Jurnal Teknologi dan Manajemen Sistem Industri
Volume 3, Nomor 1, 2024
e-ISSN : 2964-8122
DOI: 10.56071/jtmsi.v3i1.483

RESIKO KEJAHATAN TEKNOLOGI INFORMASI DAN KOMUNIKASI CYBER CRIME DAN ANALISI INOVASI PENCEGAHAN RESIKO CYBER CRIME DI INDONESIA

Nita Maharani Harahap*
Universitas Islam Negeri Sumatera Utara, Indonesia
Email: nitamaharani844@gmail.com

Article Info

Article history:
Received: December 22, 2023
Accepted: October 05, 2023
Published: March 27, 2024

Page: 52-60

Keyword:
internet, media_sosial, cyber_crime

***Corresponding Author**
Nita Maharani Harahap

Abstract

Today's internet is primarily used by children and teenagers for social media communication and information gathering. The rapid development of information technology has both positive and negative impacts. While it drives global technological growth, it also creates challenges, such as decreased attention to the accuracy of information. This leads to a sense of security until individuals become victims themselves. Such indifference weakens security awareness and vigilance. This study aims to explore the risks of cybercrime and the innovations made to prevent its spread in society. Using a qualitative method, the research collects information through various tools and techniques to understand how to prevent emerging cyber threats. A recent case revealed criminals using an app that automatically retrieves victim data. The study provides insights into the high crime rate in cyberspace and raises awareness about the importance of cybersecurity.

Internet saat ini terutama digunakan oleh anak-anak dan remaja untuk komunikasi melalui media sosial dan pengumpulan informasi. Perkembangan pesat teknologi informasi memiliki dampak positif dan negatif. Meskipun mendorong pertumbuhan teknologi global, hal ini juga menciptakan tantangan, seperti berkurangnya perhatian terhadap akurasi informasi. Hal ini menyebabkan rasa aman hingga individu menjadi korban itu sendiri. Ketidakpedulian semacam ini melemahkan kesadaran dan kewaspadaan terhadap keamanan. Penelitian ini bertujuan untuk mengeksplorasi risiko kejahatan dunia maya dan inovasi yang telah dilakukan untuk mencegah penyebarannya di masyarakat. Dengan menggunakan metode kualitatif, penelitian ini mengumpulkan informasi melalui berbagai alat dan teknik untuk memahami cara mencegah ancaman dunia maya yang muncul. Sebuah kasus terbaru mengungkapkan bahwa para pelaku kejahatan menggunakan aplikasi yang secara otomatis mengambil data korban. Penelitian ini memberikan wawasan tentang tingginya tingkat kejahatan di dunia maya dan meningkatkan kesadaran tentang pentingnya keamanan siber.

Pendahuluan

Dunia sekarang berada di zaman Informasi ke zaman yang merupakan pergantian dari tahap lanjutan dari zaman prasejarah, pertanian, dan Industri. Memiliki informasi yang dimana mempunyai arti dan tugas yang sangat penting dalam segala bidang kehidupan di era informasi[1], dan merupakan salah satu dari kebutuhan hidup bagi tiap orang, baik individu maupun organisasi, sehingga dapat dikatakan bahwa. Dalam kehidupan masyarakat, informasi bekerja seperti aliran darah tubuh manusia sebagai sumber kehidupan. Yang dimana diantara seluruh penemuan ada satu penemuan yang mempunyai pengaruh terbesar pada masyarakat informasi yaitu penemuan Internet. Adanya penemuan ini sebagai bentuk dari sebuah teknologi baru telah memungkinkan manusia lepas dari arus informasi dan komunikasi. Internet telah membuat satu kemajuan besar dalam hidup[2]. Seperti teknologi lainnya, Internet tidak lepas dari nilainya. Teknologi akan efektif bila kita memperhatikan manfaat teknologi, disesuaikan dengan nilai pribadi dan sosial, dan pemerintah yang memiliki peraturan untuk melindungi masyarakat dari konsikuensi negatifnya.

