perkembangan dan hasilnya. Ini membantu untuk mengidentifikasi masalah yang muncul dan memungkinkan perbaikan segera jika dibutuhkan. Evaluasi juga

membantu dalam menilai efektivitas rencana dan membuat perubahan jika diperlukan.

6. Penyesuaian dan Perbaikan:

   Implementasi seringkali melibatkan tantangan dan hambatan yang tidak terduga. Oleh karena itu, fleksibilitas dan kemampuan untuk menyesuaikan diri adalah kunci untuk mengatasi masalah dan memperbaiki proses implementasi.

Kesimpulannya, implementasi adalah tahap penting dalam menerjemahkan rencana dan ide menjadi tindakan nyata. Proses ini melibatkan perencanaan yang cermat, pengaturan sumber daya, komunikasi yang efektif, dan kemampuan untuk beradaptasi dengan perubahan yang mungkin terjadi. Keberhasilan implementasi dapat menjadi kunci kesuksesan dalam mencapai tujuan yang telah ditetapkan.

B. ASEAN

ASEAN (Asosiasi Negara-Negara Asia Tenggara) adalah sebuah organisasi politik dan ekonomi regional yang terdiri dari sepuluh negara anggota di Asia Tenggara. Tujuan utama ASEAN adalah meningkatkan kerjasama dan integrasi antara negara-negara anggotanya untuk mencapai kemajuan ekonomi, sosial, budaya, dan politik di kawasan Asia Tenggara. Didirikan pada 8 Agustus 1967 dengan penandatanganan Deklarasi Bangkok oleh lima negara pendiri, yaitu Indonesia, Malaysia, Filipina, Singapura, dan Thailand, organisasi ini telah berkembang pesat dalam beberapa dekade terakhir dengan bergabungnya enam negara anggota lainnya.

Pengertian ASEAN secara lebih mendalam dapat diuraikan sebagai berikut:

1. Tujuan dan Misi: Tujuan utama ASEAN adalah menciptakan kawasan yang stabil, damai, dan sejahtera melalui kerjasama yang erat di antara negara-negara anggotanya. Misi ini dicapai dengan memperkuat hubungan politik, memajukan perdagangan dan ekonomi, meningkatkan kerjasama sosial-budaya, dan memajukan kawasan Asia Tenggara dalam kancah global.[15]
2. Prinsip-Prinsip ASEAN: ASEAN didasarkan pada prinsip-prinsip seperti saling menghormati kedaulatan dan integritas wilayah, non-intervensi dalam urusan dalam negeri masing-masing negara, keterbukaan dan kesetaraan, serta penyelesaian perbedaan dengan cara damai melalui dialog dan konsultasi.[16]
3. Struktur Organisasi: ASEAN memiliki struktur organisasi yang terdiri dari KTT (Konferensi Tingkat Tinggi), KOM (Komite Menteri), SOM (Komite Pejabat Senior), dan berbagai badan-badan lain yang bertanggung jawab atas bidang-bidang tertentu seperti ekonomi, politik, keamanan, sosial-budaya, dan lingkungan.[17]
4. Kerjasama Ekonomi: ASEAN memiliki persetujuan kerjasama ekonomi yang dikenal sebagai AFTA (ASEAN Free Trade Area), yang bertujuan untuk menciptakan pasar tunggal dan basis produksi yang terintegrasi di kawasan. Selain itu, ASEAN juga terlibat dalam berbagai perjanjian

[15] 1 Deklarasi Bangkok adalah perjanjian yang ditandatangani oleh lima negara pendiri ASEAN pada 8 Agustus 1967 di Bangkok, Thailand. Negara-negara pendiri tersebut adalah Indonesia, Malaysia, Filipina, Singapura, dan Thailand. (Sumber: ASEAN Secretariat, www.asean.org)
[16] ASEAN Secretariat, www.asean.org
[17] *Ibid.*

perdagangan dengan mitra-mitra di luar kawasan, seperti China, Jepang, Korea Selatan, dan Australia.

5. Keamanan dan Politik: ASEAN berkomitmen untuk memajukan perdamaian dan stabilitas di kawasan melalui dialog dan diplomasi. Organisasi ini juga telah menandatangani Piagam ASEAN tentang Keamanan Bersama (TAC - Treaty of Amity and Cooperation) yang menegaskan prinsip ketidakagresi di antara negara-negara anggota.
6. Kerjasama Sosial-Budaya: ASEAN juga berupaya meningkatkan kerjasama di bidang sosial-budaya melalui program-program pertukaran budaya, pendidikan, dan peningkatan kesadaran antarbangsa di kalangan warganya.
7. Hubungan Eksternal: ASEAN memiliki hubungan kerjasama dengan berbagai negara dan organisasi di luar kawasan, termasuk dengan pihak seperti Perserikatan Bangsa-Bangsa (PBB), Uni Eropa (UE), dan negara-negara di kawasan Pasifik.

C. Perjanjian Persahabatan Dan Kerjasama

Perjanjian persahabatan adalah suatu kesepakatan resmi antara dua negara atau lebih untuk memperkuat hubungan dan kerjasama di berbagai bidang, serta untuk menciptakan lingkungan yang harmonis dan damai di antara para pihak yang terlibat. Tujuan utama dari perjanjian persahabatan adalah mempromosikan saling pengertian, saling menghormati kedaulatan, dan mendorong kerjasama dalam berbagai aspek kehidupan internasional.[18]

[18] *Kementerian Luar Negeri Republik Indonesia, www.kemlu.go.id*

Pengertian perjanjian persahabatan mencakup beberapa poin penting:

1. Memperkuat Hubungan Bilateral: Perjanjian persahabatan bertujuan untuk meningkatkan hubungan bilateral antara negara-negara yang terlibat. Dalam konteks ini, negara-negara tersebut berkomitmen untuk saling mendukung dan menghormati hak kedaulatan masing-masing. Hal ini mencakup pengakuan atas batas wilayah, non-intervensi dalam urusan dalam negeri, dan menghormati prinsip saling menghormati dan saling menguntungkan.
2. Menciptakan Lingkungan Damai: Perjanjian persahabatan juga berfungsi sebagai sarana untuk menciptakan lingkungan yang damai di kawasan atau di dunia internasional secara keseluruhan. Dalam perjanjian ini, negara-negara berkomitmen untuk menyelesaikan perbedaan atau sengketa yang mungkin muncul melalui jalur damai dan dialog, bukan dengan kekerasan atau konflik militer.
3. Mendorong Kerjasama dalam Berbagai Bidang: Perjanjian persahabatan mencakup aspek kerjasama di berbagai bidang, seperti ekonomi, perdagangan, investasi, teknologi, pendidikan, budaya, dan lainnya. Hal ini bertujuan untuk membangun kemitraan yang saling menguntungkan dan meningkatkan kesejahteraan masyarakat di kedua negara.[19]

4. Memberikan Landasan Hukum: Perjanjian persahabatan memberikan landasan hukum yang kuat untuk mengatur dan mengawasi pelaksanaan

[19] *The Diplomat, www.thediplomat.com*

kerjasama antara negara-negara yang terlibat. Ini mencakup pembentukan badan atau komite bersama yang bertanggung jawab atas pelaksanaan perjanjian dan penyelesaian sengketa.

5. Memperkuat Diplomasi dan Hubungan Internasional: Perjanjian persahabatan juga menjadi instrumen penting dalam diplomasi dan hubungan internasional. Ini menandakan komitmen yang kuat dari masing-masing negara terhadap hubungan baik, stabilitas, dan perdamaian di kawasan maupun di tingkat global.

D. Kejahatan Siber

Pengertian kejahatan ciber menurut hukum di Indonesia sebetulnya belum ada yang definitif diatur dalam peraturan perundang-undangan. Dalam Undang-Undang tentang informasi dan Transaksi Elektronik yaitu Undang-Undang Nomor 11 Tahun 2008 yang diubah dengan UU Nomor 19 tahun 2016 yang pada dasarnya merupakan pengaturan perundang-undangan administratif tetapi dalam undang-undang ini juga dimasukkan beberapa pasal atau ketentuan tentang perbuatan pidana yang kemudian dikenal dengan istilah kejahatan siber.

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Indonesia Dan ASEAN Dalam Mengatasi Cyber Crime

Indonesia dan ASEAN (Asosiasi Negara-Negara Asia Tenggara) memiliki peran penting dalam mengatasi kejahatan siber atau cyber crime yang semakin meningkat dalam era digital ini. Kejahatan siber merupakan tantangan yang kompleks karena tidak mengenal batas negara dan dapat berdampak luas terhadap masyarakat, bisnis, dan infrastruktur. Oleh karena itu, upaya kolaboratif dan koordinasi antara negara-negara anggota ASEAN, termasuk Indonesia, sangat penting dalam menghadapi ancaman cyber crime.

Sebelum mengurai pengertian dari *cyber crime* secara terperinci maka terlebih dahulu akan dijelaskan "induk" *cybercrimes* yaitu *cyber space. Cyber space* dipandang sebagai sebuah dunia komunikasi yang berbasis komputer. Dalam hal ini, cyber space dianggap sebagai sebuah realitas baru dalam kehidupan manusia yang dalam bahasa sehari-hari dikenal dengan internet

Realitas baru ini dalam kenyataannya terbentuk melalui jaringan komputer yang menghubungkan antar negara atau antar benua yang berbasis protokol *transmission control protocol/internet protokol* . Hal ini berarti, dalam sistem kerjanya dapatlah dikatakan bahwa *cyber space* (internet) telah mengubah jarak dan waktu menjadi tidak terbatas. Internet digambarkan sebagai kumpulan jaringan komputer yang terdiri dari sejumlah jaringan yang lebih kecil yang mempunyai sistem jaringan yang berbeda-beda[20]

[20] Kenny Wiston, 2002, the internet: Issues of Jurisdictio and Controversies Surounding Domain Names, Bandung : Citra Aditya, halaman 7

1. Pengenalan tentang Cyber *Crime* dan Ancaman di Era Digital

Pengenalan tentang Cyber Crime dan Ancaman di Era Digital mencakup pemahaman tentang kejahatan siber atau cyber crime serta dampak dan ancaman yang timbul dalam era digital. Mengikuti perkembangan teknologi komputer, dan telekomunikasi yang cepat dapatlah diketahui bahwa komputer dan internet yang semula dimaksudkan sebagai alat untuk mempercepat dan memudahkan perhitungan, setelah dikombinasika dengan teknologi telekomunikasi secara *online* tidak saja lokal nasional, bahkan global melalui satelit dan bersamaan dengan berbagai perkembangan kegiatan lainnya, antara lain niaga dalam bentuk *e-commerce*, maka memerlukan penyesuaian kontrak dan syarat-syarat transaksi baru.

Dalam era digital yang terus berkembang pesat, teknologi komputer dan internet telah menjadi bagian integral dari kehidupan manusia. Namun, di balik kemudahan dan kenyamanan yang ditawarkan oleh era digital ini, muncul pula ancaman baru yang kompleks, yaitu kejahatan siber atau cyber crime. Kejahatan siber merujuk pada serangkaian aktivitas kriminal yang dilakukan oleh individu atau kelompok menggunakan teknologi informasi dan jaringan komputer untuk tujuan yang melanggar hukum. Tindakan kriminal ini mencakup berbagai bentuk seperti peretasan, serangan malware, pencurian data, penipuan daring, penyebaran konten ilegal, dan banyak lagi.

Cyber crime menjadi ancaman serius karena perkembangan teknologi digital memberikan celah bagi pelaku kejahatan untuk beroperasi secara anonim, melintasi batas negara, dan menyamarkan identitas mereka. Selain itu, tingginya ketergantungan masyarakat pada teknologi informasi dan internet membuat kita semakin rentan terhadap serangan cyber crime. Oleh karena itu, pemahaman tentang cyber crime menjadi penting agar kita dapat mengidentifikasi dan mengatasi ancaman ini dengan lebih efektif.[21]

a. Kejahatan Sibe (*Cyber Crime*)

Kejahatan siber adalah tindakan kriminal yang dilakukan melalui jaringan komputer atau internet. Ini mencakup berbagai aktivitas ilegal yang dilakukan oleh individu, kelompok, atau organisasi dengan tujuan mencuri data, merusak sistem, menipu, mengganggu layanan, atau mencemarkan reputasi. Kejahatan siber mencakup, tetapi tidak terbatas pada peretasan, serangan DDoS, pencurian identitas, penipuan daring, dan penyebaran malware.[22]

b. Dampak Cyber Crime

Dampak cyber crime dapat sangat merugikan dan luas. Di tingkat individual, kejahatan siber dapat menyebabkan pencurian identitas, kehilangan data pribadi, dan kerugian finansial. Pada tingkat korporat, serangan cyber crime dapat mengakibatkan hilangnya data sensitif, merusak reputasi perusahaan, dan menyebabkan kerugian finansial yang signifikan. Di tingkat nasional, ancaman cyber crime dapat mengganggu

[21] Cybercrime.gov, "What Is Cybercrime?", www.cybercrime.gov/about-us
[22] National Crime Agency, "Cyber Crime", www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime

infrastruktur kritis, mencuri data rahasia negara, dan menyebabkan kerugian ekonomi secara keseluruhan.[23]

Kejahatan siber juga dapat menyebabkan penyebaran informasi pribadi yang sensitif, mengancam privasi dan keamanan seseorang. Di sisi lain, serangan terhadap perusahaan dapat menyebabkan kerugian besar, termasuk kehilangan data klien atau karyawan, merusak citra merek, dan menghambat operasional bisnis.

