Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

Antisipasi Dan Perkembangan Kejahatan Dunia Maya

Hartanto, Yoga Ade Rhamadani, Bagus Anwar Hidayatullah
Fakultas Hukum, Univ. Widya Mataram, Yogyakarta
hartanto.yogya@gmail.com

Abstract

Cybercrime is constantly evolving, from speed to acceleration, so negligence in guarding a country's cyberspace has the potential to cause disasters in various sectors of national and state life. The government as the regulator has a central role in initiating protection for internet users and taking firm action against perpetrators of cyber crime. The phenomenon of this era is that the Indonesian legal system has not been able to overcome internet user crimes, and some still rely on public complaints. The level of law enforcement is still constrained by limited legal norms, investigator capabilities, evidence, and computer forensics. Further studies are needed in relation to cybercrime, especially in law enforcement agencies (government). This normative research is expected to contribute to a deeper understanding of cybercrime. Research shows that the misuse of digital technology (especially related to the internet) still occurs in society, so cybercrime will continue to occur, either intentionally or due to negligence.
Keywords: cybercrime, criminal law, cyber, jurisdiction

Abstrak

Kejahatan dunia maya senantiasi berkembang, dari ukuran kecepatan menjadi percepatan, maka kelengahan penjagaan suata negara terhadap dunia mayanya berpotensi menimbulkan bencana diberbagai sektor kehidupan berbangsa dan bernegara. Pemerintah sebagai pemegang regulasi memiliki peran sentral dalam memprakarsai perlindungan terhadap pengguna internet dan menindak tegas bagi para pelaku *cyber crime*. Fenoma era ini sistem hukum Indonesia belum dapat menanggulangi kejahatan pengguna internet, dan sebagian masih mengandalkan adanya aduan masyarakat. Tataran penegakan hukum masih terkendala keterbatasan norma hukum, kemampuan penyidik, alat bukti, dan komputer forensik. Perlu adanya kajian lebih lanjut kaitannya dengan kejahatan di dunia maya ini terutama pada lembaga penegakan hukum (pemerintah). Penelitian normatif ini diharapkan dapat memberikan kontribusi terhadap pemahaman lebih dalam mengenai *cyber crime*. Penelitian menunjukkan bahwa penyalahgunaan teknologi digital (terutama terkait internet) masih terjadi di masyarakat, maka kejahatan di dunia maya akan terus terjadi, baik disengaja maupun karena kelalaian.
Kata Kunci: kejahatan, dunia maya, hukum pidana, siber, yurisdiksi

Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

A. PENDAHULUAN

Laporan AwanPintar.id® semester II tahun 2023, bahwa serangan siber terhadap Indonesia dari luar negeri meningkat sebesar 97,53% dibandingkan semester I tahun yang sama. Peningkatan serangan yang tidak biasa dilaporkan pada paruh pertama tahun 2024, sehingga menarik perhatian lebih lanjut dan meningkatkan kewaspadaan (Awanpintar.id, 2024).

Kejahatan dunia maya memang menjadi isu global yang semakin meresahkan seiring dengan pesatnya perkembangan teknologi informasi. Di Indonesia, penggunaan layanan digital seperti email, e-banking, dan e-commerce semakin meningkat, yang juga membuka peluang bagi pelaku kejahatan untuk melakukan aksi mereka. Maraknya transaksi online dan komunikasi digital tanpa pengamanan yang memadai seringkali menjadikan pengguna rentan terhadap berbagai bentuk penipuan dan pencurian.

Salah satu bentuk kejahatan yang paling umum adalah pencurian identitas. Dalam kasus ini, pelaku menggunakan teknik *phishing* untuk mendapatkan informasi pribadi, seperti nama, alamat, nomor telepon, dan informasi keuangan. Biasanya, mereka akan mengirimkan email yang tampak sah, berisi tautan ke situs web palsu yang menyerupai situs resmi. Ketika korban memasukkan data mereka, informasi tersebut langsung jatuh ke tangan penjahat. Dengan data ini, pelaku dapat melakukan berbagai tindakan merugikan, seperti membuka rekening bank baru atau melakukan transaksi belanja online atas nama korban.

Penipuan dalam *e-commerce* juga menjadi masalah serius. Banyak pengguna yang tergiur dengan penawaran harga murah atau produk yang tidak nyata. Dalam kasus ini, pelaku sering kali menciptakan situs web palsu yang menawarkan produk atau jasa dengan harga yang sangat menarik. Setelah korban melakukan pembayaran, barang yang dijanjikan tidak pernah dikirimkan, dan pelaku menghilang tanpa jejak. Kasus-kasus seperti ini sering kali terjadi di platform media sosial, di mana iklan yang tampak menarik bisa sangat menyesatkan.

Selain itu, kejahatan dunia maya di Indonesia juga mencakup penipuan melalui layanan *e-banking*. Di sini, pelaku dapat menggunakan teknik memahami relasi sosial/ psikologi untuk meyakinkan korban agar memberikan informasi login atau mengakses akun bank mereka. Beberapa penjahat bahkan menggunakan malware untuk menyusup ke perangkat korban dan mencuri data keuangan secara langsung. Ketidakpahaman pengguna tentang keamanan transaksi online menjadi faktor utama yang dimanfaatkan oleh pelaku.