Penggunaan internet sudah menjadi kebutuhan pokok dimana semua operasionalnya kini berbasis teknologi. Madiun merilis program web service gratis kepada masyarakat sebagai program diseminasi teknologi di kabupaten dan kabupaten[3]. Penyebaran Internet berdampak positif bagi kehidupan . orang, di mana menggunakan Internet sebagai sarana komunikasi, mengandalkan media sosial, mengakses layanan publik, menggunakannya sebagai alat pemasaran,. produk UMKM dan transaksi perbankan. Untuk pengguna internet, selain banyak hal positif yang menonjol, juga banyak kejahatan yang diakibatkan oleh penggunaan Internet[4]. Pengguna internet yang hanya bisa menikmati layanan tentunya tidak pernah memikirkan ancaman cyber istilah untuk kejahatan digital yang meliputi pencurian identitas, penipuan, pornografi, bahkan bullying dimana serangan mental. tanpa menimbulkan kontak fisik.

Pertumbuhan teknologi elektronik sejalan dengan peningkatan jumlah kasus kriminal, mulai dari yang tradisional berubah menjadi sebuah kejahatan di mana pengetahuan teknologi informasi digunakan untuk keperluan diri sendiri dan orang lain. Pada dasarnya kasus yang menggunakan teknologi informasi bisa digolongkan sebagai kerah putih, karena pelaku kejahatan kerah putih dicirikan oleh orang yang menggunakan kecerdasan dan/atau keahliannya untuk melakukan kejahatan dengan cara yang tidak diketahui oleh pelakunya sendiri dari korban kejahatan[5]. Tindakan yang dilaksanakan dengan menggunakan sebuah alat internet dan computer untuk memanipulasi data untuk keuntungan ilegal.

Saat ini, keterkaitan masyarakat terhadap teknologi informasi semakin besar dan risikonya juga semakin meningkat. Saat ini, semua aspek ekonomi, masyarakat dan pertahanan negara sangat bergantung pada Internet. Didalam perbankan ada kegiatan ekonomi, pemeliharaan, interaksi sosial, pengendalian senjata, dan operasi transportasi yang dimana merupakan bagian integral dari hubungan ini. Dalam hukum pidana Indonesia, kejahatan dunia maya digolongkan sebagai kejahatan khusus, meskipun bagian pokok mungkin sesuai dengan segala syarat hukum pidana[6], tetapi diterapkan dalam sistem baru dari kejahatan itu, jenis. File hukum yang lebih kompleks. Sarana dan prasarana yang dimana merupakan salah satu faktor yang mengajak penegakan hukum atau sarana yang mendukung penegakan hukum, karena aspek aspek tersebut juga ialah sebuah ukuran penegakan hukum dan efektivitas kepolisian. DPR RI mengesahkan Transaksi Elektronik dan UU Informasi[7]. Tuntunan perundang-undangan yang berjalan dari mulai tahun 1999 secara luas dapat dijadikan sebagai data hukum yang bisa meningkatkan pertumbuhan pemusnahan cybercrime dengan bagus. Namun, hukum mempunyai persoalan dalam beberapa unsur, baik dari sisi yang bukan hukum maupun

hukum.

Istilah c*ybercrime* dicetuskan pertama kali oleh William Gibson, yang sudah menulis tentang angka dalam sebuah noveln yang sudah beliau buat yaitu Neuromancer pada tahun 1998[8]. Dimana dalam novelnya berisi sebuah istilah yaitu "cyberspace" yang dimana menggambarkan dunia maya yang berhubungan dengan angka aktivitas komputer dan konsep "*cybercrime*", yang menggambarkan kejahatan yang telah terjadi di dunia maya dan mengintimidasi kedamaian[9]. Indra Safitri menyatakan kalau cybercrime merupakan kejahatan yang melibatkan pemakai teknologi informasi sebagai alat dan mencari lubang keamanan dalam sistem yang digunakan oleh pengguna internet. Sesuai dengan perkembangannya, cybercrime tumbuh dengan cepat dalam bentuk yang berbeda. Keberagaman ini tidak hanya berlaku pada individu aktor, tetapi juga mencakup negara sebagai faktornya. Salah satu jenis kejahatan dunia maya adalah spionase dunia maya. cyber spionage atau ancaman cyber yang mampu dijelaskan dengan menafsirkan istilah cyber dan spionase secara terpisah. Cyber didefinisikan sebagai "dunia siber", yang merupakan wahana bagi kejahatan dan spionase atau spionase adalah upaya individu atau negara untuk mengumpulkan informasi[10]. Objek yang diharapkan oleh pemerintah dan dilakukan oleh orang yang tidak memiliki tugas dengan menggunakan dunia maya atau cyberspace.