Pada tingkat yang lebih luas, serangan terhadap infrastruktur kritis seperti kelistrikan, telekomunikasi, atau transportasi dapat memiliki konsekuensi serius bagi masyarakat secara keseluruhan. Kondisi ini menunjukkan pentingnya perlunya upaya kolektif dari pemerintah, sektor swasta, dan masyarakat untuk menghadapi ancaman cyber crime dengan serius.[24]

c. Ancaman di Era Digital

Ancaman cyber crime di era digital bukan hanya menjadi masalah nasional, tetapi juga mengharuskan kerja sama dan koordinasi antara negara-negara di tingkat regional dan internasional. Di dalam kawasan Asia Tenggara, ASEAN memiliki peran penting dalam menciptakan lingkungan yang aman dan bermutu dalam hal keamanan siber dengan membangun kerjasama di antara negara-negara anggotanya.[25]

---

[23] PricewaterhouseCoopers, "Global Economic Crime and Fraud Survey 2020", www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html

[24] United Nations, "Global Cybersecurity Index 2021", www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[25] ASEAN Secretariat, "ASEAN Cybersecurity Cooperation Programme (ACCP)", www.asean.org/asean/asean-cybersecurity-cooperation-programme/

Era digital telah membawa perubahan besar dalam cara kita berkomunikasi, bekerja, dan bertransaksi. Namun, ini juga membawa ancaman baru dalam bentuk cyber crime. Teknologi digital yang terus berkembang memberikan celah bagi para pelaku kejahatan siber untuk mengembangkan metode baru dan lebih canggih untuk mencuri data, merusak sistem, dan menyebabkan kerugian.[26]

d. Tingkat Global dan Regional

Ancaman cyber crime bersifat lintas negara dan tidak mengenal batas wilayah. Pelaku kejahatan siber dapat beroperasi dari negara-negara yang berbeda, menyulitkan penegakan hukum dan pertahanan. Di tingkat regional, ASEAN memiliki peran kunci dalam mengatasi ancaman cyber crime dengan memperkuat kerjasama antar negara anggota dan membangun kapasitas keamanan siber.[27]

2. Definisi Cyber Crime dan Jenis-jenisnya

a. Definisi Cyber Crime

Cyber crime, juga dikenal sebagai kejahatan siber, merujuk pada berbagai tindakan kriminal yang dilakukan menggunakan teknologi komputer dan internet sebagai sarana untuk mencuri, merusak, atau merugikan individu, kelompok, atau organisasi lainnya.[28] Kejahatan siber melibatkan penyalahgunaan teknologi informasi dan komunikasi untuk

---

[26] Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2020", www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[27] Council of Europe, "Guidelines for the Creation of a National Cybercrime Strategy", www.coe.int/en/web/cybercrime/cybercrime-strategies

[28] NortonLifeLock, "Cybercrime Definitions and Terms", www.nortonlifelock.com/cybersecurity-definition

mencapai tujuan yang melanggar hukum. Aktivitas ini dapat dilakukan oleh individu atau kelompok dengan berbagai motif, termasuk mencari keuntungan finansial, memperoleh informasi rahasia, menyebabkan kerusakan atau ketidaknyamanan, serta melakukan tindakan ilegal lainnya.[29]

b. Jenis-Jenis Cyber Crime

- Peretasan (Hacking): Peretasan adalah tindakan masuk secara tidak sah ke dalam sistem komputer, jaringan, atau perangkat lunak dengan tujuan mengakses, mengubah, atau mencuri data. Pelaku peretasan, yang sering disebut sebagai hacker, dapat memanfaatkan celah keamanan dalam infrastruktur teknologi untuk mencapai tujuan mereka.
- Serangan DDoS (Distributed Denial of Service): Serangan DDoS adalah upaya untuk menghancurkan aksesibilitas sebuah situs web atau layanan daring dengan membanjiri server target dengan lalu lintas data yang berlebihan. Akibatnya, server menjadi tidak mampu melayani permintaan pengguna yang sah.
- Pencurian Identitas (Identity Theft): Pencurian identitas terjadi ketika seseorang mencuri informasi pribadi seseorang, seperti nomor identifikasi, nama, atau data keuangan, untuk melakukan penipuan atau aktivitas ilegal lainnya atas nama korban.
- Phishing: Phishing adalah taktik penipuan di mana penyerang mencoba memperoleh informasi sensitif, seperti kata sandi atau informasi kartu

[29] United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime", www.unodc.org/documents/organized-crime/cybercrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

kredit, dengan menyamar sebagai entitas tepercaya melalui email, pesan teks, atau situs web palsu.

- Ransomware: Ransomware adalah jenis malware yang mengenkripsi data pada perangkat korban dan kemudian menuntut pembayaran tebusan agar data tersebut dikembalikan atau dekripsi diberikan.
- Cyber Espionase (Spionase Siber): Cyber espionase adalah kegiatan memantau dan mencuri informasi rahasia atau data sensitif dari perusahaan, pemerintah, atau individu untuk tujuan intelijen atau keuntungan komersial.
- Pornografi Anak (Child Pornography): Kejahatan ini melibatkan produksi, distribusi, atau konsumsi materi pornografi yang melibatkan anak di bawah umur. Pornografi anak merupakan tindakan ilegal yang serius dan keji yang harus diberantas dengan tegas.
- Cyberbullying (Pembullyan Siber): Cyberbullying adalah penggunaan teknologi digital dan media sosial untuk menyerang, mengintimidasi, atau merendahkan seseorang secara online, yang dapat menyebabkan dampak psikologis yang serius pada korban.

3. Tren dan Perkembangan Cyber Crime di Tingkat Global dan Regional

Tren dan perkembangan cyber crime di tingkat global dan regional adalah aspek penting dalam memahami bagaimana kejahatan siber terus berkembang dan beradaptasi dengan lingkungan digital yang selalu berubah. Cyber crime telah menjadi ancaman yang semakin kompleks dan menantang, yang melibatkan pelaku dari berbagai latar belakang dengan motivasi yang beragam. Dalam sub bab ini, kita akan menjelaskan tentang tren dan perkembangan

terbaru dalam cyber crime di tingkat global dan regional, serta dampaknya terhadap masyarakat dan perekonomian.

a. Tren dan Perkembangan Cyber Crime di Tingkat Global.

- **Peningkatan Frekuensi dan Kekuatan Serangan:**

  Di tingkat global, terjadi peningkatan frekuensi dan kompleksitas serangan cyber crime. Pelaku kejahatan siber menggunakan teknologi yang semakin canggih dan metode yang lebih canggih untuk meretas sistem, mencuri data sensitif, dan mengakibatkan gangguan besar pada infrastruktur dan layanan.

- **Ransomware dan Extortion:**

  Serangan ransomware menjadi salah satu tren paling mengkhawatirkan dalam kejahatan siber. Pelaku menggunakan ransomware untuk mengenkripsi data korban dan meminta tebusan dalam bentuk kripto-mata uang agar data dapat dikembalikan. Perusahaan besar, lembaga pemerintah, dan bahkan rumah sakit telah menjadi sasaran serangan ransomware yang merugikan.

- **Targetisasi Terhadap Industri dan Sektor Tertentu:**

  Pelaku kejahatan siber semakin menargetkan sektor tertentu, seperti sektor kesehatan, perbankan, dan energi. Serangan terhadap infrastruktur kritis dan industri yang vital bagi perekonomian sering kali dilakukan untuk mencuri data strategis atau menciptakan ketidakstabilan.

- **Peningkatan Kejahatan Terkait Finansial:**

Kejahatan siber yang terkait dengan keuangan, seperti pencurian data kartu kredit dan skimming, masih menjadi ancaman serius bagi konsumen dan bisnis. Serangan phishing juga menjadi metode populer bagi pelaku cyber crime untuk mencuri informasi keuangan korban.

b. Tren dan Perkembangan Cyber Crime di Tingkat Regional (ASEAN)

- **Kerjasama Regional dalam Menghadapi Ancaman Cyber Crime:**

  Di tingkat regional ASEAN, negara-negara anggota berupaya untuk meningkatkan kerjasama dalam mengatasi cyber crime. Inisiatif seperti ASEAN Cyber Security Cooperation Program (ACSCP) dan pembentukan Pusat Pemantauan Kejahatan Siber ASEAN (ACCC) adalah langkah-langkah positif dalam membangun kerjasama antar negara anggota.

- **Pelatihan dan Peningkatan Kapasitas:**

  Negara-negara anggota ASEAN berfokus pada pelatihan personel keamanan siber dan penegak hukum untuk meningkatkan kapasitas dalam menghadapi ancaman cyber crime. Pertukaran informasi tentang ancaman dan teknik serangan juga menjadi bagian dari upaya meningkatkan kesadaran dan resiliensi.

- **Ancaman terhadap Infrastruktur Kritis dan Industri:**

  Seperti di tingkat global, terjadi peningkatan ancaman terhadap infrastruktur kritis dan industri penting di kawasan ASEAN. Ini menekankan pentingnya memperkuat sistem keamanan untuk melindungi infrastruktur dan data vital.

- **Pelanggaran Data Pribadi:**

Tren serangan yang terkait dengan pelanggaran data pribadi juga meningkat di tingkat regional. Hal ini menekankan perlunya mengadopsi regulasi dan kebijakan yang ketat untuk melindungi data pribadi warga negara ASEAN.

4. Peran Indonesia dalam Mengatasi Cyber Crime

Peran Indonesia dalam mengatasi cyber crime menjadi hal yang sangat penting mengingat kompleksitas dan dampak yang ditimbulkan oleh kejahatan siber dalam era digital ini. Pemerintah Indonesia telah mengambil langkah-langkah strategis dan upaya kolaboratif dalam menghadapi ancaman cyber crime untuk melindungi warganya, infrastruktur, serta keamanan nasional secara keseluruhan. Berikut adalah penjelasan lebih mendalam tentang peran Indonesia dalam mengatasi cyber crime:

a. Kebijakan dan Regulasi Terkait Keamanan Siber

Pemerintah Indonesia telah menetapkan kebijakan dan regulasi yang mengatur keamanan siber dan cyber crime. Di antaranya adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur tindakan kriminal di dunia maya, seperti penyebaran konten ujaran kebencian, penipuan, dan pencemaran nama baik melalui media elektronik. UU ITE juga mengatur mengenai perlindungan data dan informasi dalam transaksi elektronik.

b. Pembentukan Badan Nasional Keamanan Siber (BSSN)

Pada tahun 2017, Indonesia membentuk Badan Siber dan Sandi Negara (BSSN) sebagai lembaga yang bertanggung jawab untuk mengkoordinasikan upaya keamanan siber di tingkat nasional. BSSN

memiliki peran strategis dalam mencegah dan menanggulangi ancaman cyber crime serta membangun kerja sama dengan lembaga terkait di dalam negeri dan luar negeri.

c. Peningkatan Kapasitas dan Pelatihan Personel Keamanan Siber

Pemerintah Indonesia telah melakukan upaya untuk meningkatkan kapasitas dalam menghadapi cyber crime dengan memperkuat tim ahli keamanan siber dan melatih personel penegak hukum dalam penanganan kasus-kasus cyber crime. Ini mencakup pelatihan dalam identifikasi, analisis, dan penindakan terhadap serangan kejahatan siber.

d. Kerjasama Internasional dalam Menghadapi Ancaman Cyber Crime

Indonesia juga telah bekerja sama dengan negara-negara lain, termasuk anggota ASEAN, dalam pertukaran informasi dan intelijen terkait ancaman cyber crime. Kerjasama ini membantu dalam menghadapi serangan yang bersifat lintas negara dan memperkuat upaya penegakan hukum global terhadap pelaku cyber crime.

e. Perlindungan Infrastruktur Kritis dan Sektor Strategis

Pemerintah Indonesia juga telah memberikan perhatian khusus terhadap perlindungan infrastruktur kritis dan sektor-sektor strategis yang menjadi sasaran utama serangan cyber crime. Ini mencakup sektor kesehatan, perbankan, energi, telekomunikasi, dan sektor publik lainnya.

f. Peningkatan Kesadaran Masyarakat tentang Keamanan Cyber

Selain upaya penanganan secara teknis, pemerintah juga berfokus pada meningkatkan kesadaran masyarakat tentang ancaman cyber crime dan tindakan pencegahannya. Melalui kampanye kesadaran publik, seminar, dan

pelatihan, masyarakat didorong untuk lebih berhati-hati dan waspada terhadap ancaman cyber crime.

g. Penyuluhan dan Edukasi tentang Penggunaan Internet yang Aman

Pemerintah Indonesia juga aktif melakukan penyuluhan dan edukasi kepada masyarakat, khususnya anak-anak dan remaja, tentang penggunaan internet yang aman dan bertanggung jawab. Hal ini bertujuan untuk mengurangi risiko penipuan dan eksploitasi anak secara daring.

h. Pengembangan Sumber Daya Manusia di Bidang Keamanan Siber

Pemerintah Indonesia juga telah memberikan perhatian pada pengembangan sumber daya manusia di bidang keamanan siber. Ini meliputi program pendidikan dan pelatihan bagi generasi muda yang tertarik untuk berkarir dalam keamanan siber, serta dukungan bagi para peneliti dan profesional keamanan siber di Indonesia.

i. Kolaborasi dengan Sektor Swasta dan Dunia Usaha

Pemerintah Indonesia juga menggandeng sektor swasta dan dunia usaha untuk bersama-sama mengatasi ancaman cyber crime. Kolaborasi ini mencakup berbagi informasi intelijen tentang serangan cyber, mengadopsi praktik keamanan siber yang baik, serta membentuk komunitas keamanan siber yang berfokus pada pertukaran pengalaman dan pengetahuan.

j. Penanganan dan Penyidikan Kasus Cyber Crime

Pemerintah Indonesia juga aktif dalam penanganan dan penyidikan kasus cyber crime. Unit-unit khusus dalam kepolisian dan penegak hukum telah dibentuk untuk mengidentifikasi dan menindak pelaku kejahatan siber,

serta melacak jejak digital untuk memperoleh bukti yang kuat dalam proses hukum.

