

Peran Interpol dalam Menangani dan Menanggulangi Kejahatan Siber di Indonesia

Jansen Chandra¹, Vincent Tanaka², Ricky Banke³

^{1,2,3}Program Studi Hukum, Fakultas Hukum, Universitas Pelita Harapan Kampus Medan, Indonesia

E-mail: 03051220007@student.uph.edu¹, 03051220024@student.uph.edu², ricky.banke@uph.edu³

Article History:

Received: 01 April 2025

Revised: 15 April 2025

Accepted: 17 April 2025

Keywords: *Interpol, Kejahatan Siber Indonesia, Menanggulangi Kejahatan Siber, Pencegahan Kejahatan Siber, Penegakan Hukum Siber.*

Abstract: *Kejahatan siber merupakan ancaman global yang terus berkembang seiring dengan kemajuan teknologi digital. Sebagai organisasi penegak hukum internasional, Interpol memainkan peran penting dalam menangani dan menanggulangi kejahatan siber, termasuk di Indonesia. Penelitian ini bertujuan untuk menganalisis peran Interpol dalam menghadapi kejahatan siber di tingkat internasional serta bagaimana upaya Interpol membantu Indonesia menangani dan menanggulangi kejahatan siber. Penelitian ini menggunakan metode normatif yang berfokus pada analisis kebijakan dan menggunakan desain deskriptif-analitis, mengkaji struktur, strategi, serta kerja sama lembaga penegak hukum nasional dengan Interpol/aktor global lainnya. Hasil penelitian menunjukkan bahwa Interpol berperan dalam meningkatkan sistem deteksi dini, memperkuat kerja sama internasional, serta memberikan pelatihan bagi aparat penegak hukum di Indonesia. Selain itu, strategi Interpol dalam menanggulangi kejahatan siber mencakup pencegahan berupa edukasi digital, investigasi kejahatan lintas batas, serta pengembangan teknologi, dan database global. Meskipun demikian, masih terdapat tantangan berupa keterbatasan yurisdiksi, kompleksitas ancaman siber, serta kebutuhan akan regulasi yang lebih adaptif. Oleh karena itu, diperlukan peningkatan koordinasi dan inovasi teknologi dalam upaya pemberantasan kejahatan siber di masa depan.*

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk komunikasi, ekonomi, dan pemerintahan. Namun, kemajuan ini juga disertai dengan meningkatnya ancaman kejahatan siber (*cybercrime*). Kejahatan siber mencakup berbagai bentuk aktivitas ilegal yang dilakukan melalui internet atau perangkat digital, seperti peretasan (*hacking*), pencurian data, penipuan online, serangan *ransomware*, serta tindakan kriminal yang berkaitan dengan terorisme dan perdagangan ilegal.

Kejahatan siber dalam skala internasional menjadi semakin kompleks karena sifatnya yang

lintas batas negara (*transnational crime*). Pelaku dapat beroperasi dari satu negara dan menyerang sistem di negara lain tanpa harus hadir secara fisik. Hal ini menciptakan tantangan besar dalam sistem penegakan hukum, terutama karena perbedaan regulasi hukum siber di setiap negara serta kesulitan dalam menangkap dan mengadili pelaku.

Berbagai kasus kejahatan siber yang memiliki dampak global, seperti serangan *ransomware WannaCry* pada tahun 2017 dan peretasan data Equifax, menunjukkan betapa seriusnya ancaman ini. Oleh karena itu, diperlukan koordinasi dan kerja sama internasional untuk mengatasi masalah ini, salah satunya melalui peran Interpol sebagai organisasi penegak hukum global yang memfasilitasi kerja sama antarnegara dalam memerangi kejahatan lintas batas, termasuk kejahatan siber.

Penelitian ini berfokus pada kejahatan siber dalam skala internasional serta peran Interpol dalam menanggulangi ancaman tersebut. Adapun ruang lingkup pembahasan meliputi:

1. Konsep Kejahatan Siber - pembahasan ini mencakup pada klasifikasi dan definisi dari kejahatan siber, jenis kejahatan yang termasuk dalam kejahatan dunia maya. Serta membandingkan regulasi dengan negara negara lain.
2. Peran Interpol dalam Menangani Kejahatan Siber - pembahasan ini lebih mencakup pada peran interpol Indonesia dalam menangani kasus kejahatan siber, rekomendasi yang diberikan seperti Tindakan hukum atau kerja sama dengan pihak internasional sangat dibutuhkan karena kejahatan dunia maya merupakan salah satu produk dari *Blue Collar Crime*.
3. Statergi Interpol dalam Menanggulangi Kejahatan Siber - pembahasan ini juga membahas tentang bagaimana seharusnya peran interpol Indonesia dalam mencegah kejahatan siber ini muncul dan membahas strategi untuk kedepannya. Bukan hanya peran pemerintah, tetapi peran masyarakat juga dibutuhkan dalam pencegahan kejahatan siber.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode hukum normatif dengan fokus pada analisis terhadap peraturan perundang-undangan dan bahan hukum lainnya yang berkaitan dengan peran Interpol dalam menangani kejahatan transnasional. Subjek penelitian ini mencakup berbagai regulasi yang mengatur kerja sama internasional dalam bidang penegakan hukum, termasuk konvensi internasional, undang-undang nasional, serta kebijakan yang relevan.

Penelitian ini menggunakan desain deskriptif-analitis, yang bertujuan untuk menggambarkan aturan hukum yang berlaku serta menganalisis efektivitas penerapannya dalam praktik. Data dikumpulkan melalui studi kepustakaan (*library research*) dengan menelusuri berbagai bahan hukum. Bahan hukum primer meliputi konvensi internasional, undang-undang, dan peraturan yang mengatur peran Interpol. Selain itu, bahan hukum sekunder seperti buku, jurnal, dan artikel ilmiah digunakan untuk memberikan analisis lebih mendalam. Sementara itu, bahan hukum tersier seperti kamus hukum dan ensiklopedia digunakan untuk memperjelas konsep hukum yang mendukung penelitian ini.

Penelitian ini tidak terdapat prosedur intervensi karena penelitian bersifat normatif dan tidak melibatkan eksperimen atau perubahan terhadap subjek penelitian. Data yang telah dikumpulkan dianalisis dengan metode deskriptif-analitis, yaitu dengan menguraikan dan menginterpretasikan isi dari peraturan hukum yang berlaku serta membandingkan penerapannya dalam kasus-kasus terkait. Analisis ini bertujuan untuk memahami sejauh mana regulasi yang ada dapat mendukung efektivitas peran Interpol dalam menangani kejahatan transnasional.

HASIL DAN PEMBAHASAN

Konsep Kejahatan Siber dalam Hukum Internasional

Kejahatan siber telah menjadi ancaman global yang berkembang pesat seiring dengan kemajuan teknologi informasi dan komunikasi. Dalam menghadapi kejahatan ini, hukum internasional berperan penting dalam menetapkan definisi, klasifikasi, serta regulasi yang mengatur penanggulangannya.

1. Definisi dan Klasifikasi Kejahatan Siber

a. Definisi Kejahatan Siber

Kejahatan siber (*cybercrime*) adalah tindakan kriminal yang dilakukan dengan menggunakan teknologi digital atau internet sebagai sarana utama dalam meluncurkan kejahatan. Organisasi internasional seperti Interpol, United Nations Office on Drugs and Crime (UNODC), dan Council of Europe memiliki definisi masing-masing terkait kejahatan siber. Menurut *Konvensi Budapest* tentang Kejahatan Siber (2001), kejahatan siber didefinisikan sebagai: "Tindakan ilegal yang dilakukan dengan menggunakan sistem komputer atau jaringan komputer sebagai alat, target, atau tempat terjadinya kejahatan."

b. Klasifikasi Kejahatan Siber

Kejahatan terhadap sistem komputer dan jaringan merupakan ancaman serius dalam dunia digital yang dapat menyebabkan kerugian besar bagi individu maupun organisasi. Salah satu bentuk kejahatan ini adalah peretasan (*hacking*), yaitu akses ilegal ke dalam sistem komputer tanpa izin dengan tujuan mencuri data, mengubah informasi, atau merusak sistem. Selain itu, terdapat serangan DoS (*Denial of Service*) dan DDoS (*Distributed Denial of Service*), yaitu serangan yang membanjiri server dengan lalu lintas data berlebih sehingga sistem menjadi lumpuh dan tidak dapat diakses oleh pengguna yang sah. Kejahatan siber lainnya adalah penyebaran malware, seperti virus, trojan, spyware, ransomware, dan worms, yang merupakan program berbahaya yang dirancang untuk merusak, mencuri informasi, atau mengambil alih kendali suatu sistem komputer. Jenis kejahatan ini tidak hanya merugikan secara finansial, tetapi juga dapat mengancam keamanan data serta privasi pengguna.