Selain jenis serangan yang semakin beragam, pada dasarnya ada empat jenis aktivitas di dunia IT yang sering digolongkan sebagai kejahatan[11]. Yang pertama adalah penyadapan, yaitu penyadapan transmisi yang diantara satu grup dengan grup lain. Seperti yang sudah kita ketahui, di Indonesia misalnya yang beberapa instansi yang berhak melasanakan pengintaian atau penyadapan, seperti Polri , BIN (Badan Intelegen Negara) dan KPK (Komisi Pemberantasan Korupsi). Entitas atau individu yang tidak berwenang untuk melakukannya bisa dituntut kalau mereka terlibat dalam operasi penyadapan. Yang kedua ialah pemutusan, yaitu dimana artinya berupa perlakuan yang dampaknya dapat terhentinya sebuah hubungan antara dua bagian yang seharusnya berkomunikasi[12]. Distributed Denial of Service atau Denial of Service ialah merupakan bagian dari salah satu serangan yang bisa menyebabkan sistem komputer menjadi down. ketiga adalah modifikasi, yaitu. membuat perubahan pada file, konten, atau informasi yang bergerak di prasarana TI tanpa sepengetahuan pengirim/penerima. Website korupsi adalah yang dimana salah satu jenis serangan yang dapat diklasifikasikan dalam kategori ini. Dan yang keempat adalah tipuan yang menipu agar terlihat seperti seseorang telah menerima permintaan interaksi[13].

Badan hukum cybercrime terkhusus di Indonesia sangat dikuasai oleh lima penyebab yaitu mentalisat polisi, hukum, fasilitas, perilaku masyarakat dan budaya[14]. Yang dimana hukum tidak bisa dipenuhi, selalu menyangkut dengan tindakan dan orangnya. Tanpa kepatuhan terhadap , hukum itu sendiri tidak dapat ditegakkan. Instansi kepolisian tidak hanya harus untuk menjalankan sebuah hukum secara cerdas dan professional akan tetapi juga harus mengatasi tersangka kriminal dan bahkan suatu kumpulan masyarakat[15]. Dengan era dan pertumbuhan yang dimana tumbuhnya suatu dunia kriminal terkhusus yang makin meningkat dan meresahkan perkembangan cybercrime, badan penegak hukum seharusnya bisa bekerja lebih keras lagi hal itu dikarenakan badan penegak hukum ialah sebuah lembaga terdepan yang mampu untuk menangani kasus cybercrime[16].

Internet dan Media Sosial

Kehadiran internet dan media sosial tidak hanya memberikan dampak positif bagi kehidupan masyarakat tetapi juga berdampak negatif. Salah satu jenis kejahatan yang sering mengganggu tatanan sosial adalah kekerasan[17]. Kekerasan identik dengan perilaku fisik, tetapi kekerasan pada dasarnya adalah setiap perilaku, baik verbal maupun non-

verbal, oleh seseorang atau sekelompok orang terhadap orang lain atau sekelompok orang, yang menimbulkan efek fisik, emosional yang negatif. dan efek psikologis. mempengaruhi jumlah diantaranya. Kekerasan mengacu pada perbuatan atau ancaman yang melanggar hukum atau merupakan perbuatan nyata yang menimbulkan kerugian harta benda atau fisik, atau perbuatan yang menyebabkan kematian orang[18]. Kekerasan terbagi menjadi dua bagian, yaitu kekerasan fisik dan kekerasan verbal. Namun, hanya sekitar orang yang tidak mengetahui bahwa kekerasan verbal atau verbal ternyata memiliki dampak yang lebih besar daripada kekerasan fisik.