Melalui berbagai upaya dan inisiatif di atas, peran Indonesia dalam mengatasi cyber crime terus berkembang dan berupaya mengurangi risiko serta dampak negatif dari kejahatan siber. Meskipun tantangan dalam menghadapi kejahatan siber tetap ada, dengan kolaborasi antara pemerintah, sektor swasta, dan masyarakat, Indonesia dapat menjadi lebih tangguh dalam menjaga keamanan siber dan membentengi diri dari ancaman cyber crime di era digital ini.

5. Peran ASEAN dalam Mengatasi Cyber Crime

Peran ASEAN dalam mengatasi cyber crime adalah kunci untuk menciptakan lingkungan digital yang aman dan stabil di kawasan Asia Tenggara. ASEAN, sebagai organisasi regional yang terdiri dari 10 negara anggota, telah mengambil langkah-langkah strategis untuk meningkatkan kerjasama dan koordinasi dalam menghadapi ancaman cyber crime yang semakin kompleks dan menantang. Berikut adalah penjelasan mendalam tentang peran ASEAN dalam mengatasi cyber crime.

a. Cyber Security Cooperation Program (ACSCP)

Salah satu inisiatif utama ASEAN dalam mengatasi cyber crime adalah ASEAN Cyber Security Cooperation Program (ACSCP). Program ini bertujuan untuk meningkatkan kapasitas negara-negara anggota dalam menghadapi ancaman keamanan siber melalui pelatihan, pertukaran informasi, dan pembentukan pusat keamanan siber.

b. Pusat Pemantauan Kejahatan Siber ASEAN (ACCC)

Selanjutnya, ASEAN juga merencanakan pembentukan Pusat Pemantauan Kejahatan Siber ASEAN (ACCC) sebagai platform untuk mendeteksi, menganalisis, dan menanggulangi serangan cyber crime di tingkat regional. Pusat ini akan memungkinkan negara-negara anggota untuk berbagi informasi tentang ancaman keamanan siber dan merespons secara cepat.

c. Pertukaran Informasi Intelijen

ASEAN telah mendorong pertukaran informasi intelijen tentang ancaman cyber crime antara negara-negara anggotanya. Hal ini memungkinkan para pihak untuk saling memahami pola serangan, teknik, dan metode pelaku kejahatan siber, sehingga dapat mengambil langkah-langkah pencegahan dan penanggulangan yang lebih efektif.

d. Kerjasama dengan Mitra Eksternal

ASEAN juga telah menjalin kerjasama dengan negara-negara mitra eksternal, termasuk China, Jepang, Korea Selatan, dan Amerika Serikat, dalam mengatasi cyber crime. Kerjasama ini mencakup pertukaran intelijen, penanganan insiden bersama, dan dialog kebijakan tentang isu-isu keamanan siber.

e. Mendorong Kesadaran tentang Keamanan Siber

Selain kerjasama antar pemerintah, ASEAN juga berfokus pada meningkatkan kesadaran masyarakat tentang ancaman cyber crime dan tindakan pencegahannya. Ini mencakup kampanye kesadaran publik, seminar, dan pelatihan untuk mengedukasi masyarakat tentang pentingnya keamanan siber dalam era digital.

B. Implementasi Treaty Of Amity And Cooperation Terhadap Cyber Crime Di Indonesia

Treaty of Amity and Cooperation (TAC) atau Perjanjian Persahabatan dan Kerjasama adalah perjanjian multilateral yang menjadi landasan penting bagi kerjasama politik, keamanan, dan ekonomi di kawasan Asia Tenggara, yang terdiri dari negara-negara anggota ASEAN dan beberapa negara mitra di luar kawasan. TAC, yang ditandatangani pada tanggal 24 Februari 1976 di Bali, Indonesia, bertujuan untuk mempromosikan perdamaian dan stabilitas di kawasan serta membangun hubungan yang saling menguntungkan antar negara-negara anggota. Selama beberapa dekade terakhir, perkembangan teknologi informasi dan komunikasi yang pesat telah membawa tantangan baru bagi keamanan kawasan, khususnya dalam bentuk cyber crime.

Dalam era digital yang terus berkembang, cyber crime telah menjadi ancaman global yang semakin serius dan kompleks. Serangan siber dapat mengakibatkan kerugian finansial, pencurian data pribadi, merusak reputasi, serta mengancam infrastruktur kritis dan keamanan nasional. Oleh karena itu, mengatasi cyber crime memerlukan kerjasama yang erat antar negara, terutama di tingkat regional, untuk membangun resiliensi dan memberikan perlindungan yang lebih baik bagi warga negara dan infrastruktur.

Implementasi TAC dalam menghadapi cyber crime di Indonesia menjadi sangat relevan karena ASEAN, sebagai organisasi regional yang beranggotakan Indonesia dan negara-negara lain di Asia Tenggara, telah berkomitmen untuk menjaga perdamaian, stabilitas, dan keamanan di kawasan. Perjanjian ini mencakup prinsip-prinsip seperti menghormati kedaulatan negara, tidak

melakukan intervensi dalam urusan dalam negeri, menyelesaikan perbedaan secara damai, serta tidak menggunakan kekuatan untuk mengancam integritas wilayah negara lain.

a. Pertimbangan Implementasi TAC dalam Mengatasi Cyber Crime

Pertimbangan implementasi Treaty of Amity and Cooperation (TAC) dalam mengatasi cyber crime memiliki peran yang penting dalam menciptakan kerjasama regional yang efektif dan saling menguntungkan dalam menghadapi ancaman keamanan siber di kawasan ASEAN. Pentingnya pertimbangan implementasi TAC dalam mengatasi cyber crime adalah untuk menciptakan lingkungan regional yang aman dan stabil dalam menghadapi tantangan keamanan siber yang semakin kompleks. Dengan mengikuti prinsip-prinsip TAC dan memperkuat kerjasama regional, negara-negara anggota ASEAN dapat lebih efektif dalam melindungi warga negara dan infrastruktur dari serangan cyber crime, serta membangun resiliensi dalam menghadapi ancaman siber di era digital ini.

a) Penjelasan mengapa TAC relevan dalam konteks mengatasi ancaman cyber crime dan keamanan siber di era digital.

Treaty of Amity and Cooperation (TAC) adalah perjanjian penting yang menjadi landasan kerjasama antara negara-negara anggota ASEAN dalam menjaga perdamaian, stabilitas, dan kemajuan di kawasan Asia Tenggara. Meskipun TAC awalnya tidak secara khusus menyebutkan tentang cyber crime dan keamanan siber, perjanjian ini tetap relevan dalam konteks menghadapi ancaman siber di era digital.

Berikut adalah penjelasan mengapa TAC relevan dan penting dalam mengatasi ancaman cyber crime dan keamanan siber di era digital:

1) **Prinsip Penghormatan Kedaulatan dan Integritas Wilayah (Principle of Respecting Sovereignty and Territorial Integrity)**

   TAC menegaskan pentingnya menghormati kedaulatan dan integritas wilayah negara-negara anggota ASEAN. Dalam konteks keamanan siber, negara-negara anggota harus menghormati integritas wilayah di ruang siber dan tidak melakukan serangan siber yang mengancam kedaulatan negara lain. Hal ini relevan karena serangan siber dapat menyerang infrastruktur kritis dan data sensitif, dan melalui prinsip ini, negara-negara anggota dapat bekerja sama untuk melindungi wilayah masing-masing dari serangan siber yang bersifat merusak.[30]

2) **Prinsip Non-Intervensi (*Principle of Non-Interference*)**

   TAC juga menekankan prinsip non-intervensi dalam urusan dalam negeri negara anggota. Dalam konteks keamanan siber, prinsip ini relevan karena negara-negara anggota harus menghormati hak kedaulatan negara lain untuk mengelola dan melindungi keamanan siber di wilayahnya sendiri. Ini berarti negara-negara anggota tidak boleh melakukan serangan siber atau campur tangan dalam infrastruktur keamanan siber negara lain.[31]

---

[30] ASEAN Secretariat, "ASEAN Treaty of Amity and Cooperation," www.asean.org/asean/about-asean/asean-treaty-of-amity-and-cooperation/

[31] *Ibid*

3) **Prinsip Penyelesaian Perbedaan dengan Damai (*Principle of Settling Disputes by Peaceful Means*)**

Dalam menghadapi ancaman cyber crime, TAC mendorong negara-negara anggota untuk menyelesaikan perbedaan atau sengketa yang mungkin muncul melalui jalur damai dan dialog, bukan dengan kekerasan atau konflik militer. Prinsip ini relevan karena cyber crime dapat menyebabkan ketegangan antara negara-negara anggota, dan melalui pendekatan damai, negara-negara anggota dapat menangani masalah tersebut dengan bijaksana dan menghindari eskalasi konflik.[32]

4) **Pertukaran Informasi dan Kerjasama (Information Sharing and Cooperation)**

TAC memberikan landasan bagi negara-negara anggota untuk meningkatkan kerjasama dalam berbagai bidang, termasuk keamanan siber. Melalui pertukaran informasi tentang ancaman cyber crime, teknik serangan, dan taktik pelaku kejahatan siber, negara-negara anggota dapat saling membantu dalam menghadapi ancaman siber yang semakin kompleks.[33]

5) **Penguatan Kerjasama Regional dan Internasional (Strengthening Regional and International Cooperation)**

[32] *Ibid*
[33] *Ibid*

TAC mendorong penguatan kerjasama regional dan internasional untuk menjaga perdamaian dan keamanan di kawasan. Dalam konteks keamanan siber, hal ini relevan karena ancaman cyber crime seringkali bersifat lintas negara. Dengan mengadopsi prinsip TAC, negara-negara anggota dapat bekerja sama dengan negara-negara mitra di luar kawasan ASEAN untuk menghadapi ancaman siber secara lebih efektif.[34]

6) **Pengembangan Kapasitas Nasional (National Capacity Building)**

TAC juga mengakui pentingnya pengembangan kapasitas nasional dalam menghadapi tantangan keamanan. Dalam konteks keamanan siber, negara-negara anggota perlu memperkuat kapasitas keamanan siber nasional untuk menghadapi serangan cyber crime. Dengan kerjasama regional yang diberdayakan oleh TAC, negara-negara anggota dapat saling mendukung dalam pengembangan kapasitas keamanan siber masing-masing.[35]

b) Analisis tentang bagaimana TAC dapat memberikan landasan hukum dan kerangka kerjasama bagi negara-negara anggota ASEAN dalam menghadapi cyber crime.