Peretasan atau *hacking* adalah tindakan mengakses sistem komputer, jaringan, atau data secara ilegal tanpa izin dari pemiliknya. Tujuan dari peretasan dapat bervariasi, mulai dari sekadar eksplorasi teknologi hingga melakukan tindakan kriminal seperti pencurian data, sabotase sistem, atau spionase siber. Peretas atau hacker terbagi menjadi beberapa kategori seperti *White Hat Hackers*, *Black Hat Hackers*, dan *Grey Hat Hackers*. Dalam dunia keamanan siber, peretas atau hacker dikategorikan berdasarkan niat dan tujuan mereka dalam melakukan peretasan. *White Hat Hackers* adalah peretas etis yang bekerja secara legal untuk meningkatkan keamanan sistem. Mereka biasanya dipekerjakan oleh perusahaan atau lembaga pemerintah untuk mengidentifikasi celah keamanan dan membantu memperbaikinya sebelum dapat dieksploitasi oleh pihak jahat. Dengan melakukan penetration testing atau simulasi serangan, mereka memastikan sistem tetap aman dan terlindungi. Aktivitas mereka dilakukan dengan izin pemilik sistem serta mengikuti hukum dan kode etik keamanan siber.

Berbeda dengan *White Hat*, *Black Hat Hackers* adalah peretas yang melakukan aktivitas ilegal dengan tujuan mengeksploitasi sistem untuk keuntungan pribadi atau merusak suatu entitas. Mereka sering kali mencuri data, menyebarkan malware, atau

melumpuhkan sistem tanpa izin dari pemiliknya. Teknik yang mereka gunakan beragam, seperti phishing, malware injection, dan serangan ransomware. Serangan mereka sering kali menyebabkan kerugian besar bagi individu maupun perusahaan, baik secara finansial maupun dalam bentuk kebocoran data penting.

Selain dari *White Hat* dan *Black Hat* terdapat *Grey Hat Hackers*, yang berada di zona abu-abu karena mereka mengakses sistem tanpa izin, tetapi tidak selalu untuk tujuan jahat. Mereka sering menemukan celah keamanan dan melaporkannya kepada pemilik sistem, tetapi dalam beberapa kasus, mereka juga meminta imbalan sebagai kompensasi atas informasi tersebut. Meskipun tindakan mereka tidak selalu merusak, tetap saja mereka melanggar hukum karena masuk ke dalam sistem tanpa izin. Dalam beberapa kasus, *Grey Hat Hackers* bisa menjadi ancaman jika mereka memilih mengeksploitasi celah yang ditemukan demi keuntungan pribadi.

Serangan *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS) adalah bentuk serangan siber yang bertujuan untuk membuat suatu layanan atau sistem tidak dapat diakses oleh pengguna sah dengan cara membanjiri server dengan lalu lintas data yang sangat besar (Mirkovic & Reiher, 2004). Serangan DoS dilakukan oleh satu sumber yang mengirimkan permintaan berlebihan ke server target sehingga server tidak mampu menangani beban tersebut dan akhirnya berhenti merespons (Stallings, 2020). Serangan ini sering kali dilakukan dengan memanfaatkan celah pada protokol komunikasi jaringan atau menggunakan perangkat lunak otomatis untuk mengirimkan paket data dalam jumlah besar dalam waktu singkat.

Serangan DDoS merupakan versi yang lebih kompleks dan berbahaya karena melibatkan banyak sumber serangan yang tersebar di berbagai lokasi. Penyerang biasanya menggunakan botnet, yaitu jaringan komputer yang telah dikompromikan dan dikendalikan secara remote untuk mengirimkan lalu lintas data dalam jumlah besar ke satu target secara bersamaan (Ullrich, 2017). Karena berasal dari berbagai sumber, serangan DDoS jauh lebih sulit untuk dihentikan dibandingkan DoS biasa. Serangan ini sering kali menargetkan situs web perusahaan besar, layanan perbankan, dan infrastruktur kritis seperti sistem pemerintahan atau jaringan telekomunikasi (Kaspersky Lab, 2021). Dampaknya bisa sangat merugikan, mulai dari gangguan layanan hingga kerugian finansial yang besar akibat sistem yang lumpuh dalam waktu lama.

2. Dampak Kejahatan Siber terhadap Indonesia

Dampak Kejahatan siber telah menjadi ancaman serius bagi ekonomi, keamanan nasional, dan stabilitas sosial di Indonesia. Dari segi ekonomi, serangan siber seperti ransomware dan pencurian data menyebabkan kerugian finansial yang besar. Contohnya, serangan ransomware WannaCry tahun 2017 menginfeksi banyak sistem di Indonesia, termasuk sektor kesehatan dan pemerintahan, yang mengakibatkan gangguan operasional dan kerugian finansial (Stallings, 2020). Selain itu, banyak perusahaan mengalami kebangkrutan akibat kebocoran data pelanggan, yang merusak kepercayaan publik terhadap layanan digital (BSSN, 2021).