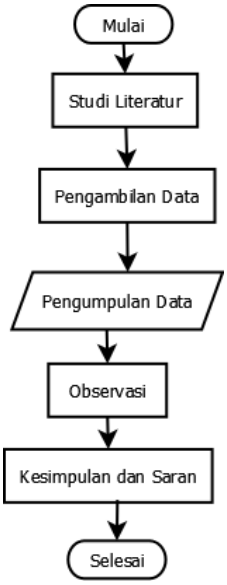
Pesatnya perkembangan teknologi dan media sosial juga menyoroti berbagai bentuk kekerasan seksual di berbagai media sosial, yang dapat dikelompokkan sebagai berikut: a) Cyber-bullying, b) Deceptive training (Cyber), c) Hacking, d) Violation privasi, e) Penyebarluasan foto/video pribadi (malicious distribution), f) porno balas dendam, g) peniruan, h) pencemaran nama baik produk, i) rekrutmen Internet (online). pengantar[19]. Indonesia kini memiliki bentuk terbaru dan alasan penangkapan korban di bawah umur yaitu menggunakan sihir kekanak-kanakan. Kekerasan terhadap anak merupakan tindakan atau perbuatan yang disengaja dan dapat menimbulkan kerugian (baik fisik maupun emosional) pada anak. Merujuk pada definisi organisasi internasional Society for the Prevention of Cruelty to Children atau National Society for the Prevention of Cruelty to Children (NSPCC)[20], pola asuh adalah upaya individu untuk membangun hubungan, kepercayaan dan hubungan emosional dengan seorang anak atau remaja sehingga mereka dapat memanipulasi, mengeksploitasi, dan melecehkan mereka. Pencarian online kini telah menemukan anak[21].

Mengasuh anak dianggap sebagai bentuk kejahatan baru di Indonesia. Pelecehan anak di Indonesia juga dikenal sebagai pelecehan seksual anak di jejaring sosial, meningkat karena permintaan pasar seks global[22]. Tentu saja kejahatan ini dilarang oleh semua hukum di seluruh dunia karena melanggar hak dan dapat berdampak negatif terhadap perkembangan anak, sehingga perlindungan anak harus diperhatikan. Mengasuh anak adalah proses menghubungi anak-anak dengan tujuan mempersiapkan mereka untuk aktivitas seksual[23]. Penjahat menggunakan berbagai teknik untuk mengakses dan mengontrol korbannya. Proses ini membutuhkan keterampilan akses, waktu dan komunikasi dari penulis. Jika pengasuhan ditangani dengan benar, korban secara tidak sadar dengan mudah bekerja sama dengan pelaku. Semakin baik penjahat memilih dan mengetahui korban mereka yang rentan, semakin berhasil perawatan anak tersebut. keterampilan kriminal meliputi memilih korban, mengidentifikasi dan memahami kebutuhan korban, waktu yang diperlukan untuk mendekati, merayu dan mengontrol korban pekerja anak yang menjadi korban pelecehan seksual[24]. Kekerasan seksual adalah segala bentuk pelecehan seksual atau pemaksaan hubungan seksual tanpa persetujuan korban atau ketika korban tidak menginginkannya, dan/atau hubungan seksual dengan cara yang tidak adil atau tidak menyenangkan. korban dan jarak dari kebutuhan seksualnya. Lebih lanjut, pelecehan seksual merupakan bentuk kekerasan yang dapat dilakukan oleh siapa saja, di mana saja dan kapan saja. Perempuan dan anak-anak adalah orang yang dianggap lemah, sehingga memiliki kemungkinan menjadi korban pelecehan seksual. Pelecehan seksual anak adalah setiap hubungan atau interaksi antara anak dan orang dewasa mana anak digunakan sebagai objek untuk kebutuhan pelanggar seks[25].

Metode Penelitian

Penelitian merupakan sebuah proses yang sistematis dan terstruktur untuk memperoleh pengetahuan baru atau memperkuat pemahaman terhadap suatu fenomena. Tahapan awal penelitian dimulai dengan studi literatur, yaitu pengumpulan dan telaah terhadap sumber-sumber yang relevan sebagai dasar teori dan referensi. Selanjutnya

dilakukan pengambilan dan pengumpulan data yang menjadi bahan utama dalam analisis. Observasi juga dilakukan untuk mengamati secara langsung objek atau kondisi yang diteliti. Dengan mengikuti tahapan ini secara berurutan, penelitian dapat berjalan dengan sistematis dan menghasilkan data yang valid. Pendekatan ini memastikan bahwa setiap langkah penelitian saling terkait dan mendukung pencapaian tujuan akhir penelitian.