[34] *Ibid*
[35] *Ibid*

Treaty of Amity and Cooperation (TAC) adalah perjanjian multilateral yang menjadi landasan penting bagi kerjasama politik, keamanan, dan ekonomi di kawasan Asia Tenggara. Dalam menghadapi tantangan ancaman cyber crime yang semakin kompleks di era digital, TAC memiliki potensi untuk memberikan landasan hukum dan kerangka kerjasama bagi negara-negara anggota ASEAN dalam menghadapi ancaman keamanan siber secara efektif. Berikut adalah analisis tentang bagaimana TAC dapat memberikan landasan hukum dan kerangka kerjasama tersebut:

1) **Menegakkan Prinsip-Prinsip Dasar Hukum Internasional**

   TAC mengakui dan menegakkan prinsip-prinsip dasar hukum internasional, termasuk penghormatan kedaulatan, integritas wilayah, dan non-intervensi. Dalam konteks cyber crime, prinsip-prinsip ini menjadi landasan hukum bagi negara-negara anggota ASEAN untuk melindungi wilayahnya dari serangan siber yang dapat mengancam kedaulatan dan keamanan nasional.[36]

2) **Mengakui Cyber Space sebagai Area yang Dihormati (*Respect for Cyberspace as a Respectable Area*)**

   TAC tidak secara khusus menyebutkan tentang cyber space, tetapi prinsip menghormati kedaulatan negara dan wilayah secara tidak langsung dapat diterapkan dalam ruang siber. Hal ini memberikan landasan hukum bagi negara-negara anggota ASEAN

[36] ASEAN Secretariat, "ASEAN Treaty of Amity and Cooperation," www.asean.org/asean/about-asean/asean-treaty-of-amity-and-cooperation/

untuk saling menghormati wilayah siber masing-masing dan tidak menggunakan cyber space untuk melakukan serangan atau campur tangan dalam urusan dalam negeri negara lain.[37]

3) **Mendukung Pertukaran Informasi dan Intelijen (*Supporting Information and Intelligence Sharing*)**

Dalam menghadapi ancaman cyber crime, TAC dapat memberikan landasan hukum bagi negara-negara anggota ASEAN untuk saling bertukar informasi dan intelijen tentang ancaman keamanan siber. Dalam perjanjian ini, negara-negara anggota diberi kebebasan untuk saling memberikan peringatan dini dan informasi terkait serangan siber, sehingga dapat meningkatkan kesadaran dan kewaspadaan dalam menghadapi ancaman cyber crime.[38]

4) **Mendorong Kerjasama di Bidang Keamanan Siber (Promoting Cooperation in Cybersecurity)**

TAC mendorong negara-negara anggota ASEAN untuk bekerja sama dalam bidang keamanan siber. Ini mencakup pengembangan kapasitas keamanan siber, pertukaran teknologi dan keahlian, serta penyusunan kebijakan dan strategi bersama dalam menghadapi ancaman cyber crime. Prinsip ini memberikan landasan kerangka kerjasama yang lebih kuat dan terkoordinasi dalam mengatasi ancaman keamanan siber.

---

[37] ASEAN Secretariat, "ASEAN Treaty of Amity and Cooperation," www.asean.org/asean/about-asean/asean-treaty-of-amity-and-cooperation/

[38] ASEAN Secretariat, "ASEAN Treaty of Amity and Cooperation," www.asean.org/asean/about-asean/asean-treaty-of-amity-and-cooperation/

5) **Menumbuhkan Kerjasama dengan Pihak Ketiga (Promoting Cooperation with Third Parties)**

TAC memungkinkan negara-negara anggota ASEAN untuk menjalin kerjasama dengan pihak ketiga, termasuk negara mitra di luar kawasan ASEAN, dalam menghadapi cyber crime. Kerjasama ini dapat mencakup pertukaran informasi dan pengalaman, pelatihan, serta koordinasi tindakan dalam menangani ancaman siber yang bersifat lintas negara.

6) **Mendukung Inisiatif Kerjasama Regional dan Internasional (Supporting Regional and International Cooperation Initiatives)**

TAC mendorong negara-negara anggota untuk mendukung inisiatif kerjasama regional dan internasional dalam menghadapi ancaman cyber crime. Ini mencakup partisipasi dalam program kerjasama keamanan siber di tingkat ASEAN, seperti *ASEAN Cyber Security Cooperation Program* (ACSCP) dan *ASEAN Regional Forum* (ARF), yang dapat memperkuat kapasitas dan resiliensi dalam menghadapi ancaman siber di kawasan dan dunia internasional.

7) **Mengikatkan Diri dalam Prinsip Saling Mendukung (Committing to the Principle of Mutual Support)**

TAC menetapkan prinsip saling mendukung antara negara-negara anggota ASEAN. Dalam konteks keamanan siber, prinsip ini menggarisbawahi pentingnya negara-negara anggota untuk saling membantu dan berkoordinasi dalam menghadapi ancaman cyber crime yang dapat berdampak secara luas pada kawasan ASEAN.

8) Menghadirkan Forum Diplomasi untuk Penyelesaian Sengketa (Providing Diplomatic Forum for Dispute Resolution)

Dalam konteks menghadapi ancaman cyber crime, TAC dapat memberikan landasan hukum bagi negara-negara anggota ASEAN untuk menggunakan forum diplomatik sebagai sarana penyelesaian sengketa terkait keamanan siber. Forum seperti ASEAN Regional Forum (ARF) dapat menjadi platform untuk membahas isu-isu keamanan siber dan mencari solusi bersama dalam mengatasi ancaman cyber crime di kawasan.

Dengan berbagai prinsip dan landasan hukum yang diberikan oleh TAC, negara-negara anggota ASEAN dapat menciptakan kerjasama yang lebih erat dan terkoordinasi dalam menghadapi ancaman cyber crime dan meningkatkan keamanan siber di kawasan ASEAN. Implementasi prinsip-prinsip TAC secara efektif dalam mengatasi ancaman keamanan siber akan memperkuat kemampuan negara-negara anggota untuk melindungi wilayahnya dari serangan siber dan membangun lingkungan digital yang aman dan stabil di era digital ini.

c) Penerapan Prinsip-Prinsip TAC dalam Penanggulangan Cyber Crime di Indonesia

Treaty of Amity and Cooperation (TAC) merupakan perjanjian yang penting bagi negara-negara anggota ASEAN, termasuk Indonesia, dalam menciptakan kerjasama politik, keamanan, dan ekonomi di kawasan Asia Tenggara. Prinsip-prinsip TAC, seperti menghormati kedaulatan negara, menghormati integritas wilayah, dan non-intervensi, menjadi panduan bagi Indonesia dalam upaya penanggulangan cyber crime. Berikut adalah penjelasan tentang bagaimana Indonesia menerapkan prinsip-prinsip TAC tersebut dalam upaya penanggulangan cyber crime.

1) Penjelasan tentang bagaimana Indonesia menerapkan prinsip-prinsip TAC, seperti menghormati kedaulatan negara, menghormati integritas wilayah, dan non-intervensi, dalam upaya penanggulangan cyber crime.

a. Menghormati Kedaulatan Negara (Respecting National Sovereignty)

Indonesia menghormati kedaulatan negara-negara anggota ASEAN, termasuk dalam konteks keamanan siber. Dalam upaya penanggulangan cyber crime, Indonesia menjamin bahwa kegiatan keamanan siber yang dilakukan di wilayahnya tidak melanggar kedaulatan negara-negara lain. Hal ini berarti bahwa Indonesia tidak akan melakukan serangan siber atau campur

tangan dalam infrastruktur keamanan siber negara lain tanpa izin atau permintaan dari negara tersebut.

Dalam menghormati kedaulatan negara-negara anggota ASEAN, Indonesia juga aktif dalam membangun kerjasama bilateral dan multilateral dalam hal penanggulangan cyber crime. Indonesia berkomitmen untuk menghormati hak kedaulatan negara lain untuk melindungi wilayah sibernya sendiri, dan sebaliknya, Indonesia juga berharap negara-negara lain menghormati kedaulatan wilayah siber Indonesia.

b. Menghormati Integritas Wilayah (Respecting Territorial Integrity)

Prinsip menghormati integritas wilayah dalam TAC juga relevan dalam konteks keamanan siber. Indonesia memahami bahwa ancaman cyber crime dapat menyasar infrastruktur kritis, data sensitif, dan sumber daya penting negara. Dalam upaya penanggulangan cyber crime, Indonesia menjaga integritas wilayah sibernya agar tetap aman dari serangan siber yang dapat mengancam keutuhan dan stabilitas nasional.

Selain itu, Indonesia juga berkomitmen untuk tidak melakukan serangan siber yang dapat mengancam integritas wilayah siber negara lain. Negara-negara anggota ASEAN, termasuk Indonesia, saling menjaga agar tidak ada tindakan yang merusak wilayah siber negara-negara lain, sejalan dengan prinsip menghormati integritas wilayah dalam TAC.

c. Prinsip Non-Intervensi (Principle of Non-Interference)

TAC menegaskan pentingnya prinsip non-intervensi dalam urusan dalam negeri negara-negara anggota. Dalam penanggulangan cyber crime, prinsip ini relevan karena Indonesia tidak akan menggunakan serangan siber atau campur tangan dalam urusan keamanan siber negara lain tanpa izin atau permintaan resmi.

Indonesia juga menghormati prinsip non-intervensi dalam keamanan siber dengan tidak melakukan kegiatan siber yang dapat merusak infrastruktur atau sistem komunikasi negara-negara lain. Sebaliknya, Indonesia memfokuskan upaya penanggulangan cyber crime pada melindungi dan meningkatkan keamanan siber nasional tanpa campur tangan dalam urusan keamanan siber negara-negara anggota ASEAN lainnya.

d. Mendorong Kerjasama Regional dan Internasional (Promoting Regional and International Cooperation)

Salah satu prinsip utama dalam TAC adalah mendorong kerjasama regional dan internasional untuk menciptakan lingkungan yang aman dan stabil. Dalam upaya penanggulangan cyber crime, Indonesia aktif berpartisipasi dalam inisiatif kerjasama regional dan internasional yang bertujuan untuk mengatasi ancaman keamanan siber.

Indonesia mendukung kerjasama bilateral dan multilateral dalam pertukaran informasi intelijen tentang ancaman cyber crime, pelatihan untuk meningkatkan kemampuan penanggulangan cyber crime, dan pengembangan kapasitas keamanan siber. Melalui kerjasama regional dan internasional ini, Indonesia bersama negara-negara anggota ASEAN lainnya dapat saling mendukung dalam upaya penanggulangan cyber crime secara lebih efektif

2) Contoh konkrit tindakan atau kebijakan yang diambil oleh pemerintah Indonesia berdasarkan prinsip-prinsip TAC dalam menghadapi ancaman cyber crime.

Pemerintah Indonesia telah mengambil berbagai tindakan dan kebijakan berdasarkan prinsip-prinsip TAC dalam menghadapi ancaman cyber crime. Berikut adalah beberapa contoh konkrit tindakan atau kebijakan yang diambil oleh pemerintah Indonesia

a. Pembentukan Lembaga dan Kebijakan Keamanan Siber

Pemerintah Indonesia telah membentuk lembaga dan kebijakan khusus untuk menghadapi ancaman cyber crime dan meningkatkan keamanan siber di negara ini. Salah satu contoh adalah Badan Siber dan Sandi Negara (BSSN) yang berfungsi sebagai lembaga pusat untuk mengkoordinasikan kebijakan, standar, dan koordinasi nasional terkait keamanan siber. BSSN juga bertugas melindungi infrastruktur kritis negara dari serangan siber dan memberikan bimbingan serta dukungan

teknis kepada sektor publik dan swasta dalam meningkatkan keamanan siber.

b. Peningkatan Kapasitas dan Pelatihan Keamanan Siber

Pemerintah Indonesia telah mengambil langkah-langkah untuk meningkatkan kapasitas dan pelatihan dalam bidang keamanan siber. Melalui program-program pelatihan dan sertifikasi, pemerintah berupaya meningkatkan kemampuan personel dan profesional dalam mengatasi ancaman cyber crime. Selain itu, pemerintah juga menyediakan pelatihan khusus bagi aparat penegak hukum untuk mengidentifikasi, menyelidiki, dan menuntut pelaku kejahatan siber.

c. Pengembangan Kerjasama Bilateral dan Multilateral

Indonesia aktif menjalin kerjasama dengan negara-negara anggota ASEAN lainnya dan mitra internasional dalam menghadapi ancaman cyber crime. Melalui forum-forum seperti ASEAN Regional Forum (ARF) dan ASEAN Ministerial Conference on Cybersecurity (AMCC), Indonesia berpartisipasi dalam dialog dan kerjasama dengan negara-negara lain untuk pertukaran informasi dan pengalaman, serta membahas isu-isu keamanan siber secara bersama-sama.

d. Penandatanganan Perjanjian Kerjasama Cyber Crime

Indonesia telah menandatangani perjanjian kerjasama bilateral dengan beberapa negara dalam upaya penanggulangan cyber crime. Melalui perjanjian tersebut, negara-negara berkomitmen untuk saling bertukar informasi intelijen, berkoordinasi dalam menyelidiki tindakan kejahatan siber lintas negara, dan mendukung dalam penuntutan terhadap pelaku kejahatan siber.

e. Partisipasi dalam Inisiatif Internasional

Indonesia juga aktif berpartisipasi dalam inisiatif internasional yang bertujuan untuk meningkatkan keamanan siber di tingkat global. Sebagai contoh, Indonesia menjadi anggota Dewan Keamanan PBB (United Nations Security Council) untuk periode 2019-2020 dan berkontribusi dalam upaya internasional dalam menghadapi ancaman cyber crime di tingkat global.

f. Penyusunan Rancangan Undang-Undang Keamanan Siber

Pemerintah Indonesia sedang menyusun Rancangan Undang-Undang Keamanan Siber sebagai landasan hukum dalam menghadapi ancaman cyber crime dan meningkatkan keamanan siber secara komprehensif. Rancangan undang-undang ini diharapkan akan memberikan kerangka kerja yang lebih kuat dan komprehensif dalam penanggulangan ancaman cyber crime di Indonesia.