Serangan terhadap infrastruktur strategis seperti listrik, telekomunikasi, dan layanan pemerintah semakin meningkat. Beberapa serangan siber yang menargetkan lembaga pemerintahan menunjukkan adanya indikasi espionase siber dari aktor luar negeri yang berusaha mencuri data strategis negara (Kementerian Komunikasi dan Informatika, 2022). Jika tidak ditangani dengan baik, serangan ini dapat mengganggu stabilitas nasional dan melemahkan sistem pertahanan negara.

Penyebaran hoaks dan propaganda digital jika dilihat dari sisi sosial dan politik, telah mempengaruhi opini publik, terutama dalam konteks politik. Misinformasi dan disinformasi yang tersebar melalui media sosial sering kali digunakan untuk memanipulasi pemilih dan menciptakan polarisasi di masyarakat (Nugroho & Putri, 2021). Selain itu, kasus kebocoran data pribadi, seperti yang terjadi pada penyedia layanan telekomunikasi di Indonesia, memperlihatkan bahwa privasi digital masih rentan dan membutuhkan regulasi lebih ketat (CNN Indonesia, 2022).

3. Perbandingan Regulasi Kejahatan Siber di Berbagai Negara

Setiap negara memiliki regulasi yang berbeda dalam menangani kejahatan siber. Namun, ada beberapa instrumen hukum internasional yang menjadi acuan utama:

a. Konvensi Budapest (2001)

Konvensi Budapest, yang juga dikenal sebagai Convention on Cybercrime, adalah perjanjian internasional pertama yang secara khusus mengatur tentang kejahatan siber. Konvensi ini diadopsi oleh Dewan Eropa pada 23 November 2001 dan mulai berlaku pada 1 Juli 2004. Konvensi ini bertujuan untuk menstandarisasi hukum pidana terkait kejahatan siber, memperkuat kerja sama antarnegara, serta menyediakan mekanisme ekstradisi dan pertukaran informasi guna menghadapi ancaman global di dunia digital (Council of Europe, 2001).

Salah satu aspek penting dari Konvensi Budapest adalah kriminalisasi aktivitas ilegal di dunia maya. Beberapa bentuk kejahatan siber yang diatur dalam konvensi ini meliputi akses ilegal ke sistem komputer (hacking), penyebaran malware, penipuan komputer, pemalsuan dokumen elektronik, dan pelanggaran hak cipta digital. Selain itu, konvensi ini juga mengatur tentang tindakan hukum terhadap pornografi anak di internet, yang menjadi perhatian utama banyak negara. Dengan demikian, konvensi ini menetapkan kerangka hukum yang jelas bagi negara-negara anggotanya dalam menangani kejahatan siber secara efektif. Selain aspek kriminalisasi, Konvensi Budapest juga menekankan pentingnya kerja sama internasional dalam menangani kejahatan siber, mengingat serangan siber sering kali melibatkan pelaku dari berbagai negara. Melalui konvensi ini, negara-negara anggota diwajibkan untuk menyediakan bantuan hukum timbal balik, berbagi informasi, serta bekerja sama dalam penyelidikan lintas batas. Hal ini penting karena kejahatan siber tidak mengenal batas wilayah dan membutuhkan koordinasi global untuk memberantasnya.

Regulasi ini telah diadopsi oleh 60 negara termasuk Amerika Serikat, Jepang, dan negara-negara Uni Eropa, beberapa negara seperti Rusia dan Tiongkok menolak untuk bergabung. Alasan utama penolakan ini adalah kekhawatiran terhadap kedaulatan nasional, di mana mereka merasa bahwa konvensi ini dapat digunakan oleh negara-negara Barat untuk melakukan intervensi dalam sistem hukum domestik mereka (Kerr, 2018). Selain itu, negara-negara yang menolak juga mengembangkan aturan dan kebijakan sendiri dalam menangani kejahatan siber, tanpa mengikuti standar internasional yang ditetapkan oleh Konvensi Budapest. Konvensi Budapest di Indonesia, menjadi acuan dalam pembentukan Undang-Undang Informasi dan Transaksi Elektronik (UU. ITE), meskipun Indonesia belum secara resmi meratifikasinya. Namun, dengan meningkatnya ancaman kejahatan siber, banyak pihak yang mendorong agar Indonesia bergabung dalam konvensi ini untuk memperkuat kerja sama internasional dalam pemberantasan kejahatan siber.