Penggunaan perangkat mobile yang terus meningkat juga menambah risiko kejahatan dunia maya. Banyak aplikasi yang tidak resmi atau tidak terjamin keamanannya dapat menjadi pintu masuk bagi para penjahat untuk mengakses data pribadi pengguna. Pengguna sering kali mengabaikan pentingnya mengunduh aplikasi hanya dari sumber yang terpercaya, dan ini dapat menyebabkan pelanggaran privasi serta kerugian finansial. Tentu saja, pemerintah Indonesia harus berusaha untuk mengatasi masalah ini, UU tentang Informasi dan Transaksi Elektronik merupakan salah satu upaya pemerintah untuk memberikan landasan hukum bagi penegakan hukum terhadap kejahatan siber. Namun, dalam penegakan hukum masih menghadapi berbagai tantangan, termasuk kurangnya sumber daya dan peralatan untuk melacak pelaku yang sering berpindah tempat secara virtual.

Masyarakat juga memiliki peran penting dalam mencegah kejahatan dunia maya. Kesadaran akan pentingnya keamanan digital harus ditingkatkan. Pengguna harus diberi pemahaman tentang cara mengenali tanda-tanda penipuan,

Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

pentingnya menjaga kerahasiaan informasi pribadi, serta cara melindungi akun mereka dengan menggunakan autentikasi dua faktor dan kata sandi yang kuat. Pelatihan dan edukasi tentang keamanan siber di sekolah dan komunitas dapat menjadi langkah awal yang baik dalam membangun budaya keamanan digital.

Di samping upaya preventif, kerjasama antara sektor publik dan swasta juga diperlukan untuk menangani kejahatan dunia maya secara lebih efektif, dikarenakan serangan dari para pelaku luar negeri ke Indonesia juga sangat besar. Perusahaan teknologi harus berkomitmen untuk mengembangkan dan menerapkan solusi keamanan yang lebih baik, seperti enkripsi data dan sistem deteksi intrusi. Ini tidak hanya melindungi pengguna mereka, tetapi juga menjaga reputasi dan kepercayaan pelanggan terhadap layanan yang mereka tawarkan. Selanjutnya, kerja sama internasional juga harus diperkuat untuk menanggulangi kejahatan dunia maya yang sering kali melintasi batas negara. Penegakan hukum yang efektif memerlukan pertukaran informasi dan kolaborasi antara negara-negara. Organisasi internasional dan badan penegak hukum di seluruh dunia harus bekerja sama untuk menciptakan kerangka kerja yang memungkinkan penanganan kasus kejahatan siber secara lintas negara.

Di era digital ini, inovasi teknologi juga bisa menjadi senjata ampuh dalam memerangi kejahatan dunia maya. Penggunaan kecerdasan buatan (AI) untuk menganalisis pola perilaku dan mendeteksi aktivitas mencurigakan dapat membantu dalam mengidentifikasi dan mencegah kejahatan sebelum terjadi. Selain itu, teknologi blockchain juga menawarkan potensi besar dalam meningkatkan keamanan transaksi dan melindungi data dari manipulasi.

Dalam konteks masyarakat yang semakin digital, penting bagi setiap individu untuk menjadi "pahlawan" dalam keamanan siber. Hal ini dapat dimulai dengan langkah-langkah sederhana seperti memeriksa keaslian *email* sebelum mengklik tautan, tidak membagikan informasi pribadi di media sosial, dan selalu menggunakan koneksi internet yang aman. Kesadaran kolektif dan tanggung jawab individu dalam melindungi diri dari kejahatan dunia maya akan menciptakan lingkungan digital yang lebih aman bagi semua orang.

Akhirnya, meskipun kejahatan dunia maya merupakan tantangan serius, dengan pemahaman yang baik, kolaborasi antara berbagai pihak, dan penggunaan teknologi yang tepat, kita dapat mengurangi risiko dan dampaknya. Keamanan siber bukan hanya tanggung jawab pemerintah atau perusahaan, tetapi juga tanggung jawab setiap individu. Dengan demikian, melalui edukasi, kerjasama, dan teknologi, kita bisa menciptakan ekosistem digital yang lebih aman dan bermanfaat bagi seluruh masyarakat.

B. TINJAUAN PUSTAKA

Cyber crime atau kejahatan dunia maya merujuk pada segala bentuk kegiatan kriminal/ ilegal yang dilakukan dengan memanfaatkan teknologi informasi dan internet. (M.R. Habibi-I.Liviani, 2020). Era ini perkembangan teknologi semakin pesat, seiring meningkatnya pengguna teknologi oleh masyarakat, hal ini menimbulkan banyak dampak positif dan negatif. Sisi yang perlu diantisipasi adalah banyak masyarakat yang melakukan penyalahgunaan dalam menggunakan teknologi komputer, yang kemudian meningkat menjadi kegiatan kriminal di dunia maya yang dikenal dengan istilah *cyber crime*. Cyber crime dimaknai kejahatan dunia maya mengacu pada aktivitas kriminal apa pun yang menggunakan komputer atau jaringan komputer sebagai alat, target, atau lokasi untuk aktivitas kriminal. (Y.M Saragih, A.P.U. Siahaan, 2016). Kejahatan terkait

Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

teknologi ini telah mencakup berbagai jenis tindakan ilegal yang dapat merugikan individu, perusahaan, dan bahkan negara. Kejahatan dunia maya pada umumnya memiliki ciri-ciri sebagai berikut: Tidak terbatasi oleh batas geografis, pelaku dapat dilakukan dari mana saja, sulitnya koordinasi antar yurisdiksi, maka mengandung konsekwensi sulit melacak dan menangkap pelaku.