Gambar 1. Flowchart Penelitian
Sumber: Data Pribadi

Setelah melalui proses pengumpulan data dan observasi, penelitian kemudian sampai pada tahap penyusunan kesimpulan dan saran yang didasarkan pada hasil analisis yang diperoleh. Tahapan ini penting untuk merangkum temuan dan memberikan rekomendasi yang bermanfaat bagi pengembangan ilmu pengetahuan maupun praktik di lapangan. Dengan menjalankan setiap langkah secara disiplin sesuai alur yang telah dirancang, penelitian menjadi lebih terarah dan hasilnya dapat dipertanggungjawabkan. Dengan demikian, penelitian tidak hanya memberikan jawaban atas pertanyaan yang diajukan, tetapi juga memberikan kontribusi yang berarti bagi bidang kajian yang bersangkutan.

Hasil dan Pembahasan

1. Resiko Cyber Crime

Perkembangan pesat teknologi informasi di era digital membawa dampak signifikan terhadap berbagai aspek kehidupan, termasuk munculnya berbagai bentuk kejahatan yang menargetkan kelompok rentan seperti anak-anak. Anak-anak yang tidak selalu berada dalam pengawasan orang tua dan menggunakan teknologi informasi secara bebas sangat rentan menjadi korban kejahatan pengasuhan, baik di lingkungan masyarakat maupun dalam keluarga itu sendiri. Kondisi fisik anak yang relatif lebih lemah dibandingkan dengan orang dewasa, serta ketergantungan mereka yang tinggi pada orang dewasa di sekitarnya, membuat mereka lebih mudah menjadi target kekerasan dan eksploitasi. Selain itu, pengaruh negatif dari lingkungan, seperti penyebaran konten pornografi dalam berbagai bentuk—video, film, gambar—melalui media massa, memberikan dampak buruk yang sangat besar bagi perkembangan anak, terutama di bawah umur. Paparan konten yang tidak sesuai usia tersebut dapat memicu penyimpangan perilaku seksual dan gangguan psikologis yang berkelanjutan. Oleh

karena itu, perlindungan terhadap anak di dunia maya menjadi sebuah kebutuhan yang mendesak untuk mengantisipasi risiko kejahatan siber (cybercrime) yang semakin kompleks.

Dalam konteks dunia maya, internet telah menjadi elemen esensial dalam kehidupan masyarakat modern, bahkan sejak kelahirannya pada pertengahan dekade 1990-an. Internet menciptakan sebuah dunia virtual yang memungkinkan individu dan kelompok berinteraksi, bertukar informasi, serta berkolaborasi dalam berbagai aktivitas sosial dan ekonomi. Dunia maya ini merupakan titik pertemuan antara dunia abstrak dan dunia fisik, sehingga jumlah penggunanya semakin meningkat setiap waktu. Namun, seiring dengan nilai dan manfaat yang besar yang ditawarkan dunia digital, muncul pula berbagai ancaman cyber yang tidak bisa diabaikan. Sama seperti benda berharga di dunia nyata, internet dan data digital menjadi incaran bagi oknum yang berniat melakukan kejahatan. Mereka yang tergiur dengan keuntungan dapat menggunakan cara-cara tidak sah, seperti pencurian identitas, peretasan, atau penyalahgunaan data, yang merugikan individu maupun organisasi.

Serangan siber merupakan manifestasi nyata dari ancaman-ancaman tersebut. Menurut Konvensi Budapest tentang kejahatan dunia maya, serangan tersebut dapat dikategorikan ke dalam beberapa jenis, antara lain penggunaan teknologi informasi sebagai senjata dalam melakukan kejahatan, manipulasi transaksi digital, gangguan sistem jaringan, serta penyebaran perangkat lunak berbahaya seperti virus komputer. Serangan ini tidak hanya merugikan secara materi, tetapi juga dapat mengganggu sistem komunikasi dan operasional institusi penting, bahkan membahayakan privasi dan keamanan data pengguna internet. Perkembangan teknologi komunikasi dan informasi yang semakin canggih juga memungkinkan munculnya perangkat otomatis yang mampu melakukan intrusi tanpa pengawasan manusia, sehingga meningkatkan kompleksitas dan dampak negatif kejahatan siber.