b. Regulasi di berbagai negara

Tabel 1. Regulasi di berbagai negara

Negara	Regulasi Kejahatan Siber	Fitur Utama
Amerika Serikat	Computer Fraud and Abuse Act (CFAA), Cybersecurity Information Sharing Act (CISA)	Mengatur penegakan hukum terhadap peretasan dan perlindungan infrastruktur kritis.
Uni Eropa	General Data Protection Regulation (GDPR), NIS Directive	Menekankan perlindungan data pribadi dan tanggung jawab perusahaan dalam menjaga keamanan data.
Tiongkok	Cybersecurity Law (2017)	Mengontrol penggunaan internet dan mewajibkan perusahaan untuk bekerja sama dengan pemerintah dalam investigasi kejahatan siber.
Indonesia	UU ITE (Undang-Undang Informasi dan Transaksi Elektronik)	Mengatur penghinaan online, pencemaran nama baik, serta transaksi digital dan perlindungan data.
Rusia	Sovereign Internet Law	Menerapkan kontrol ketat terhadap internet domestik dan membatasi akses informasi dari luar negeri.

Peran Interpol dalam Menangani Kejahatan Siber

Interpol Indonesia berperan penting dalam menangani kejahatan siber yang semakin kompleks dan berkembang pesat. Sebagai bagian dari jaringan global Interpol, Indonesia memiliki akses ke berbagai sumber daya internasional dalam menanggulangi ancaman kejahatan digital yang melintasi batas negara. Kejahatan siber seperti peretasan, pencurian data, penipuan online, hingga serangan ransomware menjadi ancaman serius terhadap individu, perusahaan, serta infrastruktur negara. Untuk menangani hal ini, Interpol Indonesia menerapkan berbagai strategi dan metode yang melibatkan kerja sama internasional, investigasi digital, penindakan hukum, serta penguatan regulasi dalam negeri.

Cara utama dalam menangani kejahatan siber adalah melalui kerja sama internasional. Kejahatan digital sering kali dilakukan oleh jaringan kriminal lintas negara, sehingga memerlukan koordinasi dengan otoritas penegak hukum internasional. Interpol Indonesia bekerja sama dengan Interpol Cybercrime Directorate dan Cyber Fusion Centre untuk bertukar informasi terkait modus operandi kejahatan siber. Dalam banyak kasus, Interpol Indonesia juga berkoordinasi dengan organisasi seperti *Association of Southeast Asian Chiefs of National Police* (ASEANAPOL) dan Europol untuk menangkap pelaku yang beroperasi di luar negeri.

Investigasi digital dan forensik siber menjadi bagian krusial dalam menangani kejahatan siber. Interpol Indonesia menggunakan teknologi forensik digital untuk menganalisis jejak elektronik pelaku, termasuk melacak alamat IP, transaksi keuangan mencurigakan, serta penyelidikan terhadap perangkat yang digunakan untuk kejahatan siber. Teknik ini sangat berguna dalam kasus seperti serangan ransomware, di mana pelaku sering kali menggunakan cryptocurrency untuk menyembunyikan identitasnya. Dengan teknik forensik siber, aparat hukum dapat menemukan titik lemah jaringan kriminal dan mengidentifikasi aktor utama di balik kejahatan tersebut.

Interpol Indonesia dalam operasi penangkapan dan penindakan, terlibat dalam berbagai operasi global yang bertujuan menindak jaringan kejahatan siber. Salah satu contoh adalah Operation Night Fury, yang berhasil menangkap beberapa tersangka yang terlibat dalam skema skimming kartu kredit dan pencurian data bank di Asia Tenggara. Operasi semacam ini dilakukan melalui investigasi mendalam dan kerja sama erat dengan otoritas setempat serta mitra internasional. Setelah tersangka ditangkap, mereka akan diproses secara hukum sesuai dengan peraturan yang berlaku di Indonesia atau diekstradisi ke negara yang memiliki yurisdiksi atas kasus tersebut.

Keamanan siber juga menjadi fokus utama Interpol Indonesia selain tindakan represif, Pencegahan dilakukan melalui edukasi kepada masyarakat tentang ancaman kejahatan siber dan cara melindungi diri dari serangan digital. Sosialisasi dilakukan melalui seminar, kampanye digital, serta kerja sama dengan lembaga pendidikan dan perusahaan teknologi. Selain itu, Interpol Indonesia bekerja sama dengan Badan Siber dan Sandi Negara (BSSN) untuk meningkatkan pertahanan siber nasional. Salah satu inisiatif yang dilakukan adalah penguatan sistem keamanan bagi infrastruktur vital seperti perbankan, layanan publik, serta institusi pemerintahan yang rentan terhadap serangan siber.