Tindakan dan kebijakan di atas mencerminkan komitmen pemerintah Indonesia dalam menghadapi ancaman cyber crime dengan mengikuti prinsip-prinsip TAC, termasuk menghormati kedaulatan negara, menghormati integritas wilayah, dan non-intervensi. Dengan implementasi prinsip-prinsip ini, Indonesia berusaha untuk menciptakan lingkungan siber yang aman dan stabil, tidak hanya di tingkat nasional, tetapi juga di kawasan Asia Tenggara dan dunia internasional.

g. Tantangan dan Proyeksi Masa Depan.

1) Analisis tentang tantangan yang dihadapi oleh Indonesia dalam mengimplementasikan TAC terhadap cyber crime, termasuk isu-isu hukum, teknis, dan politis yang mungkin timbul.

Secara keseluruhan, mengimplementasikan prinsip-prinsip TAC dalam menghadapi ancaman cyber crime adalah tugas yang kompleks dan menantang bagi Indonesia. Namun, dengan meningkatkan kapasitas keamanan siber, membangun kerjasama regional dan internasional, serta menyusun kebijakan yang komprehensif, Indonesia dapat menjadi lebih tangguh dalam menghadapi ancaman keamanan siber di masa depan. Proyeksi masa depan ini akan memastikan bahwa Indonesia dapat membangun lingkungan siber yang aman dan stabil bagi warganya dan juga bagi negara-negara anggota ASEAN lainnya.

a. **Tantangan Hukum**

- **Ketidakselarasan Hukum Antara Negara Anggota ASEAN**

  Setiap negara anggota ASEAN memiliki peraturan hukum dan sistem hukum yang berbeda-beda dalam mengatasi cyber crime. Hal ini dapat menyulitkan dalam koordinasi penegakan hukum lintas negara dan pertukaran informasi terkait kasus cyber crime.

- **Kekurangan Hukum Spesifik terkait Cyber Crime**

  Meskipun Indonesia telah memiliki Undang-Undang ITE (Informasi dan Transaksi Elektronik) yang mengatur cyber crime, tetapi masih ada kekurangan dalam bidang hukum spesifik yang dapat mengatasi ancaman cyber crime yang semakin kompleks. Dalam menghadapi cyber crime yang baru atau berkembang, hukum yang ada mungkin perlu diperbarui atau disempurnakan untuk tetap relevan dan efektif.

b. **Tantangan Teknis**

- **Keterbatasan Sumber Daya Manusia dan Teknologi**

  Menghadapi ancaman cyber crime yang semakin kompleks memerlukan keahlian teknis yang tinggi dan teknologi yang canggih. Namun, masih terdapat keterbatasan dalam jumlah personel keamanan siber yang terlatih dan jumlah sumber daya teknologi yang memadai di Indonesia. Hal ini dapat menyulitkan dalam menghadapi serangan cyber crime yang bersifat lintas negara dan membutuhkan kemampuan teknis yang tinggi.

- **Keterbatasan dalam Penyediaan Dana**

  Implementasi prinsip-prinsip TAC dalam menghadapi cyber crime memerlukan investasi dalam keamanan siber, termasuk teknologi keamanan terbaru dan pelatihan personel. Namun, terdapat keterbatasan dalam penyediaan dana untuk mengatasi ancaman keamanan siber yang semakin kompleks.

c. **Tantangan Politis**

- **Kerjasama Antar Lembaga Pemerintah**

  Penanggulangan cyber crime memerlukan kerjasama antar berbagai lembaga pemerintah, seperti kepolisian, militer, dan badan intelijen. Namun,

terkadang mungkin terjadi perbedaan pandangan dan kepentingan antar lembaga, yang dapat menghambat koordinasi dan kolaborasi dalam menghadapi ancaman cyber crime.

- **Isu Kedaulatan dan Privasi**

  Dalam upaya untuk menghadapi ancaman cyber crime, terkadang mungkin diperlukan kerjasama dengan negara-negara lain atau lembaga internasional. Namun, hal ini dapat menimbulkan isu-isu kedaulatan dan privasi, terutama jika informasi sensitif harus dibagikan dengan negara atau lembaga lain.

d. **Tantangan Terkait Pengaturan dan Pengawasan**

- **Regulasi Cross-Border**

  Ancaman cyber crime sering kali bersifat lintas negara, dan penegakan hukum lintas batas menjadi sulit karena perbedaan regulasi dan yurisdiksi. Indonesia perlu menghadapi tantangan pengaturan dan pengawasan dalam mengatasi serangan siber yang melibatkan negara lain.

- **Penyelidikan dan Pembuktian yang Rumit**

  Cyber crime seringkali dilakukan dengan cara yang sangat rahasia dan sulit diidentifikasi. Proses penyelidikan dan pembuktian dalam kasus cyber

crime bisa menjadi rumit dan memakan waktu, serta memerlukan kerjasama lintas sektor dan lembaga.

e. **Proyeksi Masa Depan**

- **Pengembangan Hukum dan Kebijakan yang Lebih Komprehensif**

  Indonesia perlu terus mengembangkan undang-undang dan kebijakan yang lebih komprehensif dalam mengatasi ancaman cyber crime. Penyempurnaan dan pembaruan Undang-Undang ITE serta pengembangan regulasi cyber security yang baru mungkin diperlukan untuk menangani ancaman yang semakin kompleks.

- **Peningkatan Investasi dalam Keamanan Siber**

  Proyeksi masa depan adalah peningkatan investasi dalam bidang keamanan siber untuk mengatasi tantangan teknis dan sumber daya. Pengadaan teknologi keamanan yang lebih canggih dan pelatihan personel keamanan siber yang lebih intensif dapat meningkatkan kemampuan Indonesia dalam menghadapi ancaman cyber crime.

- **Meningkatkan Kerjasama Antar Lembaga dan Lintas Sektor**

Peningkatan kerjasama antara berbagai lembaga pemerintah dan lintas sektor menjadi penting dalam menghadapi ancaman cyber crime. Koordinasi yang lebih baik antar lembaga dan sektor dapat meningkatkan efektivitas dan responsibilitas dalam penanggulangan cyber crime.

- **Kolaborasi dengan Negara-Negara Lain dan Lembaga Internasional**

  Indonesia perlu aktif berkolaborasi dengan negara-negara lain dan lembaga internasional dalam menghadapi ancaman cyber crime. Melalui pertukaran informasi dan pengalaman, Indonesia dapat memperkuat kapasitas keamanan siber dan merespons serangan cyber crime dengan lebih efektif.

- **Peningkatan Kesadaran dan Pendidikan Cyber Security**

  Peningkatan kesadaran dan pendidikan tentang cyber security menjadi proyeksi penting di masa depan. Dengan meningkatkan kesadaran publik dan pelatihan tentang praktik keamanan siber yang baik, masyarakat dapat lebih aktif dalam melindungi diri dari ancaman cyber crime.

Secara keseluruhan, menghadapi tantangan hukum, teknis, politis, dan pengaturan dalam mengimplementasikan TAC terhadap cyber crime adalah tugas yang kompleks dan memerlukan kerjasama dan komitmen dari berbagai pihak. Dengan langkah-langkah yang tepat, Indonesia dapat menghadapi ancaman cyber crime dengan lebih efektif dan menciptakan lingkungan siber yang lebih aman dan stabil bagi warganya.

C. Upaya Indonesia Dan ASEAN Dalam Mengatasi Hambatan Implementasi Treaty Of Amity And Cooperation Terhadap Cyber Crime

Keamanan siber adalah salah satu isu krusial di dunia saat ini. Ini mencakup perlindungan infrastruktur kritis, data sensitif, dan mencegah serangan siber yang dapat merusak ekonomi, keamanan nasional, dan stabilitas sosial. Ancaman cyber crime termasuk serangan siber yang dilakukan oleh individu, kelompok, atau negara dengan niat jahat, seperti pencurian data pribadi, peretasan sistem pemerintah, dan penyebaran malware. Ancaman semacam ini dapat menimbulkan kerugian besar bagi negara-negara ASEAN dan masyarakat global secara keseluruhan.

Hambatan-hambatan dalam implementasi TAC terhadap cyber crime mencakup sejumlah tantangan. Pertama, ada hambatan hukum dan regulasi yang mungkin tidak memadai atau belum diupdate untuk mengatasi perkembangan teknologi. Kedua, keterbatasan sumber daya, baik dalam hal anggaran maupun personel yang terlatih dalam keamanan siber. Ketiga, koordinasi antarlembaga di tingkat nasional seringkali menjadi masalah yang serius. Selain itu, ancaman dari aktor non-negara, seperti kelompok peretas atau entitas ilegal, semakin kompleks dan memerlukan pendekatan yang lebih

komprehensif. Terakhir, isu keamanan siber bersifat global, sehingga kerja sama regional dan internasional yang efektif sangat penting.

Indonesia telah melakukan sejumlah upaya dalam mengatasi hambatan implementasi TAC terhadap cyber crime. Ini mencakup pengembangan kebijakan nasional yang berfokus pada keamanan siber, perluasan kapasitas teknis dan manusia dalam bidang keamanan siber, serta kolaborasi dengan pihak swasta dan masyarakat sipil untuk menghadapi ancaman siber. Indonesia juga terlibat dalam kerja sama regional dan internasional dalam mengatasi keamanan siber.

ASEAN, melalui Sekretariat ASEAN, juga telah aktif dalam mengatasi hambatan implementasi TAC terhadap cyber crime. Ini mencakup berbagai inisiatif dan program yang dirancang untuk meningkatkan kapasitas anggota ASEAN dalam mengatasi ancaman siber. Kerja sama dengan mitra eksternal dan organisasi internasional juga menjadi bagian penting dari upaya ini.

a. Peran Indonesia dalam Mengatasi Hambatan Implementasi TAC

1. Kebijakan dan Inisiatif Nasional dalam Mengatasi Cyber Crime:
    a) Kebijakan Nasional Terkait Keamanan Siber: Indonesia telah mengembangkan berbagai kebijakan dan kerangka hukum yang mengatur keamanan siber. Ini mungkin termasuk pembentukan badan atau lembaga khusus yang bertugas mengatasi keamanan siber, serta penetapan hukuman dan sanksi yang tegas terhadap pelaku cyber crime. Anda dapat merinci berbagai undang-undang, peraturan, atau inisiatif nasional yang telah diambil Indonesia untuk menghadapi ancaman cyber crime.

b) Inisiatif untuk Pendidikan dan Pelatihan: Selain kebijakan hukum, Indonesia juga mungkin telah mengambil inisiatif untuk meningkatkan pendidikan dan pelatihan dalam bidang keamanan siber. Ini termasuk program-program yang dirancang untuk menghasilkan lebih banyak tenaga ahli di bidang keamanan siber, serta peningkatan kesadaran masyarakat tentang risiko cyber crime.

c) Peran Pemerintah dalam Perlindungan Data: Anda juga dapat menjelaskan peran pemerintah dalam melindungi data pribadi dan sensitif baik di sektor publik maupun swasta. Ini bisa mencakup regulasi tentang perlindungan data dan pengawasan terhadap perusahaan yang mengelola data.

2. Kolaborasi antara Pemerintah, Swasta, dan Masyarakat Sipil:

a) Kemitraan dengan Sektor Swasta: Indonesia mungkin telah membangun kemitraan yang kuat dengan perusahaan-perusahaan swasta yang memiliki kepentingan dalam keamanan siber. Ini bisa termasuk penyedia layanan internet, perusahaan teknologi, dan penyedia keamanan siber. Kolaborasi semacam ini dapat mencakup pertukaran informasi, pelatihan bersama, dan upaya bersama dalam mengatasi ancaman cyber crime.

b) Keterlibatan Masyarakat Sipil: Masyarakat sipil juga memiliki peran penting dalam mengatasi cyber crime. Anda dapat menjelaskan inisiatif yang diambil oleh pemerintah Indonesia dalam menggandeng organisasi masyarakat sipil, kelompok aktivis, dan

lembaga non-pemerintah dalam mempromosikan kesadaran tentang keamanan siber dan melaporkan tindakan cyber crime.