C. METODE PENELITIAN

Penelitian ini merupakan jenis penelitian hukum normatif, yaitu penelitian hukum yang menggunakan penelitian sumber sekunder (library/ conceptual study) dengan menggunakan kajian dokumen-dokumen hukum. Data yang diperoleh disajikan sebagai dokumen hukum berbentuk narasi dan diuraikan secara sistematis, logis, dan rasional. Artinya semua data yang diperoleh dihubungkan satu sama lain sesuai dengan pertanyaan penelitian dan membentuk satu kesatuan yang utuh.(Aida Dewi, dkk, 2023). Rumusan masalah yang dikaji adalah bagaimana antisipasi atas kejahatan dunia maya (cyber).

D. HASIL dan PEMBAHASAN

1. Pengertian Cyber Crime

Cyber Crime atau kejahatan dunia maya merujuk pada segala bentuk kegiatan kriminal yang dilakukan dengan memanfaatkan teknologi informasi dan internet. Dalam era digital saat ini, kejahatan ini telah berkembang pesat dan mencakup berbagai jenis tindakan ilegal yang dapat merugikan individu, perusahaan, dan bahkan negara. Salah satu bentuk *cyber crime* yang paling umum adalah pencurian identitas. Pelaku kejahatan ini menggunakan teknik seperti phishing untuk mendapatkan informasi pribadi, seperti nama, alamat, dan nomor rekening bank, dengan maksud untuk melakukan penipuan atau akses ilegal ke akun keuangan korban. Phishing biasanya dilakukan melalui email yang tampak sah atau situs *web* yang meniru layanan resmi. Selain pencurian identitas, penipuan online juga merupakan salah satu modus kejahatan yang sering terjadi. Dalam kasus ini, penjahat dapat menciptakan situs web palsu yang menawarkan produk atau jasa dengan harga menarik. Setelah korban melakukan pembayaran, barang yang dijanjikan tidak pernah diterima, dan pelaku menghilang tanpa jejak. Peretasan (hacking) adalah bentuk lain dari *cyber crime* di mana pelaku mencoba untuk mengakses sistem komputer atau jaringan secara ilegal. Melalui teknik ini, mereka dapat mencuri data sensitif, merusak sistem, atau menyebarkan *malware. Malware*, seperti virus, trojan, atau ransomware, adalah perangkat lunak berbahaya yang dirancang untuk merusak, mengakses, atau mengambil alih perangkat pengguna.

Cyber crime juga mencakup kejahatan yang lebih serius, seperti pembajakan data dan penyebaran konten ilegal, termasuk pornografi anak dan materi yang melanggar hak cipta. Kejahatan semacam ini tidak hanya berdampak negatif pada individu yang menjadi korban, tetapi juga dapat merusak reputasi perusahaan dan mengganggu keamanan nasional. Khusus kejahatan *cyber* terkait pornografi juga memprihatinkan, karena acapkali menimbulkan korban dikalangan perempuan dan anak. (Hartanto, 2024). Hal terkait anak juga terjadi dalam bentuk eksploitasi ekonomi terhadap waktu dan energi anak-anak demi keuntungan materi yang bertentangan dengan anak, misal *kids influencer*. (Hartanto, dkk., 2024). Salah satu tantangan utama dalam memerangi *cyber crime* adalah sifatnya yang lintas batas. Kejahatan ini sering kali melibatkan pelaku dari berbagai negara, sehingga penegakan hukum menjadi sulit. Oleh karena itu, kerjasama internasional dan kolaborasi antara pemerintah, perusahaan, dan masyarakat sangat penting dalam menghadapi tantangan ini.

Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

Penting untuk meningkatkan kesadaran tentang *cyber crime* agar individu dan organisasi dapat melindungi diri mereka. Langkah-langkah pencegahan, seperti menggunakan kata sandi yang kuat, memperbarui perangkat lunak secara teratur, dan tidak membagikan informasi pribadi secara sembarangan, sangat penting untuk mengurangi risiko terjadinya kejahatan dunia maya. Dengan pengetahuan dan kewaspadaan yang tepat, kita dapat menciptakan lingkungan digital yang lebih aman. Menurut *website* diskominfo ada 4 jeni skejahatan siber: Penipuan/ *phising*, peretasan, *cyber stalking, cyber bullying.*(Rini Pertiwi, 2024).

2. *Cyber Crime* Berdasarkan Jenis Kejahatannya:

a. *Phishing: Phishing* adalah salah satu metode yang paling umum digunakan dalam pencurian identitas. Pelaku mengirimkan email atau pesan yang tampak resmi, sering kali berpura-pura menjadi bank, layanan online, atau perusahaan terkemuka lainnya. Pesan tersebut biasanya berisi tautan yang mengarahkan korban ke situs web palsu yang menyerupai situs resmi. Di situs ini, korban diminta untuk memasukkan informasi sensitif, seperti nama pengguna, kata sandi, atau nomor kartu kredit. Salah satu contohnya adalah ketika pelaku mengirim email yang mengklaim bahwa akun bank korban telah terancam. Mereka kemudian meminta korban untuk mengklik tautan dan memperbarui informasi keamanan. Banyak pengguna yang, karena panik, segera mengikuti instruksi tersebut tanpa memeriksa keaslian email. Ini menjadi salah satu cara efektif bagi penjahat untuk mendapatkan akses langsung ke akun bank korban. (phising ini merupakan salah satu bentuk rekayasa sosial/ *social enginnering*).