Pemantauan dan penguatan regulasi menjadi langkah strategis dalam mencegah meningkatnya kejahatan siber di Indonesia. Interpol Indonesia secara aktif mengawasi aktivitas mencurigakan di dunia maya, bekerja sama dengan penyedia layanan internet untuk mendeteksi serangan siber sebelum menimbulkan dampak yang lebih besar. Dari sisi regulasi, Interpol Indonesia juga mendukung pemerintah dalam memperkuat kebijakan dan peraturan terkait kejahatan siber, seperti melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta peraturan lain yang mendukung penegakan hukum di ranah digital.

Strategi Interpol dalam Menanggulangi Kejahatan Siber

1. Strategi Interpol Indonesia dalam Menanggulangi Kejahatan Siber

Interpol Indonesia berperan sebagai penghubung antara kepolisian nasional dengan komunitas internasional dalam menangani kejahatan siber. Sebagai bagian dari Interpol Global Cybercrime Programme, Indonesia aktif dalam berbagai operasi internasional untuk menangani ancaman siber lintas negara. Beberapa strategi utama yang dilakukan oleh Interpol Indonesia meliputi penegakan hukum, kerja sama internasional, peningkatan kapasitas aparat, serta kampanye edukasi bagi masyarakat. Salah satu pendekatan utama yang harus diterapkan adalah peningkatan kapabilitas dalam investigasi siber. Interpol Indonesia bekerja sama dengan Badan Reserse Kriminal (Bareskrim) Polri dan Badan Siber dan Sandi Negara (BSSN) dalam melakukan investigasi terhadap jaringan kejahatan siber yang beroperasi secara global. Melalui pusat kejahatan siber nasional, aparat penegak hukum dapat melakukan pemantauan terhadap aktivitas mencurigakan di dunia maya serta melacak pelaku yang terlibat dalam serangan siber atau penipuan daring.

Interpol Indonesia juga aktif dalam kerja sama internasional untuk menangani kejahatan siber lintas batas. Sebagai anggota Interpol, Indonesia berpartisipasi dalam operasi global seperti Operation Pangea untuk menindak perdagangan ilegal daring dan Operation Night Fury yang menargetkan jaringan kejahatan siber yang beroperasi di kawasan Asia. Kerja sama ini memungkinkan pertukaran informasi intelijen serta koordinasi dalam penindakan terhadap pelaku yang beroperasi di berbagai negara. Di tingkat domestik, Interpol Indonesia berfokus pada peningkatan kapasitas aparat penegak hukum dalam menangani kejahatan siber. Pelatihan secara berkala diberikan kepada penyidik Polri untuk meningkatkan pemahaman mereka mengenai teknik investigasi digital, analisis forensik siber, serta cara

menangani kasus pencurian data atau serangan siber terhadap infrastruktur penting. Dengan meningkatkan keterampilan teknis aparat, diharapkan penegakan hukum terhadap pelaku kejahatan siber dapat dilakukan dengan lebih efektif.

Strategi penanggulangan kejahatan siber tidak hanya mengandalkan pendekatan represif, tetapi juga melalui upaya pencegahan dengan meningkatkan kesadaran masyarakat. Interpol Indonesia bersama Kominfo dan BSSN secara aktif melakukan kampanye edukasi mengenai keamanan digital. Program seperti Gerakan Nasional Literasi Digital bertujuan untuk meningkatkan pemahaman masyarakat mengenai ancaman siber serta cara melindungi diri dari modus-modus kejahatan daring.

2. Peran Masyarakat dalam Pencegahan Kejahatan Siber

Selain upaya yang dilakukan oleh aparat penegak hukum, masyarakat juga memiliki peran penting dalam mencegah dan menangani kejahatan siber. Salah satu langkah yang dapat dilakukan adalah dengan meningkatkan literasi digital. Masyarakat perlu memahami berbagai bentuk kejahatan siber seperti phishing, penipuan daring, serta serangan malware agar dapat menghindari ancaman tersebut. Dengan memiliki pemahaman yang baik mengenai keamanan digital, individu dapat melindungi data pribadi mereka serta mengurangi risiko menjadi korban kejahatan siber. Selain itu, masyarakat dapat berkontribusi dalam pelaporan aktivitas mencurigakan di dunia maya. Platform seperti Patroli Siber yang dikelola oleh Polri dan Lapor.go.id memungkinkan masyarakat untuk melaporkan kasus kejahatan siber secara langsung. Dengan adanya laporan dari masyarakat, aparat penegak hukum dapat lebih cepat menindaklanjuti kasus serta mencegah dampak yang lebih luas dari tindakan kriminal yang dilakukan oleh pelaku.