Dalam menanggapi fenomena tersebut, berbagai negara termasuk Indonesia berupaya mengembangkan regulasi hukum yang mampu mengatur dan menjerat pelaku kejahatan di dunia maya. Indonesia sendiri secara resmi mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang menjadi dasar hukum utama dalam penanganan tindak pidana di ranah digital. UU ITE memberikan kerangka hukum yang memungkinkan penerapan sanksi pidana dan perdata terhadap berbagai bentuk kejahatan siber, mulai dari penyebaran informasi palsu, pencurian data, hingga serangan terhadap sistem elektronik. Meskipun langkah ini terbilang terlambat jika dibandingkan dengan negara lain, keberadaan UU ITE menjadi tonggak penting dalam memperkuat keamanan dunia maya di Indonesia, sekaligus melindungi masyarakat dari dampak negatif kemajuan teknologi informasi. Dengan demikian, perlindungan terhadap anak dan masyarakat luas di dunia maya harus didukung oleh pemahaman yang baik tentang risiko kejahatan cyber serta penerapan teknologi dan regulasi yang tepat untuk menciptakan lingkungan digital yang aman dan kondusif.

2. Kebijakan Keamanan *cyber* di Indonesia

Strategi keamanan siber di Indonesia telah mengalami perkembangan signifikan sejak tahun 2007, diawali dengan penerbitan Peraturan Menteri Komunikasi dan Informatika (KOMINFO) No.26/PER/M.Kominfo/5/2007 yang mengatur keamanan penggunaan protokol internet dalam jaringan telekomunikasi berbasis teknologi informasi. Peraturan ini kemudian diperbarui menjadi Peraturan KOMINFO No.16/PER/M.KOMINFO/10/2010 dan kembali mengalami revisi dengan keluarnya Peraturan Menteri Perhubungan dan KOMINFO No.29/PER/M.KOMINFO/12/2010,

yang menunjukkan upaya pemerintah dalam memperkuat kepastian hukum di bidang keamanan siber. Di samping regulasi, pengembangan tindakan teknis dan prosedural juga menjadi elemen penting dalam membangun sistem keamanan yang kokoh. Namun, dalam pelaksanaannya, masih terdapat beberapa tantangan yang perlu diatasi, seperti kurangnya pemahaman yang memadai dari pihak pemerintah dan pengelola keamanan mengenai batasan penggunaan teknologi siber, perlunya sistem keamanan yang handal terutama bagi layanan server yang beroperasi di luar negeri, serta aspek legalitas dalam menangani serangan di dunia maya yang harus diatur secara jelas agar tindakan penegakan hukum dapat berjalan efektif. Untuk mendukung aspek organisasi dalam menghadapi kejahatan dunia maya, Kementerian Pertahanan Indonesia telah membentuk Pusat Operasi Pertahanan Siber yang berfungsi sebagai wadah utama dalam melindungi pertahanan dan keamanan negara di ranah siber. Pusat operasi ini berperan pada tingkat kebijakan keamanan siber nasional dengan tujuan menyusun sistem keamanan dan pertahanan yang komprehensif, mencakup perlindungan terhadap masyarakat, sumber daya nasional, dan wilayah kedaulatan negara dari ancaman kejahatan siber yang dapat merusak keutuhan dan kedaulatan nasional. Selain itu, kerjasama internasional menjadi salah satu pilar utama dalam memerangi kejahatan siber yang bersifat lintas batas negara. Indonesia aktif berpartisipasi dalam berbagai organisasi regional dan internasional, seperti ASEAN Network Security Action Council dan International Telecommunication Union (ITU), serta berkontribusi sebagai anggota dan pengarah di Asian Committee Pacific Computer Crisis Response Team. Melalui kolaborasi ini, Indonesia juga melakukan perjanjian bilateral dengan negara-negara seperti Inggris dan Jepang untuk memperkuat kerja sama dalam menghadapi tantangan keamanan siber. Partisipasi Indonesia dalam Global Cyber Security Action Plan yang diprakarsai pada Hari Masyarakat Telekomunikasi dan Informasi Sedunia tahun 2007 menegaskan komitmen negara dalam mengembangkan solusi dan strategi bersama untuk meningkatkan keamanan, kepercayaan, dan perlindungan di dunia informasi. Secara keseluruhan, kepastian hukum, tindakan teknis dan prosedural, struktur organisasi khusus, serta kerja sama internasional menjadi fondasi utama dalam membangun sistem keamanan siber yang efektif dan berkelanjutan di Indonesia guna melindungi masyarakat dan kepentingan nasional dari ancaman kejahatan dunia maya.