b. *Spear Phishing: Spear phishing* adalah versi lebih terfokus dari phishing. Dalam modus ini, pelaku melakukan riset mendalam untuk mengumpulkan informasi pribadi tentang korban, seperti nama, alamat, atau bahkan informasi pekerjaan. Dengan menggunakan data ini, pelaku dapat mengirimkan pesan yang tampak sangat meyakinkan, sehingga korban lebih cenderung merespons. Misalnya, jika pelaku mengetahui bahwa korban bekerja di sebuah perusahaan tertentu, mereka dapat mengirimkan email yang tampak berasal dari atasan atau rekan kerja, meminta informasi sensitif untuk tujuan "proyek". Banyak orang yang cenderung lebih percaya pada pesan yang tampaknya berasal dari orang yang mereka kenal, sehingga mereka mungkin lebih mudah terjebak.

c. *Social Engineering: Social engineering* secara umum adalah teknik manipulasi psikologis untuk mendapatkan informasi pribadi dari korban. Pelaku dapat melakukan panggilan telepon dan berpura-pura sebagai petugas bank atau layanan pelanggan, meminta korban untuk memberikan data sensitif. Taktik ini sering kali melibatkan penggunaan tekanan emosional atau urgensi, membuat korban merasa bahwa mereka harus segera memberikan informasi. Sebagai contoh, pelaku bisa berpura-pura sebagai petugas keamanan yang mengklaim bahwa akun korban sedang dalam bahaya. Dengan menciptakan rasa takut, mereka mendorong korban untuk memberikan informasi tanpa berpikir panjang. Data Breach Investigations Report menyatakan phising sebagai bagian dari rekayasa sosial menduduki peringkat sedikit lebih tinggi dari ransomware (dengan motivasi keuangan). (DBIR Report 2024).

Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

d. Menggunakan *Wi-Fi* Publik: Banyak orang menggunakan jaringan *Wi-Fi* publik tanpa menyadari risiko keamanan yang ada. Pelaku dapat menciptakan *hotspot Wi-Fi* yang tampak sah dan mengamati data yang dikirimkan pengguna yang terhubung. Ini termasuk informasi *login*, *email*, dan data sensitif lainnya. Sebagai contoh, seseorang yang menggunakan *Wi-Fi* publik di kafe dapat memasukkan kata sandi akun bank mereka. Jika mereka terhubung ke *hotspot* yang dikelola oleh pelaku, data tersebut dapat dicuri dengan mudah.
e. *Data Breach: Data breach* terjadi ketika sistem keamanan suatu perusahaan atau organisasi dilanggar, dan informasi sensitif dicuri. Banyak perusahaan besar telah mengalami kebocoran data yang melibatkan jutaan informasi pelanggan, termasuk nama, alamat, nomor kartu kredit, dan informasi lainnya.Sebagai contoh, pada tahun 2017, Equifax, salah satu lembaga laporan kredit terbesar di Amerika Serikat, mengalami kebocoran data yang mengakibatkan informasi pribadi sekitar 143 juta orang terekspos. Kejadian ini menyebabkan banyak individu menjadi korban pencurian identitas, karena informasi mereka dapat digunakan untuk membuka rekening baru atau melakukan penipuan. (A.M. Prastiwi, 2017).
f. *Mail Theft: Mail theft* adalah metode tradisional namun efektif dalam pencurian identitas. Pelaku mencuri surat dari kotak pos korban yang berisi informasi sensitif, seperti tagihan, laporan bank, atau dokumen penting lainnya. Setelah mendapatkan informasi ini, pelaku dapat menyamar sebagai korban dan mengakses akun atau melakukan penipuan. Misalnya, jika pelaku mencuri laporan bank yang berisi informasi nomor rekening, mereka dapat mencoba mengakses akun bank korban secara online dan melakukan transaksi tanpa izin.
g. *Skimming: Skimming* adalah teknik di mana pelaku memasang perangkat kecil di mesin ATM atau terminal pembayaran untuk mencuri informasi dari kartu kredit atau debit pengguna. Perangkat ini dapat membaca data dari pita magnetik kartu dan, dalam beberapa kasus, juga dapat mengambil PIN korban. Dengan menggunakan informasi yang dicuri, pelaku dapat mencetak kartu baru dan melakukan penarikan tunai atau pembelian tanpa sepengetahuan korban.
h. Penyalahgunaan Media Sosial: Media sosial merupakan ladang subur bagi pelaku pencurian identitas. Banyak orang cenderung membagikan informasi pribadi di platform-platform ini, yang kemudian dapat dimanfaatkan oleh pelaku. Dengan mengumpulkan data dari profil media sosial, pelaku dapat merancang serangan yang lebih terarah dan meyakinkan. Sebagai contoh, pelaku dapat menggunakan informasi tentang lokasi, pekerjaan, atau hubungan sosial untuk menyamar sebagai teman atau rekan kerja dan meminta informasi sensitif.