Keterlibatan masyarakat dalam komunitas digital yang bertujuan untuk meningkatkan kesadaran akan keamanan siber juga dapat menjadi langkah efektif dalam menangkal ancaman siber. Misalnya, organisasi Relawan Keamanan Siber yang dibentuk oleh berbagai kelompok teknologi di Indonesia bertujuan untuk menyebarluaskan edukasi mengenai pentingnya perlindungan data dan privasi di dunia maya. Dengan adanya komunitas seperti ini, masyarakat dapat saling berbagi informasi dan pengalaman dalam menghadapi ancaman digital. Di lingkungan keluarga dan sekolah, orang tua serta pendidik juga memiliki peran dalam mengedukasi anak-anak mengenai keamanan siber. Mengingat anak-anak dan remaja merupakan kelompok yang rentan terhadap eksploitasi daring, penting bagi mereka untuk memahami bahaya berbagi informasi pribadi secara sembarangan di internet. Program seperti Sekolah Aman Digital telah diterapkan di beberapa sekolah di Indonesia untuk meningkatkan pemahaman siswa mengenai etika dan keamanan digital.

3. Perubahan untuk Mengatasi Kejahatan Siber

Interpol telah memainkan peran penting dalam menangani dan menanggulangi kejahatan siber, baik di tingkat global maupun nasional, termasuk di Indonesia. Dalam menjalankan fungsinya, Interpol tidak hanya bertindak ketika kejahatan telah terjadi, tetapi juga berperan aktif dalam langkah-langkah pencegahan yang bertujuan untuk mengantisipasi serangan siber sejak dini. Berbagai upaya telah dilakukan, mulai dari koordinasi operasi internasional, pendirian divisi khusus siber, pengelolaan sistem komunikasi antarnegara, hingga penyediaan pelatihan dan peningkatan kapasitas bagi aparat penegak hukum. Interpol secara konsisten bekerja sama dengan lembaga penegak hukum Indonesia, seperti Polri dan Badan Siber dan Sandi Negara (BSSN), untuk membangun kesiapan nasional dalam menghadapi ancaman dunia maya.

.....

Ditinjau dari sisi represif Interpol terlibat dalam kampanye kesadaran publik mengenai pentingnya keamanan digital, mendorong literasi digital masyarakat, serta menyediakan akses bagi Indonesia terhadap sistem deteksi dini berbasis intelijen global. Langkah-langkah ini diperkuat dengan kerja sama bersama sektor swasta, seperti Google, Microsoft, IBM, dan perusahaan forensik blockchain seperti Chainalysis, untuk memantau aktivitas mencurigakan di dunia maya dan menutup akses terhadap situs-situs ilegal. Selain itu, Interpol juga berkontribusi dalam meningkatkan kesiapan sumber daya manusia dengan menyelenggarakan pelatihan di bidang forensik digital, analisis malware, dan penyelidikan ransomware.

Pendekatan represif dilakukan melalui keterlibatan Interpol dalam investigasi kejahatan siber lintas negara, pelacakan transaksi ilegal yang menggunakan cryptocurrency, serta koordinasi operasi penangkapan internasional terhadap pelaku. Dalam banyak kasus, Interpol memfasilitasi kerja sama antarnegara melalui mekanisme Red Notice untuk menangkap tersangka kejahatan siber yang melarikan diri ke negara lain. Dalam konteks Indonesia, bentuk-bentuk kerja sama semacam ini sangat membantu ketika kejahatan siber yang berdampak domestik melibatkan pelaku yang beroperasi dari luar negeri atau melalui jaringan lintas batas.

Melihat tantangan kejahatan siber yang terus berkembang, Interpol merancang strategi masa depan yang lebih progresif dan adaptif. Strategi ini meliputi pengembangan kecerdasan buatan untuk analisis ancaman secara otomatis, integrasi sistem keamanan siber antarnegara, dan mendorong harmonisasi regulasi hukum siber di tingkat internasional. Interpol juga menaruh perhatian besar terhadap negara-negara berkembang, termasuk Indonesia, yang memerlukan dukungan dalam penguatan infrastruktur digital dan transformasi kebijakan keamanan siber nasional.