Kesimpulan

Kejahatan dunia maya di Indonesia menimbulkan dampak serius, sebagaimana tercermin dari laporan CIA yang mencatat berbagai kerusakan akibat eksploitasi siber. Penanganan kejahatan ini membutuhkan pendekatan holistik karena berbeda dengan kejahatan konvensional. Penelitian ini menyoroti risiko kejahatan siber dan upaya pemerintah dalam meminimalisirnya. Perkembangan teknologi informasi yang pesat menyebabkan anak-anak menjadi kelompok rentan terhadap kejahatan, terutama karena kurangnya pengawasan dan pengaruh negatif konten pornografi di media massa. Menanggapi hal ini, pemerintah Indonesia telah menginisiasi berbagai regulasi keamanan siber sejak 2007, seperti Peraturan Menteri KOMINFO No.26/PER/M.Kominfo/5/2007 yang kemudian diperbarui dengan Peraturan KOMINFO No.16/PER/M.KOMINFO/10/2010 dan Peraturan Menteri Perhubungan serta KOMINFO No.29/PER/M.KOMINFO/12/2010. Kebijakan ini menjadi landasan penting dalam memperkuat keamanan siber nasional untuk melindungi masyarakat dan menjaga kedaulatan negara di era digital.

Daftar Pustaka

[1] M. Danuri and Suharnawi, "Trend Cyber Crime Dan Teknologi Informasi Di Indonesia," Inf. Komput. Akunt. dan Manaj., vol. 13, no. 2, pp. 55–65, 2017.

[2] B. Hartono and R. A. Hapsari, "Mutual Legal Assistance Pada pemberantasan Cyber Crime Lintas Yurisdiksi di Indonesia," Sasi, vol. 25, no. 1, p. 59, 2019, doi: 10.47268/sasi.v25i1.136.

[3] H. Ardiyanti, "Cyber-Security Dan Tantangan Pengembangannya Di Indonesia," pp. 95–110, 1986.

[4] F. Diapoldo and S. S. Kom, "KEAMANAN".

[5] Setiyawan, "Uuite Dalam Melindungi Hak Cipta Sebagai Hak Atas Kekayaan Intelektual (Hki) Dari Cybercrime," J. Chem. Inf. Model., vol. 53, no. 9, pp. 1689–1699, 2013.

[6] F. N. Latifahi, I. Mawardi, and B. Wardhana, "Ancaman Pencurian Data (Phishing) Di Tengah Trend Pengguna Fintech Pada Pandemic Covid-19," Islam. Bank. Financ. J., vol. 6, no. 1, pp. 73–85, 2022, doi: 10.21070/perisai.v6i1.

[7] S. Suyitno, "Implementasi Manajemen Resiko dalam Peningkatan Efektivitas Pembelajaran di Sekolah Menengah Kejuruan," Edukatif J. Ilmu Pendidik., vol. 4, no. 1, pp. 141–153, 2021, doi: 10.31004/edukatif.v4i1.1768.

[8] A. Irawati, H. B. Fadholi, A. N. Alamsyah, D. P. Dwipayana, and M. Muslih, "Proceeding of Conference on Law and Social Studies URGENSI CYBER LAW DALAM KEHIDUPAN MASYARAKAT INDONESIA DI ERA DIGITAL," Pros. Conf. Law Soc. Stud., pp. 1–15, 2021, [Online]. Available: http://prosiding.unipma.ac.id/index.php/COLaS

[9] S. Sugiarto and R. Qurratulaini, "Potensi Kriminal Cyber Crime pada Meme: Sebuah Kajian Linguistik Forensik," Deiksis J. Pendidik. Bhs. dan Sastra Indones., vol. 7, no. 1, p. 46, 2020, doi: 10.33603/deiksis.v7i1.2495.