3. Cyber crime dapat diklasifikasikan berdasarkan beberapa hal (modus dan motif):

a. Berdasarkan Pelaku

Salah satu cara untuk mengklasifikasikan cyber crime adalah berdasarkan pelakunya. Kejahatan ini dapat dilakukan oleh individu yang bertindak sendirian, sering kali dengan motivasi untuk mencari tantangan atau keuntungan pribadi. Misalnya, hacker yang beroperasi sendiri dapat meretas sistem untuk mencuri data pribadi atau mengakses informasi sensitif. Di sisi lain, ada juga kelompok atau organisasi yang terorganisir, seperti kelompok hacker yang bekerja sama untuk

Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

melakukan serangan lebih besar, misalnya meretas situs web pemerintah atau perusahaan besar. Dalam kasus ini, pelaku tidak hanya berorientasi pada keuntungan finansial, tetapi dapat pula memiliki agenda politik atau sosial.

b. Berdasarkan Tujuan

Cyber crime juga dapat dikelompokkan berdasarkan tujuannya. Ada kejahatan yang bertujuan untuk keuntungan finansial, seperti pencurian data kartu kredit atau penipuan *online*, di mana pelaku berusaha mendapatkan uang secara ilegal. Namun, tidak semua *cyber crime* bersifat finansial. Beberapa pelaku melakukan kejahatan dengan motivasi politik, seperti hacktivism, di mana mereka meretas situs web untuk menyampaikan pesan sosial atau politik. Di sisi lain, ada juga kejahatan yang dilakukan untuk alasan pribadi, seperti *doxxing*, di mana informasi pribadi seseorang diungkapkan sebagai bentuk balas dendam atau intimidasi.

c. Berdasarkan Metode

Dari segi metode, *cyber crime* bisa dibagi menjadi serangan langsung dan penipuan sosial. Serangan langsung mencakup tindakan yang langsung merusak sistem, seperti *hacking* dan penyebaran *malware*. Para pelaku menggunakan teknik-teknik canggih untuk mengakses dan mengendalikan sistem yang mereka targetkan. Sementara itu, penipuan sosial mengandalkan manipulasi psikologis. Misalnya, dalam kasus *phishing*, pelaku menyamar sebagai entitas tepercaya untuk mendapatkan informasi pribadi dari korban. Ini menunjukkan bahwa meskipun teknologi yang digunakan dalam *cyber crime* bisa sangat canggih, teknik psikologis juga memainkan peran penting dalam keberhasilan kejahatan ini.

d. Berdasarkan Tingkat Kerugian

Kejahatan siber juga dapat dikategorikan berdasarkan tingkat kerugian yang ditimbulkan. Ada kejahatan dengan dampak rendah, seperti spam atau pencurian identitas yang tidak signifikan. Namun, ada juga kejahatan yang dapat menyebabkan kerugian yang lebih besar, seperti penipuan online yang merugikan korban secara finansial. Di tingkat tertinggi, kita menemukan serangan ransomware yang dapat melumpuhkan perusahaan, menyebabkan kerugian finansial yang besar dan merusak reputasi bisnis.

e. Berdasarkan Target

Cyber crime juga dapat dikelompokkan berdasarkan target. Beberapa kejahatan menyasar individu, seperti kasus *cyber bullying* dan pencurian identitas. Yang lainnya menargetkan bisnis, seperti serangan DDoS dan pencurian data perusahaan. Ada juga kejahatan yang menyasar pemerintah, di mana pelaku berusaha meretas sistem pemerintah atau menyebarkan informasi palsu untuk mempengaruhi kebijakan publik. (R.D.Hapsari, K.G. Pambayun, 2023). Kejahatan dalam dunia maya (siber), semakin kompleks seiring dengan perkembangan teknologi informasi dan komunikasi. Untuk memahami jenis-jenis kejahatan ini secara lebih mendalam, kita dapat mengkategorikannya berdasarkan karakteristik tertentu. Klasifikasi ini membantu kita untuk mengenali potensi ancaman dan mengambil langkah-langkah pencegahan yang diperlukan. Dalam narasi ini, kita akan membahas beberapa kategori utama *cyber crime* berdasarkan pelaku, tujuan, metode, tingkat kerugian, dan target.

f. Berdasarkan Tujuan

Kejahatan ini dapat dikategorikan berdasarkan tujuan dan niat pelaku. Banyak *cyber crime* bertujuan untuk mendapatkan keuntungan finansial, seperti pencurian data kartu kredit atau penipuan *online*. Di sisi lain, ada juga pelaku yang melakukan tindakan ini dengan motivasi politik, seperti *hacktivism*, yang bertujuan untuk menyebarkan pesan sosial atau memprotes kebijakan pemerintah. Selain itu, kejahatan yang bersifat pribadi, seperti *doxxing*, bertujuan untuk mencemarkan nama baik

Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

atau menyakiti individu tertentu. Dengan memahami motivasi ini, kita bisa lebih waspada terhadap ancaman yang mungkin muncul.

g. Berdasarkan Metode

Cyber crime berdasar metode dapat dibagi menjadi dua kategori utama: serangan langsung dan penipuan sosial. Serangan langsung mencakup tindakan yang merusak sistem, seperti *hacking*, penyebaran *malware*, dan serangan DdoS. Metode ini sering kali melibatkan teknik teknis yang canggih untuk mengakses dan mengendalikan sistem yang ditargetkan. Sementara itu, penipuan sosial mengandalkan manipulasi psikologis untuk menipu korban, misalnya dalam bentuk phishing. Dalam kasus ini, pelaku menyamar sebagai entitas tepercaya untuk mendapatkan informasi sensitif. Keduanya menunjukkan bahwa *cyber crime* tidak hanya bergantung pada teknologi, tetapi juga pada pemahaman terhadap perilaku manusia (AI).

h. Berdasarkan Tingkat Kerugian

Cyber crime juga dapat dikategorikan berdasarkan tingkat kerugian yang ditimbulkan. Beberapa kejahatan, seperti spam, mungkin hanya menyebabkan kerugian kecil. Namun, ada kejahatan yang dapat menimbulkan kerugian finansial yang signifikan, seperti penipuan online dan pencurian identitas. Di tingkat yang lebih serius, serangan ransomware dapat melumpuhkan perusahaan, mengakibatkan kerugian besar dan bahkan mengancam kelangsungan hidup bisnis. Dengan memahami potensi kerugian ini, individu dan organisasi dapat lebih proaktif dalam mengimplementasikan langkah-langkah keamanan.