3. Keterlibatan Indonesia dalam Kerja Sama Regional terkait Cyber Security:
    a) Kerja Sama dengan Negara-Negara Tetangga: Indonesia, sebagai salah satu negara anggota ASEAN, mungkin telah aktif dalam kerja sama dengan negara-negara tetangga dalam mengatasi ancaman keamanan siber. Ini bisa termasuk pertukaran informasi tentang ancaman siber, latihan bersama, dan upaya untuk mengembangkan kerangka kerja regional yang efektif.
    b) Peran dalam Organisasi dan Forum Regional: Anda dapat menjelaskan peran Indonesia dalam organisasi dan forum regional seperti ASEAN Regional Forum (ARF) atau Konferensi Tingkat Tinggi Asia-Pasifik (APEC) yang berkaitan dengan keamanan siber.

b. Peran ASEAN dalam Mengatasi Hambatan Implementasi TAC

1. Peran Sekretariat ASEAN dalam Mendukung Implementasi TAC:

    Sekretariat ASEAN memiliki peran yang penting dalam mendukung implementasi TAC terkait keamanan siber:
    a) **Koordinasi dan Pemantauan:** Sekretariat ASEAN dapat berperan dalam mengkoordinasikan upaya antarnegara ASEAN dalam mengatasi ancaman keamanan siber. Mereka mungkin menyelenggarakan pertemuan dan dialog antarnegara untuk membahas isu-isu keamanan siber terkait TAC.

b) **Pendukung Teknis:** Sekretariat ASEAN mungkin juga memberikan dukungan teknis, seperti pelatihan dan bantuan teknis, kepada negara-negara anggota ASEAN dalam memperkuat kapasitas mereka dalam mengatasi ancaman cyber crime.

c) **Pelaporan dan Pengawasan:** Sekretariat ASEAN dapat membantu dalam pelaporan dan pengawasan implementasi TAC terkait keamanan siber. Mereka mungkin mengumpulkan data dan informasi tentang insiden siber di kawasan dan membantu negara-negara anggota dalam mengidentifikasi tren dan ancaman.

2. Inisiatif dan Program ASEAN dalam Mengatasi Cyber Crime:

   ASEAN telah meluncurkan sejumlah inisiatif dan program untuk mengatasi ancaman cyber crime:

   a) **Pengembangan Kerangka Kerja Keamanan Siber ASEAN:** ASEAN mungkin telah mengembangkan kerangka kerja keamanan siber regional yang memberikan pedoman bagi negara-negara anggota dalam menghadapi ancaman siber. Kerangka kerja ini dapat mencakup prinsip-prinsip, standar, dan panduan terkait keamanan siber.

   b) **Latihan Bersama:** ASEAN mungkin juga menyelenggarakan latihan bersama dan simulasi serangan siber untuk meningkatkan kapasitas negara-negara anggota dalam merespons insiden siber dengan cepat dan efektif.

   c) **Kampanye Kesadaran Masyarakat:** ASEAN mungkin juga meluncurkan kampanye kesadaran masyarakat tentang keamanan

siber, baik untuk masyarakat umum maupun sektor bisnis. Hal ini bertujuan untuk meningkatkan pemahaman tentang risiko cyber crime dan cara melindungi diri.

3. Kerja Sama ASEAN dengan Mitra Eksternal terkait Keamanan Siber**:**

   ASEAN sering bekerja sama dengan mitra eksternal, seperti negara-negara di luar kawasan dan organisasi internasional, dalam upaya mengatasi hambatan implementasi TAC terkait keamanan siber:

   a) **Kerja Sama dengan Mitra Dialog ASEAN:** ASEAN mungkin telah menjalin kemitraan strategis dengan negara-negara mitra dialog ASEAN dalam bidang keamanan siber. Ini bisa mencakup pertukaran informasi, pelatihan bersama, dan proyek-proyek kolaboratif terkait keamanan siber.

   b) **Kerja Sama dengan Organisasi Internasional:** ASEAN juga bisa bekerja sama dengan organisasi internasional seperti Perserikatan Bangsa-Bangsa (PBB) atau Interpol dalam mengatasi ancaman cyber crime yang bersifat global. Hal ini dapat mencakup koordinasi dalam penegakan hukum internasional terkait cyber crime.

Dengan peran aktif yang dimainkan oleh ASEAN melalui Sekretariatnya dan melalui kerja sama dengan mitra eksternal, upaya untuk mengatasi hambatan implementasi TAC terhadap keamanan siber menjadi lebih efektif dan komprehensif. Ini juga membantu meningkatkan stabilitas regional di kawasan Asia Tenggara dalam menghadapi ancaman cyber crime yang semakin kompleks.

c. Hambatan-Hambatan dalam Implementasi TAC terhadap Cyber Crime:

Pemahaman tentang hambatan-hambatan dalam implementasi TAC terhadap cyber crime krusial untuk mengatasi tantangan yang semakin kompleks dalam keamanan siber. Hambatan ini dapat dibagi menjadi faktor internal dan faktor eksternal:

1. Faktor Internal dalam Implementasi TAC:

a) **Kendala Hukum dan Regulasi:**

Hambatan internal pertama adalah kendala hukum dan regulasi di tingkat nasional. Negara-negara anggota ASEAN mungkin memiliki kerangka hukum yang tidak memadai atau belum cukup kuat dalam mengatasi cyber crime. Ini termasuk ketidakjelasan dalam definisi cyber crime, hukuman yang tidak sebanding, dan prosedur hukum yang tidak efisien. Oleh karena itu, negara-negara perlu memperbarui dan memperkuat kerangka hukum mereka untuk memastikan bahwa pelaku cyber crime dapat diidentifikasi dan dihukum dengan tegas.

b) **Keterbatasan Sumber Daya:**

Keterbatasan sumber daya adalah hambatan internal lainnya dalam implementasi TAC terhadap cyber crime. Ini mencakup keterbatasan anggaran yang dialokasikan untuk keamanan siber, kekurangan personel yang terlatih dalam penanganan insiden siber, dan keterbatasan teknologi yang digunakan untuk melindungi infrastruktur penting. Negara-negara anggota perlu mengalokasikan

sumber daya yang memadai dan mengembangkan kapasitas teknis untuk menghadapi ancaman keamanan siber yang semakin canggih.

c) **Koordinasi Antarlembaga:**

Koordinasi antarlembaga di tingkat nasional juga merupakan hambatan dalam implementasi TAC terhadap cyber crime. Banyak negara anggota ASEAN memiliki lembaga-lembaga yang berbeda yang bertanggung jawab atas keamanan siber, seperti kepolisian, militer, dan lembaga-lembaga pemerintah lainnya. Koordinasi antara lembaga-lembaga ini mungkin kurang efektif, yang dapat menghambat respons yang cepat dan efisien terhadap insiden siber. Maka, penting untuk meningkatkan koordinasi antarlembaga ini dan memastikan bahwa mereka dapat bekerja sama dengan baik dalam menghadapi ancaman cyber crime.

2. Faktor Eksternal dalam Implementasi TAC:

a) Ancaman dari Aktor Non-Negara:

Ancaman dari aktor non-negara seperti kelompok peretas dan entitas ilegal merupakan hambatan eksternal dalam implementasi TAC terhadap cyber crime. Aktor-aktor ini seringkali sulit untuk diidentifikasi dan dihadapi, karena mereka dapat beroperasi di luar batasan yurisdiksi negara-negara anggota ASEAN. Upaya yang lebih besar diperlukan untuk melacak dan menindak aktor-aktor ini secara efektif.

b) **Kerja Sama Regional dan Internasional:**

Kerja sama regional dan internasional dalam mengatasi cyber crime adalah faktor penting dalam implementasi TAC. Namun, hambatan seperti perbedaan hukum, regulasi, dan prosedur di antara negara-negara anggota ASEAN dan mitra internasional dapat menghambat kerja sama yang efektif dalam penanggulangan cyber crime. Koordinasi yang lebih baik dan harmonisasi dalam regulasi dapat membantu mengatasi hambatan ini.

c) **Isu Keamanan Siber Global:**

Keamanan siber adalah isu global yang melibatkan banyak aktor, termasuk negara-negara besar dan organisasi internasional. Ancaman seperti serangan siber yang terkait dengan kepentingan nasional atau keamanan regional dapat menciptakan ketegangan di antara negara-negara anggota ASEAN dan negara-negara mitra. Mengatasi isu keamanan siber global memerlukan diplomasi yang cerdas dan kerja sama yang kuat di tingkat internasional.

Dengan pemahaman yang lebih dalam tentang hambatan-hambatan ini, negara-negara anggota ASEAN dapat mengambil langkah-langkah untuk mengatasi tantangan implementasi TAC terhadap cyber crime dan memperkuat kerja sama regional dalam melindungi keamanan siber kawasan.

3. Studi Kasus dan Analisis:

1. Kasus Implementasi TAC dalam Mengatasi Cyber Crime di Indonesia:

a) Kebijakan Nasional:

Pada tahun-tahun sebelum pengetatan peraturan di sekitar keamanan siber, kebijakan nasional Indonesia yang berkaitan dengan keamanan siber belum terlalu terintegrasi secara khusus dalam kerangka TAC (Tata Kelola Aset dan Keterbukaan Teknologi Informasi dan Komunikasi). Namun, perubahan signifikan telah terjadi dalam beberapa tahun terakhir dalam upaya meningkatkan keamanan siber di Indonesia.

Berikut adalah beberapa langkah dan perkembangan terkait dengan kebijakan keamanan siber di Indonesia yang dapat dihubungkan dengan kerangka TAC:

1) **Rencana Aksi Nasional Keamanan Siber (RAN Keamanan Siber):** Pemerintah Indonesia telah merumuskan RAN Keamanan Siber sebagai bagian dari upaya untuk mengatasi ancaman keamanan siber. RAN Keamanan Siber berisi langkah-langkah yang harus diambil dalam jangka pendek, menengah, dan panjang untuk memperkuat pertahanan siber Indonesia. Ini dapat dianggap sebagai bagian dari upaya TAC untuk mengelola aset dan teknologi informasi dan komunikasi yang lebih aman.
2) **Undang-Undang ITE (Informasi dan Transaksi Elektronik):** Meskipun bukan bagian eksplisit dari TAC, Undang-Undang ITE telah diubah dan diperketat untuk mengatasi masalah keamanan siber. Beberapa perubahan ini

termasuk penambahan pasal terkait dengan kejahatan siber, termasuk tindak pidana siber dan perlindungan data pribadi.

3) **Kebijakan Perlindungan Data Pribadi:** Pemerintah Indonesia juga telah mengeluarkan Peraturan Pemerintah No. 71 Tahun 2019 tentang Perlindungan Data Pribadi. Ini adalah bagian dari upaya untuk melindungi data pribadi warga negara Indonesia dari potensi pelanggaran keamanan siber.
4) **Peningkatan Kesadaran Keamanan Siber:** Pemerintah dan badan-badan terkait juga aktif dalam mengkampanyekan kesadaran keamanan siber di kalangan masyarakat, termasuk pelaku bisnis. Ini adalah langkah penting dalam mengimplementasikan aspek TAC yang berkaitan dengan keterbukaan teknologi informasi dan komunikasi dengan aman.

Meskipun TAC mungkin tidak secara eksplisit menyebutkan kebijakan keamanan siber, upaya-upaya ini mencerminkan langkah-langkah untuk memastikan bahwa aset dan teknologi informasi dan komunikasi yang digunakan di Indonesia dilindungi dengan baik dari ancaman siber. Hal ini penting dalam konteks global yang semakin terhubung di mana keamanan siber telah menjadi salah satu isu utama yang harus diatasi oleh setiap negara.

b) Kolaborasi Antarlembaga:

Kerja sama dan koordinasi antara lembaga pemerintah di Indonesia dalam mengatasi kejahatan siber, termasuk dalam konteks TAC (Tata Kelola Aset dan Keterbukaan Teknologi Informasi dan Komunikasi), merupakan bagian penting dari upaya untuk meningkatkan keamanan siber di negara ini. Berikut beberapa contoh inisiatif konkret yang telah diambil:

1) **Pembentukan Badan Siber Nasional (BSN):** Pemerintah Indonesia telah membentuk Badan Siber Nasional (BSN) sebagai lembaga yang bertanggung jawab untuk mengkoordinasikan dan mengintegrasikan upaya penanggulangan ancaman siber di seluruh lembaga pemerintah. BSN berperan sebagai pemimpin dalam upaya mengatasi kejahatan siber dan memastikan koordinasi yang efektif antara lembaga-lembaga yang terlibat.
2) Keterlibatan Kepolisian: Kepolisian Republik Indonesia (POLRI) memiliki divisi yang khusus menangani kejahatan siber, yaitu Direktorat Tindak Pidana Siber (Dittipidsiber). Mereka bekerja sama dengan BSN dan lembaga-lembaga lainnya dalam penyelidikan dan penanggulangan kasus kejahatan siber.
3) **Kerja Sama dengan Kementerian Terkait:** Sejumlah kementerian seperti Kementerian Komunikasi dan Informatika (Kemenkominfo), Kementerian Hukum dan Hak Asasi Manusia (Kemenkumham), serta Kementerian

Keuangan terlibat dalam upaya penanggulangan kejahatan siber dan perlindungan data pribadi. Mereka berkolaborasi dengan BSN dalam merumuskan kebijakan dan peraturan terkait keamanan siber.