Menghadapi tantangan kedepan dibutuhkan perubahan dalam pola kerja Interpol dan negara anggotanya. Kerja sama internasional harus ditingkatkan, tidak hanya sebatas berbagi informasi, tetapi juga melalui kolaborasi strategis dalam operasi gabungan dan pertukaran teknologi. Di sisi lain, regulasi di tingkat nasional dan internasional juga harus diperbarui untuk mengakomodasi bentuk-bentuk baru kejahatan digital, seperti kejahatan berbasis kecerdasan buatan, pemalsuan deepfake, dan kejahatan dalam ekosistem blockchain. Negara-negara anggota Interpol juga harus memperkuat kapasitas lokal mereka dengan membentuk unit-unit respons cepat terhadap serangan siber, yang didukung oleh pelatihan berkelanjutan dan investasi pada sistem keamanan digital.

Peran Interpol dalam menanggulangi kejahatan siber terus berkembang dari waktu ke waktu. Melalui pendekatan yang mencakup aspek preventif dan represif, serta visi strategis untuk masa depan, Interpol diharapkan mampu menjadi garda terdepan dalam menciptakan keamanan digital global yang tangguh. Namun, kesuksesan dari upaya ini sangat bergantung pada komitmen bersama antarnegara dalam mewujudkan sistem penegakan hukum yang adaptif, kolaboratif, dan inovatif dalam menghadapi kejahatan siber yang tidak mengenal batas wilayah.

KESIMPULAN

Kejahatan siber merupakan ancaman global yang terus berkembang seiring kemajuan teknologi, mencakup berbagai bentuk seperti peretasan, penyebaran malware, serta serangan DoS dan DDoS. Regulasi dalam hukum internasional, seperti Konvensi Budapest, telah berupaya

mengatasi permasalahan ini dengan menetapkan standar kriminalisasi serta kerja sama antarnegara. Namun, implementasi regulasi ini masih menghadapi tantangan, terutama karena tidak semua negara meratifikasinya. Di Indonesia, kejahatan siber berdampak signifikan terhadap keamanan nasional dan stabilitas sosial, terutama dalam bentuk pencurian data, serangan terhadap infrastruktur kritis, serta penyebaran hoaks yang dapat memengaruhi opini publik dan bahkan jalannya proses hukum.

Interpol berperan penting dalam upaya penanggulangan kejahatan siber melalui investigasi digital, penindakan hukum, serta koordinasi dengan berbagai negara untuk menangkap pelaku kejahatan lintas batas. Di Indonesia, kerja sama Interpol dengan lembaga penegak hukum nasional bertujuan untuk meningkatkan keamanan siber dan mencegah eskalasi ancaman digital. Dalam konteks hukum pembuktian, tantangan utama adalah bagaimana alat bukti digital dapat diakui di pengadilan serta memastikan keadilan substantif dalam penyelesaian kasus kejahatan siber. Oleh karena itu, pendekatan multidimensi yang mencakup aspek regulasi, teknologi, dan kerja sama global sangat diperlukan agar kejahatan siber dapat ditanggulangi secara efektif.

DAFTAR REFERENSI

- Badan Siber dan Sandi Negara. (2021). *Laporan tahunan keamanan siber Indonesia*.
- Badan Siber dan Sandi Negara. (2022). *Laporan Keamanan Siber Nasional 2022*. Jakarta: BSSN.
- Badan Siber dan Sandi Negara. (2023). *Laporan Keamanan Siber Nasional 2023*. Jakarta: BSSN.
- Budiarti, A. (2020).
- CNN Indonesia. (2022). *Kebocoran data di Indonesia dan ancaman bagi pengguna internet*.
- Europol. (2022). *Internet Organised Crime Threat Assessment (IOCTA) Report*. Hague: Europol.
- Fadhillah, S., Matakupan, M., & Minggu, B. (2023). Peran Interpol dalam penyelesaian kasus kejahatan siber berdasarkan Konvensi Budapest on Cybercrimes. *Journal on Education*, 5(4), 16553–16564. Retrieved from <https://jonedu.org>
- Interpol Indonesia. (n.d.). *Cybercrime: Sebuah fenomena di dunia maya*. INTERPOL.
- Kominfo RI. (2023). *Strategi Nasional Keamanan Siber Indonesia*. Jakarta: Kementerian Komunikasi dan Informatika.
- NCB-Interpol Indonesia. (n.d.). *Peran National Central Bureau (NCB) Interpol Indonesia dalam pemberantasan tindak kejahatan cybercrime*. Retrieved from <https://www.neliti.com>
- Nurwahyudi, T. (2021). *Kejahatan siber: Tantangan dan penegakan hukum di era digital*. Yogyakarta: Deepublish.
- Polri. (2023). *Strategi penegakan hukum terhadap kejahatan siber di Indonesia*. Jakarta: Divisi Siber Polri.