4. Kontributor Kejahatan Siber berdasarkan IP

Sumber: awanpintar.id, Laporan Semester 1, 2024

Penjahat di dunia maya selalau ada bahkan berkembang, karena mereka yakin dapat bersembunyi dengan akun anonimitas di internet. Namun perilaku mereka senantiasi menimbulkan perhatian di dunia digital terutama karena menimbulkan korban. Jejak digital sulit dihilangkan, salah satunya dapat ditelusuri melalui alamat IP yang mereka gunakan. Berikut jejak data yang ditelusuri *AwanPintar.id®* ke infrastruktur jaringan Indonesia. Fokus utama dari 10 penyerang IP teratas adalah bahwa pengguna IP Singapura merupakan mayoritas melakukan serangan, namun masih berada di bawah pengguna IP Belanda secara keseluruhan. Hal yang menarik adalah bahwa Singapura sama sekali tidak masuk dalam 10 besar tahun lalu. Sementara itu, pengguna alamat IP AS, yang sejauh ini merupakan pengguna dominan pada paruh pertama tahun lalu, menghilang dari lalu lintas, dengan penurunan yang sangat besar dalam 10 besar pengguna alamat IP AS, namun tetap ada kemungkinan penyerang memodifikasi serangannya menggunakan IP dari negara lain, membajaknya, dan menggunakannya sebagai BOT. (AwanPintar.Id, 2024)

5. Antisipasi *Cyber Crime* di Indonesia

Kejahatan dunia maya adalah tantangan serius yang memerlukan perhatian lebih dari semua pihak. Di Indonesia, di tengah pesatnya transformasi

Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

digital, tindakan pencegahan yang efektif harus dilakukan untuk melindungi masyarakat dari risiko yang semakin meningkat. Berikut adalah beberapa langkah yang dapat diambil untuk mencegah *cyber crime* dan menciptakan lingkungan digital yang lebih aman. Pembentuk undang-undang telah membuat aturan buat menaikkan kapasitas penegakan aturan pada memperkuat prosedur keamanan siber, dengan pembentukan Badan Siber & Sandi Negara (BSSN) & senatiasi merevis UU tentang Informasi & Transaksi Elektronik, dan UU lain sejenisnya, dengan tujuan melindungi infrastruktur digital Indonesia & memerangi kejahatan siber (Saleh & Winata, 2023).

1. Meningkatkan Edukasi dan Kesadaran

Edukasi merupakan kunci utama dalam mencegah kejahatan dunia maya. Masyarakat harus dilibatkan dalam program-program edukasi yang fokus pada keamanan digital. Sekolah dan institusi pendidikan harus menyertakan materi tentang keamanan siber dalam kurikulum mereka. Pelatihan tentang cara mengenali tanda-tanda penipuan, melindungi data pribadi, dan menggunakan internet dengan aman dan sehat sangat diperlukan untuk semua kalangan dan semua usia. Selain pendidikan formal, kampanye kesadaran publik melalui media sosial, seminar, dan *workshop* juga dapat meningkatkan pengetahuan masyarakat tentang risiko *cyber crime*. Menggunakan *influencer* atau tokoh masyarakat untuk menyebarkan pesan keamanan siber dapat membuat informasi tersebut lebih menarik dan mudah diterima.

2. Implementasi Teknologi Keamanan yang Kuat

Perusahaan dan organisasi harus menginvestasikan sumber daya untuk menerapkan teknologi keamanan yang lebih baik. Ini mencakup penggunaan perangkat lunak keamanan yang mutakhir, enkripsi data, dan sistem deteksi intrusi yang mampu mengidentifikasi aktivitas mencurigakan. Selain itu, penggunaan autentikasi dua faktor untuk semua akun yang memiliki akses ke data sensitif harus menjadi standar. Langkah-langkah ini tidak hanya melindungi informasi perusahaan, tetapi juga memberikan rasa aman kepada pengguna. Sektor perbankan, misalnya, harus terus memperbarui sistem keamanan mereka agar tetap selangkah lebih maju dari para pelaku kejahatan. Penggunaan biometrik, seperti sidik jari atau pengenalan wajah, dapat menjadi tambahan yang efektif untuk melindungi akses ke akun.

3. Mendorong Kerjasama Antara Sektor Publik dan Swasta

Kerjasama antara pemerintah, perusahaan teknologi, dan lembaga penegak hukum sangat penting dalam menghadapi ancaman cyber crime. Pemerintah perlu membuat kebijakan yang mendukung kolaborasi ini, misalnya dengan menyediakan insentif bagi perusahaan yang mengembangkan solusi keamanan yang inovatif. Dalam hal ini, pertemuan rutin antara semua pihak terkait dapat menciptakan forum untuk berbagi informasi dan strategi. Perusahaan juga harus berkomitmen untuk melaporkan insiden keamanan dan berbagi informasi mengenai serangan yang mereka alami. Dengan berbagi informasi ini, pihak lain dapat belajar dan meningkatkan sistem mereka untuk mencegah serangan serupa.