4) **Sertifikasi Profesional Keamanan Siber**: Pemerintah Indonesia juga mendukung pengembangan profesionalisme di bidang keamanan siber melalui sertifikasi, seperti Certified Information Systems Security Professional (CISSP) dan Certified Information Security Manager (CISM). Ini adalah upaya untuk meningkatkan kapasitas personel yang bekerja dalam bidang keamanan siber di berbagai lembaga pemerintah.
5) **Kampanye Kesadaran Keamanan Siber:** Berbagai lembaga pemerintah juga bekerja sama dalam kampanye kesadaran keamanan siber untuk meningkatkan pemahaman masyarakat dan bisnis tentang risiko kejahatan siber dan cara melindungi diri mereka.

Semua inisiatif ini bertujuan untuk meningkatkan koordinasi antara lembaga-lembaga pemerintah dalam upaya bersama untuk mengatasi kejahatan siber. Ini juga merupakan bagian penting dari upaya untuk melindungi aset dan teknologi informasi dan komunikasi yang ada dalam kerangka TAC, dengan memastikan bahwa keterbukaan teknologi tersebut tetap aman dari ancaman siber.

c) Keterlibatan Swasta dan Masyarakat Sipil

Keterlibatan sektor swasta dan masyarakat sipil dalam upaya mengatasi kejahatan siber di Indonesia merupakan komponen penting dalam kerangka TAC (Tata Kelola Aset dan Keterbukaan Teknologi Informasi dan Komunikasi). Sejauh ini, pemerintah Indonesia telah berupaya melibatkan sektor swasta dan masyarakat sipil dalam berbagai cara, meskipun masih ada tantangan dalam mencapai tingkat keterlibatan yang optimal. Berikut adalah beberapa contoh keterlibatan tersebut:

1) **Kemitraan dengan Industri Teknologi:** Pemerintah Indonesia telah menjalin kemitraan dengan perusahaan teknologi besar dan organisasi industri untuk berbagi informasi tentang ancaman siber, serta untuk mengembangkan solusi keamanan. Beberapa perusahaan teknologi juga terlibat dalam inisiatif pendidikan dan pelatihan keamanan siber.
2) **Forum Diskusi Publik dan Seminar:** Pemerintah Indonesia sering mengadakan forum diskusi publik dan seminar yang melibatkan pemangku kepentingan dari sektor swasta dan masyarakat sipil untuk membahas isu-isu keamanan siber dan solusi yang mungkin.
3) **Kampanye Kesadaran Keamanan Siber:** Keterlibatan masyarakat sipil dalam kampanye kesadaran keamanan siber adalah salah satu komponen utama dalam upaya pemerintah

untuk melibatkan publik dalam melindungi diri dari ancaman siber. Berbagai kampanye tersebut mencakup penyuluhan dan pelatihan kepada masyarakat umum dan pelaku bisnis.

4) **Kemitraan dengan Perguruan Tinggi:** Pemerintah juga berkolaborasi dengan perguruan tinggi dan lembaga pendidikan untuk mengembangkan kurikulum dan program pelatihan di bidang keamanan siber. Hal ini bertujuan untuk menghasilkan tenaga kerja yang siap bekerja dalam bidang keamanan siber.

Meskipun telah ada upaya untuk melibatkan sektor swasta dan masyarakat sipil dalam upaya mengatasi kejahatan siber sesuai dengan TAC, masih ada beberapa tantangan yang perlu diatasi. Salah satu tantangan utama adalah koordinasi yang lebih baik antara sektor publik dan swasta serta masyarakat sipil, terutama dalam hal berbagi informasi tentang ancaman siber. Selain itu, perlu upaya lebih lanjut dalam mendorong perusahaan swasta untuk secara aktif mengadopsi praktik keamanan siber yang kuat.

Pemerintah juga harus terus mengembangkan regulasi dan kebijakan yang mendukung keterlibatan sektor swasta dan masyarakat sipil dalam upaya mengatasi kejahatan siber, serta meningkatkan kesadaran masyarakat tentang pentingnya keamanan siber dalam dunia digital yang semakin terhubung.

c. Pencapaian dan Tantangan:

Pencapaian dan tantangan dalam implementasi TAC (Tata Kelola Aset dan Keterbukaan Teknologi Informasi dan Komunikasi) terkait keamanan siber di Indonesia mencerminkan perkembangan yang telah dicapai sejauh ini dan juga masalah yang masih harus diatasi. Berikut adalah tinjauan singkat tentang hal ini:

- Pencapaian:
    1) **Pembentukan Badan Siber Nasional (BSN):** Pembentukan BSN adalah salah satu pencapaian signifikan dalam upaya meningkatkan keamanan siber di Indonesia. BSN bertindak sebagai lembaga koordinasi utama dalam menghadapi ancaman siber, memastikan kerjasama antara lembaga pemerintah, sektor swasta, dan masyarakat sipil.
    2) **Penyusunan Rencana Aksi Nasional Keamanan Siber (RAN Keamanan Siber):** Indonesia telah merumuskan RAN Keamanan Siber sebagai panduan untuk mengatasi ancaman siber. Ini mencakup langkah-langkah konkret yang harus diambil dalam jangka pendek, menengah, dan panjang untuk memperkuat pertahanan siber.
    3) **Peningkatan Kesadaran Keamanan Siber:** Pemerintah Indonesia telah aktif dalam kampanye kesadaran keamanan siber, termasuk pelatihan dan pendidikan kepada masyarakat umum dan pelaku bisnis tentang risiko dan praktik keamanan yang baik.
    4) **Regulasi dan Peraturan:** Pemerintah telah mengeluarkan peraturan dan undang-undang yang mengatur keamanan siber, termasuk

perubahan pada Undang-Undang ITE dan Peraturan Pemerintah tentang Perlindungan Data Pribadi.

- Tantangan:
    1) Koordinasi Antarlembaga: Meskipun BSN telah dibentuk untuk memfasilitasi koordinasi, masih ada tantangan dalam mengintegrasikan berbagai lembaga pemerintah yang terlibat dalam keamanan siber. Diperlukan upaya lebih lanjut untuk memastikan kolaborasi yang efektif antara mereka.
    2) Keterlibatan Swasta: Meskipun ada upaya untuk melibatkan sektor swasta dalam upaya keamanan siber, perusahaan seringkali masih kurang aktif dalam mengadopsi praktik keamanan yang kuat. Meningkatkan keterlibatan dan kesadaran di kalangan bisnis adalah tantangan yang masih perlu diatasi.
    3) Kekurangan Tenaga Kerja Terlatih: Masih ada kekurangan tenaga kerja terlatih di bidang keamanan siber di Indonesia. Diperlukan investasi dalam pelatihan dan pendidikan untuk menghasilkan lebih banyak profesional keamanan siber yang kompeten.
    4) Tantangan Hukum dan Etika: Penyusunan regulasi terkait keamanan siber dan perlindungan data pribadi masih menghadapi tantangan, terutama dalam konteks perlindungan privasi sambil memastikan keamanan. Selain itu, etika dalam penggunaan teknologi dan pengumpulan data juga menjadi isu yang harus diatasi.

Pemerintah Indonesia telah membuat kemajuan yang signifikan dalam mengatasi tantangan keamanan siber dengan pembentukan lembaga seperti BSN

dan pembuatan RAN Keamanan Siber. Namun, upaya lebih lanjut diperlukan untuk memperkuat kerjasama antarlembaga, mendorong sektor swasta untuk mengambil peran lebih aktif, dan mengatasi kekurangan tenaga kerja terlatih. Selain itu, regulasi dan etika terkait dengan keamanan siber perlu terus diperbarui dan disempurnakan sesuai dengan perkembangan teknologi dan ancaman siber yang terus berkembang.

2. Kasus-Kasus Implementasi TAC dalam Mengatasi Cyber Crime di Negara-Negara ASEAN Lainnya:

a. Perbedaan Pendekatan:

1) Pendekatan masing-masing negara anggota ASEAN (Asosiasi Negara-Negara Asia Tenggara) terhadap TAC (Tata Kelola Aset dan Keterbukaan Teknologi Informasi dan Komunikasi) dalam mengatasi kejahatan siber dapat berbeda berdasarkan perbedaan dalam regulasi, kapasitas, dan prioritas nasional. Di bawah ini adalah beberapa contoh perbedaan pendekatan negara-negara anggota ASEAN terhadap keamanan siber:

- Singapura: Singapura dikenal sebagai pemimpin dalam mengadopsi teknologi dan memiliki regulasi yang kuat terkait keamanan siber. Negara ini aktif dalam berbagi informasi tentang ancaman siber dan berkolaborasi dengan sektor swasta untuk melindungi infrastruktur kritis. Singapura juga memprioritaskan pelatihan dan pengembangan tenaga kerja keamanan siber.
- Indonesia: Indonesia adalah negara dengan populasi terbesar di ASEAN, dan upaya untuk mengatasi kejahatan siber di sini

mencerminkan tantangan yang unik. Pemerintah Indonesia telah membentuk Badan Siber Nasional (BSN) dan mengeluarkan Rencana Aksi Nasional Keamanan Siber (RAN Keamanan Siber) sebagai panduan untuk mengatasi ancaman siber. Selain itu, regulasi yang mengatur keamanan siber telah diperketat, termasuk perubahan pada Undang-Undang ITE.

- Malaysia: Malaysia memiliki kerangka hukum yang kuat untuk mengatasi kejahatan siber, termasuk Akta Kejahatan Siber. Pemerintah Malaysia juga aktif dalam mempromosikan kesadaran keamanan siber melalui kampanye dan pelatihan.
- Thailand: Thailand telah meningkatkan upayanya dalam mengatasi ancaman siber dengan pembentukan National Cybersecurity Agency (NCA) untuk mengkoordinasikan kebijakan dan tindakan terkait keamanan siber. Mereka juga telah merancang undang-undang baru yang akan mengatur keamanan siber lebih rinci.
- Vietnam: Vietnam telah menunjukkan komitmen untuk meningkatkan keamanan siber dengan pembentukan National Cybersecurity Committee dan regulasi yang mengatur perlindungan data pribadi. Mereka juga aktif dalam menghadapi serangan siber yang datang dari luar negeri.
- Brunei Darussalam: Brunei memiliki kerangka hukum yang mengatur kejahatan siber dan perlindungan data pribadi. Mereka juga aktif dalam meningkatkan kesadaran keamanan siber di kalangan masyarakat.

Pendekatan masing-masing negara anggota ASEAN mencerminkan perbedaan dalam tingkat kesiapan, respon terhadap ancaman yang dihadapi, dan prioritas nasional. Meskipun ada upaya untuk meningkatkan kerjasama regional dalam mengatasi kejahatan siber melalui ASEAN, perbedaan ini tetap ada dan menggambarkan kompleksitas tantangan yang dihadapi dalam mengelola keamanan siber di kawasan tersebut.

b. Perbandingan Kebijakan:

Perbandingan kebijakan nasional terkait dengan TAC (Tata Kelola Aset dan Keterbukaan Teknologi Informasi dan Komunikasi) dan keamanan siber di negara-negara ASEAN (Asosiasi Negara-Negara Asia Tenggara) menunjukkan berbagai kesamaan dan perbedaan dalam pendekatan mereka. Di bawah ini adalah perbandingan kebijakan nasional terkait TAC dan keamanan siber di beberapa negara ASEAN:

1) Singapura:
   - Kesamaan: Singapura dan negara-negara ASEAN lainnya umumnya memiliki kesamaan dalam mengakui pentingnya keamanan siber dan mengadopsi regulasi yang memadai untuk melindungi infrastruktur kritis dan data pribadi.
   - Perbedaan: Singapura mungkin lebih maju dalam aspek teknologi dan keamanan siber dibandingkan dengan beberapa negara ASEAN lainnya. Mereka telah membangun kerangka kerja yang kuat untuk mengelola aset teknologi dan komunikasi serta melindungi keamanan siber.

2) Indonesia:

- Kesamaan: Indonesia juga mengakui pentingnya keamanan siber dan telah memperkuat regulasi, seperti perubahan pada Undang-Undang ITE dan pembentukan Badan Siber Nasional (BSN) sebagai bagian dari RAN Keamanan Siber.
- Perbedaan: Dengan populasi yang besar dan keragaman geografis yang luas, tantangan keamanan siber di Indonesia mungkin lebih rumit. Upaya untuk melibatkan sektor swasta dan masyarakat sipil juga merupakan perbedaan signifikan dalam pendekatan mereka.