4. Mengembangkan Infrastruktur Keamanan Siber yang Kuat

Infrastruktur keamanan siber di Indonesia perlu diperkuat dengan pengembangan pusat respon insiden yang mampu merespons serangan siber secara cepat dan efektif. Pusat ini dapat bekerja sama dengan lembaga penegak hukum dan perusahaan swasta untuk mengatasi insiden keamanan secara terpadu. Pelatihan untuk personel yang terlibat dalam penanganan insiden *cyber*, agar memiliki keterampilan yang diperlukan untuk menghadapi situasi kompleks.

Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

5. Memperkuat Kerja Sama Internasional

Keberhasilan penegakan hukum dalam kasus cyber crime sering kali bergantung pada kerja sama internasional. Indonesia harus aktif berpartisipasi dalam forum-forum internasional yang membahas isu keamanan siber, seperti ASEAN *Cybersecurity Cooperation*. Melalui forum-forum ini, Indonesia dapat berbagi praktik terbaik dan menerima dukungan dari negara lain dalam penanganan kejahatan dunia maya. Badan penegak hukum internasional, seperti Interpol, juga dapat membantu dalam melacak pelaku kejahatan yang beroperasi lintas negara. Dengan membangun jaringan global yang kuat, Indonesia dapat meningkatkan efektivitas penegakan hukum dalam menangani kejahatan siber.

6. Memanfaatkan Inovasi Teknologi

Inovasi teknologi dapat berfungsi sebagai alat ampuh dalam memerangi kejahatan dunia maya. Kecerdasan buatan (AI) dapat digunakan untuk menganalisis data besar dan mendeteksi pola-pola mencurigakan dalam aktivitas online. Teknologi machine learning juga dapat membantu mengidentifikasi serangan sebelum mereka terjadi, memberikan peluang untuk respons yang lebih cepat. *Blockchain*, dengan sifatnya yang aman dan transparan, juga menawarkan solusi untuk melindungi data dan transaksi dari manipulasi. Penggunaan teknologi ini di sektor-sektor kritis, seperti perbankan dan e-commerce, dapat meningkatkan keamanan dan kepercayaan pengguna.

7. Keterlibatan Komunitas dalam Keamanan Siber

Setiap individu harus merasa bertanggung jawab untuk menjaga keamanan siber. Ini termasuk mematuhi praktik-praktik baik, seperti memperbarui perangkat lunak secara berkala, menggunakan kata sandi yang kuat, dan tidak sembarangan membagikan informasi pribadi. Komunitas dapat berperan aktif dengan membentuk kelompok diskusi atau forum yang membahas isu keamanan siber. Dengan saling berbagi pengalaman dan pengetahuan, mereka dapat menciptakan lingkungan yang lebih aman bagi diri mereka dan orang lain.

Edukasi, kerjasama, dan penerapan teknologi yang canggih adalah kunci untuk menciptakan ekosistem digital yang aman dan bermanfaat bagi seluruh masyarakat. Dalam menghadapi tantangan ini, masyarakat diharapkan tidak hanya menjadi konsumen teknologi, tetapi juga menjadi pengelola dan pelindung dari kejahatan yang mengintai di dunia maya. Dalam menghadapi tantangan kejahatan dunia maya, sangat penting bagi kita untuk mengadopsi pendekatan yang holistik dan terintegrasi. Setiap individu, komunitas, dan institusi memiliki peran vital dalam membangun ekosistem keamanan siber yang lebih baik. Pengetahuan dan kesadaran masyarakat mengenai potensi risiko yang ada di dunia digital harus ditingkatkan. Ini dapat dilakukan melalui kampanye edukasi yang menyasar semua lapisan masyarakat, dari anak-anak hingga orang dewasa, tentang cara aman berinteraksi di internet. Edukasi bukan hanya tentang informasi teknis, tetapi juga membentuk budaya kritis dalam menggunakan teknologi. Masyarakat perlu diajarkan untuk selalu skeptis terhadap tawaran yang tampak terlalu baik untuk menjadi kenyataan, serta mengenali tanda-tanda potensi penipuan. Dengan memahami dasar-dasar keamanan siber, mereka dapat mengambil langkah-langkah preventif yang akan melindungi diri mereka dan orang-orang di sekitar mereka. Kolaborasi antara sektor publik dan swasta menjadi esensial dalam menciptakan infrastruktur keamanan yang kuat. Pemerintah perlu mendorong perusahaan untuk berinvestasi dalam sistem keamanan yang canggih dan memberi insentif bagi mereka yang berinovasi dalam menciptakan solusi yang efektif. Di sisi lain, perusahaan juga harus proaktif dalam

Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

berbagi informasi mengenai ancaman dan insiden keamanan yang mereka alami, agar semua pihak dapat belajar dari pengalaman satu sama lain. Kejahatan dunia maya juga mencakup dampak serius, mulai dari kerugian finansial individu hingga ancaman terhadap keamanan nasional. Teknologi modern, seperti kecerdasan buatan (AI) dan *blockchain*, dapat dimanfaatkan untuk mendeteksi dan mencegah kejahatan siber, namun inovasi ini tetap memerlukan peningkatan kesadaran dan edukasi masyarakat.

Kerja sama internasional juga tidak kalah penting. Karena kejahatan siber sering kali bersifat lintas batas, koordinasi antara negara-negara akan sangat membantu dalam penegakan hukum. Organisasi internasional harus menjadi jembatan bagi negara-negara untuk bertukar informasi dan membangun standar keamanan yang diakui secara global. Ini akan meningkatkan kemampuan semua negara dalam menangani kejahatan yang semakin kompleks. Organisasi internasional dan badan penegak hukum di berbagai negara harus bekerja sama secara fleksibel dan rutin untuk menciptakan kerangka kerja yang efektif dalam menangani kasus-kasus kejahatan siber. Sebagai individu, kita juga harus menyadari bahwa setiap tindakan kecil yang kita ambil dapat memberikan dampak yang signifikan. Menggunakan kata sandi yang kuat, tidak mengklik tautan yang mencurigakan, dan selalu memperbarui perangkat lunak adalah langkah-langkah sederhana yang dapat membantu menjaga keamanan siber kita sendiri. Akhir kata, menciptakan lingkungan digital yang aman adalah tanggung jawab bersama. Dengan saling mendukung, berkolaborasi, dan memanfaatkan teknologi secara bijak, kita dapat meredakan risiko kejahatan dunia maya dan membangun masyarakat yang lebih *resilient* di era digital.

E. SIMPULAN

Meningkatnya penggunaan layanan digital di Indonesia membuka peluang bagi pelaku kejahatan untuk melakukan berbagai tindakan ilegal, seperti pencurian identitas, penipuan *e-commerce*, dan peretasan. Tingkat literasi digital masyarakat Indonesia masih kurang, sehingga pelaku masih merajalela. Untuk mengatasi masalah ini, diperlukan kolaborasi antara pemerintah, sektor swasta, dan masyarakat untuk meningkatkan kesadaran akan keamanan siber, serta penerapan regulasi yang lebih ketat dan edukasi yang efektif untuk melindungi individu dari berbagai ancaman di dunia maya. Regulasi terkait Informasi dan Transaksi Elektronik (UU ITE) telah diimplementasikan untuk memberikan landasan hukum dalam menangani kejahatan siber. Namun, penegakan hukum masih menghadapi berbagai tantangan, seperti keterbatasan sumber daya, kurangnya kemampuan penyidik, dan kerumitan dalam melacak pelaku yang sering berpindah tempat secara virtual. Masyarakat perlu diberikan edukasi dan kesadaran tentang pentingnya keamanan digital, agar mereka dapat melindungi diri dari kejahatan siber. Penting juga untuk memperkuat kerjasama internasional dalam menghadapi cyber crime, karena banyak kejahatan ini bersifat lintas batas. Tanpa kerjasama ini, penegakan hukum akan mengalami kesulitan dalam mengejar pelaku yang banyak beroperasi secara global. Akhirnya, dalam era digital yang terus berkembang, individu harus menjadi "pahlawan" bagi keamanan siber. Tindakan sederhana seperti memeriksa keaslian email, menjaga kerahasiaan informasi pribadi, dan menggunakan autentikasi dua faktor dapat membantu menciptakan lingkungan digital yang lebih aman. Dengan pemahaman yang lebih baik, kolaborasi yang kuat, dan penggunaan teknologi yang tepat, kita bisa mengurangi risiko dan dampak dari kejahatan dunia maya. Keamanan siber adalah investasi untuk masa depan kita; disamping tanggung

Vol. 2 No. 2 2024
e-ISSN: 3025-5414
p-ISSN: 3025-5619

jawab negara, maka masyarakat harus berkomitmen untuk menjaga keamanan dan integritas dunia maya (siber).

DAFTAR PUSTAKA

JURNAL

Aida Dewi, dkk., 2023. Illegal Access Through "Wireless Fidelity" In Criminal Law, *Meta-Yuridis*, Volume 6 Nomor 2

Hartanto, 2024. Criminal Law: Chemical Castration Against People Sexual Violence Against Children, *De'Rechtsstaat,* Volume 10 Nomor 2

Hartanto, dkk., 2024. Urgensi Perlindungan Hukum Terhadap Eksploitasi Anak Dibawah Umur (Melalui Media Sosial), *Journal of Law, Administration, and Social Science*, Volume 4 Nomor 3

Miftakhur R.Habibi, I. Liviani, 2020. Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, Volume 23 Nomor 2

Rian D. Hapsari, Kuncoro G. Pambayun, 2023. ANCAMAN CYBERCRIME DI INDONESIA Sebuah Tinjauan Pustaka Sistematis, *Jurnal Konstituen*, Volume 5 Nomor 1

Yasmirah M. Saragih, Andysah P.U Siahaan. 2016. Cyber Crime Prevention Strategy in Indonesia. *SSRG International Journal of Humanities and Social Science (SSRG-IJHSS)*, Volume 3 Nomor 6

WEBSITE

_____, 2024. Top takeaways DBIR Report. From https://www.verizon.com/business/resources/reports/dbir/, diakses 15 Novermber 2024

Arie M. Prastiwi, 2017, Firma Kredit Equifax Diretas, Data 143 Juta Warga AS Terekspos. From https://www.liputan6.com/global/read/3086903/firma-kredit-equifax-diretas-data-143-juta-warga-as-terekspos, diakses 16 November2024

AwanPintar.Id, 2024. Indonesia Waspada (Laporan Ancaman Digital Indonesia), From https://www.awanpintar.id/wp-content/uploads/2024/08/2024_AwanPntar.id_Laporan_Ancaman_Digital_sem1_2024_Green.pdf, 21

Rini Pertiwi. ___,. Kenali 4 Jenis Kejahatan Siber. From https://kominfo.kotabogor.go.id/index.php/post/single/740, diakses 1 Desember 2024

Saleh, A. I., & Winata, M. D. 2023. Indonesia's Cyber Security Strategy: Problems and Challenges. In International Joint Conference on Arts and Humanities 2023, 1675-1696. *Atlantis Press*. https://doi.org/10.2991/978-2-38476-152-4_169