3) Malaysia:
   - Kesamaan: Malaysia memiliki kerangka hukum yang kuat untuk mengatasi kejahatan siber, termasuk Akta Kejahatan Siber. Mereka juga aktif dalam meningkatkan kesadaran keamanan siber.
   - Perbedaan: Seperti Singapura, Malaysia juga terkenal dengan kecanggihannya dalam teknologi dan keamanan siber.
4) Thailand:
   - Kesamaan: Thailand juga telah meningkatkan upayanya dalam mengatasi ancaman siber dengan pembentukan National Cybersecurity Agency (NCA) dan kerangka hukum yang mengatur keamanan siber.
   - Perbedaan: Thailand mungkin memiliki tantangan yang unik dalam menghadapi ancaman siber yang berasal dari luar negeri.

5) Filipina:

- Kesamaan: Filipina telah mengadopsi undang-undang Cybercrime Prevention Act untuk mengatasi kejahatan siber.
- Perbedaan: Filipina aktif dalam kerjasama regional dalam pertukaran informasi tentang ancaman siber.

6) Vietnam:

- Kesamaan: Vietnam memiliki National Cybersecurity Committee dan regulasi perlindungan data pribadi.
- Perbedaan: Vietnam juga menghadapi tantangan ancaman siber yang berasal dari luar negeri dan kerjasama dengan negara-negara tetangga dalam mengatasi hal ini.

7) Brunei Darussalam:

- Kesamaan: Brunei memiliki kerangka hukum yang mengatur kejahatan siber dan perlindungan data pribadi.
- Perbedaan: Mereka juga aktif dalam meningkatkan kesadaran keamanan siber di kalangan masyarakat.

Meskipun ada kesamaan dalam pengakuan pentingnya keamanan siber dan regulasi yang ada, perbedaan dalam tingkat kesiapan teknologi, keamanan siber, dan respon terhadap ancaman yang dihadapi menciptakan variasi dalam pendekatan masing-masing negara ASEAN. Upaya untuk meningkatkan kerjasama regional melalui ASEAN dapat membantu mengatasi perbedaan ini dan mempromosikan keamanan siber di seluruh kawasan.

c. Hasil Implementasi:

Tinjauan hasil dan dampak implementasi TAC (Tata Kelola Aset dan Keterbukaan Teknologi Informasi dan Komunikasi) terkait keamanan siber di negara-negara ASEAN menunjukkan berbagai prestasi dan pengalaman yang dapat dipelajari. Berikut adalah beberapa hasil dan dampak yang telah dicapai oleh negara-negara tersebut:

1) Peningkatan Kesadaran Keamanan Siber:
   - Dampak: Hampir semua negara ASEAN telah berhasil meningkatkan kesadaran keamanan siber di kalangan masyarakat dan pelaku bisnis. Kampanye kesadaran, pelatihan, dan pendidikan telah menjadi efektif dalam membantu orang memahami risiko dan praktik keamanan yang baik.
   - Pelajaran yang dapat dipelajari: Upaya untuk meningkatkan kesadaran adalah langkah awal yang penting dalam menghadapi ancaman siber. Negara-negara dapat mengambil contoh dari strategi kampanye kesadaran yang sukses.
2) Pembentukan Lembaga Khusus Keamanan Siber:
   - Dampak: Pembentukan lembaga seperti Badan Siber Nasional (BSN) di Indonesia, National Cybersecurity Committee di Vietnam, dan National Cybersecurity Agency (NCA) di Thailand telah membantu mengkoordinasikan dan memperkuat upaya keamanan siber di tingkat nasional.
   - Pelajaran yang dapat dipelajari: Membentuk lembaga khusus untuk mengurus keamanan siber dapat meningkatkan koordinasi antarlembaga dan pengelolaan ancaman siber secara efisien.

3) Peningkatan Regulasi dan Kebijakan:
   - Dampak: Banyak negara ASEAN telah mengeluarkan atau memperbarui regulasi dan undang-undang yang mengatur keamanan siber, termasuk perlindungan data pribadi. Hal ini menciptakan kerangka kerja hukum yang lebih kuat untuk melindungi aset teknologi dan data.
   - Pelajaran yang dapat dipelajari: Regulasi yang jelas dan kuat adalah kunci dalam melindungi keamanan siber. Negara-negara dapat mempertimbangkan untuk memperbarui dan memperkuat kerangka hukum mereka sesuai dengan perkembangan teknologi.

4) Keterlibatan Swasta dan Masyarakat Sipil:
   - Dampak: Upaya untuk melibatkan sektor swasta dan masyarakat sipil dalam melindungi keamanan siber telah menghasilkan kolaborasi yang bermanfaat dan lebih banyak sumber daya yang dapat digunakan dalam menghadapi ancaman siber.
   - Pelajaran yang dapat dipelajari: Keterlibatan sektor swasta dan masyarakat sipil adalah komponen penting dalam pengelolaan keamanan siber yang efektif. Negara-negara dapat mengupayakan kerjasama lebih erat dengan pihak-pihak ini.
5) Kolaborasi Regional:
   - Dampak: Negara-negara ASEAN telah meningkatkan kerjasama regional dalam mengatasi ancaman siber, termasuk pertukaran informasi dan peningkatan kapasitas.

- Pelajaran yang dapat dipelajari: Kerjasama regional adalah penting dalam menghadapi ancaman siber yang melintasi batas negara. Negara-negara dapat mengambil contoh dari upaya koordinasi regional dalam melindungi infrastruktur kritis dan data.

6) Pemberdayaan Tenaga Kerja Keamanan Siber:

- Dampak: Banyak negara ASEAN telah meluncurkan program pelatihan dan sertifikasi untuk meningkatkan keterampilan tenaga kerja keamanan siber.
- Pelajaran yang dapat dipelajari: Investasi dalam pendidikan dan pelatihan tenaga kerja keamanan siber penting untuk membangun kapasitas dalam mengatasi ancaman siber.

Sementara ada kemajuan yang signifikan dalam melindungi keamanan siber di negara-negara ASEAN, masih ada banyak tantangan yang perlu diatasi, termasuk koordinasi yang lebih baik antarlembaga, peningkatan peran sektor swasta, dan perbaruan regulasi yang sesuai dengan perkembangan teknologi. Pengalaman dari negara-negara ASEAN dapat menjadi sumber inspirasi bagi negara-negara lain yang ingin meningkatkan keamanan siber mereka dalam era digital yang semakin terhubung.

BAB IV

KESIMPULAN DAN SARAN

A. Kesimpulan

Dalam penelitian ini, telah diselidiki dan dianalisis implementasi Perjanjian Persahabatan dan Kerjasama (TAC) Indonesia dan ASEAN dalam mengatasi kejahatan siber. Temuan utama dari penelitian ini adalah sebagai berikut:

1. Pentingnya Keamanan Siber di ASEAN: Keamanan siber telah menjadi isu yang semakin penting di kawasan ASEAN dan secara global. Ancaman-ancaman seperti serangan siber, pencurian data, dan disinformasi memiliki potensi yang serius untuk mengganggu stabilitas regional dan keamanan nasional.
2. Peran Indonesia dalam TAC: Indonesia memiliki peran penting dalam mempromosikan implementasi TAC dalam mengatasi kejahatan siber di kawasan ASEAN. Pemerintah Indonesia telah mengambil berbagai inisiatif dalam mengatasi ancaman keamanan siber, termasuk pembentukan kebijakan nasional dan kerja sama dengan sektor swasta.
3. Kerja Sama Regional: Kerja sama regional melalui ASEAN adalah kunci dalam mengatasi tantangan keamanan siber di kawasan ini. TAC menjadi kerangka kerja yang relevan dalam memfasilitasi kerja sama ini, dengan menciptakan landasan hukum untuk upaya bersama dalam melindungi infrastruktur siber dan mengatasi insiden siber.
4. Tantangan dalam Implementasi: Namun, terdapat sejumlah tantangan dalam implementasi TAC terkait keamanan siber, baik pada tingkat nasional

maupun regional. Tantangan tersebut meliputi keterbatasan sumber daya, kendala hukum, dan koordinasi antarlembaga di beberapa negara anggota ASEAN.

B. Saran

Berdasarkan temuan-temuan di atas, ada beberapa rekomendasi untuk perbaikan dan tindakan lanjutan dalam upaya mengatasi kejahatan siber melalui implementasi TAC:

1. Penguatan Kerangka Hukum Nasional: Negara-negara anggota ASEAN, termasuk Indonesia, harus terus memperkuat kerangka hukum nasional yang relevan dengan keamanan siber. Ini mencakup pengembangan regulasi yang lebih spesifik, sanksi yang lebih tegas, dan prosedur hukum yang lebih efisien dalam menangani kasus kejahatan siber.
2. investasi dalam Kapasitas Teknis: Negara-negara anggota ASEAN perlu mengalokasikan lebih banyak sumber daya untuk meningkatkan kapasitas teknis dalam mengatasi kejahatan siber. Ini termasuk pelatihan lebih lanjut untuk personel penegak hukum dan pengembangan teknologi keamanan siber yang lebih canggih
3. Koordinasi Antarlembaga: Peningkatan koordinasi antarlembaga di tingkat nasional adalah kunci untuk respons yang lebih cepat dan efektif terhadap insiden siber. Negara-negara anggota ASEAN harus memastikan bahwa lembaga-lembaga terkait dapat bekerja sama dengan baik dalam mengatasi kejahatan siber.
4. Perluasan Kerja Sama Regional: ASEAN harus terus memperluas kerja sama regional dalam mengatasi kejahatan siber. Hal ini mencakup

pertukaran informasi yang lebih aktif tentang ancaman siber, pelatihan bersama, dan pengembangan kerangka kerja regional yang lebih solid untuk keamanan siber.

5. Sensibilisasi dan Pendidikan Masyarakat: Meningkatkan kesadaran masyarakat tentang risiko kejahatan siber dan cara melindungi diri adalah langkah penting. Kampanye kesadaran publik harus ditingkatkan di seluruh kawasan ASEAN

DAFTAR PUSTAKA

A. Buku

Lee, T. B., & Lim, M. (Eds.). (2017). The ASEAN way and non-interference: A national interest test? World Scientific.

Diposkan, D. I. (2016). Cybersecurity in ASEAN and East Asia: Policies, challenges, and recommendations. Institute of Southeast Asian Studies.

Kim-Kwong, S. (Ed.). (2017). Cybersecurity in ASEAN: An overview and practical guide. World Scientific.

Koh, T. C., & Umar, M. U. (2014). ASEAN and the problem of common action. Institute of Southeast Asian Studies.

Graham, J. H. (2015). The ASEAN Regional Forum. Routledge.

Ida Hanifah, dkk,. 2018. Pedoman Tugas Akhir Mahasiswa Fakultas HukumUMSU. Medan: Pustaka Prima

Ida Hanifah, dkk,. 2018. Pedoman Tugas Akhir Mahasiswa Fakultas HukumUMSU. Medan: Pustaka Prima

Mukti Fajar dan Yulianto Achmad. 2017. Dualisme Penelitian Hukum Normatif danEmpiris. Yogyakarta: Pustaka Pelajar

Warren, C. (2018). Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats. Academic Press.

Nunn, A., & Qasmi, S. M. (Eds.). (2018). Cybersecurity in ASEAN and East Asia: Policies, Challenges, and Recommendations. Institute of Southeast Asian Studies.

Leong, A. B. H. (2016). Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait. Springer.

Niniek Suparni, SH. MH, (2009) *Cyberspace : Problematika & Antisipasi Pengaturannya.* Aceh : Sinar Grafika

B. Jurnal

Lee, S. (2018). "Cybersecurity challenges in ASEAN: Trend, threat, and policy." International Journal of Cyber Warfare and Terrorism (IJCWT), 8(1), 30-46.

Husin, S., & Heng, Y. K. (2017). "The role of ASEAN in cyber security." Asian Journal of Political Science, 25(1), 1-16.

Tung, C. H. (2019). "ASEAN Cybersecurity Cooperation: Progress and Challenges." Asian Security, 15(4), 288-304.

Acharya, A., & Ajo, A. (2018). "ASEAN Cybersecurity Initiatives: A Critical Assessment." RSIS Commentary, (62).

Soh, C., & Surbakti, R. E. (2016). "Cybersecurity and regionalism in Southeast Asia: Beyond securitisation and regionalisation." The Pacific Review, 29(3), 413-429.

Grabosky, P., Smith, R. G., & Dempsey, G. (2018). "Cybercrime: Key issues and debates." Annual Review of Criminology, 1, 171-192.

Holt, T. J., & Bossler, A. M. (2016). "The cybercrime handbook." Routledge International Handbooks. Routledge.

Wall, D. S. (2018). "Cybercrime, media, and insecurity: The shaping of public perceptions of cybercrime." International Journal of Cyber Criminology, 12(1), 7-23.

Holt, T. J., & Bossler, A. M. (2019). "The cybercrime landscape: Cross-national comparisons of hacking techniques and malware types." International Journal of Cyber Criminology, 13(1), 1-17.

C. Internet

https://www.interpol.int/en/Crimes/Cybercrime

https://krebsonsecurity.com/

https://www.cybercrimejournal.com/