[10] C. Handoko, "Kedudukan Alat Bukti Digital Dalam Pembuktian Cybercrime Di Pengadilan," J. Jurisprud., vol. 6, no. 1, p. 1, 2017, doi: 10.23917/jurisprudence.v6i1.2992.

[11] Hamdan Mustameer, "Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0," J. Yustika Media Huk. Dan Keadilan, vol. 25, no. 01, pp. 40–53, 2022, doi: 10.24123/yustika.v25i01.5090.

[12] M. Desa, P. Serai, and L. Perspektif, "NUSANTARA : Jurnal Ilmu Pengetahuan Sosial ُ ى ل ْ ّ َ تلا و َ ع َ لا و َ او ُ ن وا ِ ب ِ لا َ ت و َ ى و َ ق َ ر َ ع الل ّ َ َ او ْ ن, وا ِ ث ل ا ى َ ل ع َ ّ َ ن َ َ ت َ د ُ ع لا و َ م َ ع ْ ُ دي ِ د ش ب ِ ا َ ق ع," vol. 9, no. 4, pp. 1483–1490, 2022.

[13] D. Wahyudi, "Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia," J. Ilmu Huk. Jambi, vol. 4, no. 1, p. 43295, 2013.

[14] I. P. N. Andaru, "Cyber Child Grooming sebagai Bentuk Kekerasan Berbasis Gender Online di Era Pandemi," J. Wan. dan Kel., vol. 2, no. 1, pp. 41–51, 2021, doi: 10.22146/jwk.2242.

[15] L. Luo and Z. Wang, "Literature Review of Innovation and Entrepreneurship Management," Proc. 2022 7th Int. Conf. Financ. Innov. Econ. Dev. (ICFIED 2022), vol. 648, no. Icfied, pp. 2623–2629, 2022, doi: 10.2991/aebmr.k.220307.427.

[16] M. Risal, "Aspek menjaga dan melindungi dunia maya".

[17] A. Syaputra, "Penilaian IT Governance dalam Manajemen Risiko IT Menggunakan Metode Quantitative dan Qualitative Risk Analysis Assessment of IT Governance in IT Risk Management Using Quantitative Methods and Qualitative Risk Analysis," vol. 12, no. April, pp. 63–73, 2022.

[18] Suparyanto dan Rosad (2015, "済無No Title No Title No Title," Suparyanto dan Rosad (2015, vol. 5, no. 3, pp. 248–253, 2020.

[19] S. Saifulloh, S. Anardani, and Q. R. Pratama, "Edukasi penggunaan internet sehat untuk mengenali berita Hoax bagi pemuda Dusun Pepe Desa Pajaran Kab. Madiun," SOROT J. Pengabdi. Kpd. Masy., vol. 1, no. 2, pp. 29–32, 2022, doi: 10.32699/sorot.v1i2.3010.
[20] D. Daryono and B. Sugiantoro, "Pengembangan Framework Pelaporan Cyber Crime," JISKA (Jurnal Inform. Sunan Kalijaga), vol. 1, no. 3, pp. 133–147, 2017, doi: 10.14421/jiska.2017.13-05.
[21] I. B. Mewengkang, R. N. Warong, and M. Kuntag, "Kajian Yuridis Cyber Crime Penanggulangan Dan Penegakan Hukumnya," Lex Crim., vol. 10, no. 5, pp. 26–35, 2021.
[22] Y. M. Putra, U. M. Buana, E. Kurniawan, and U. M. Buana, "Informasi Pada Pt . Jasaneka Bina Management Disusun Oleh :," no. May, 2021.
[23] K. D. Kurniawan and D. R. I. Hapsari, "Kejahatan Dunia Maya Pada Sektor Perbankan Di Indonesia: Analisa Perlindungan Hukum Terhadap Nasabah," Pleno Jure, vol. 10, no. 2, pp. 122–133, 2021, doi: 10.37541/plenojure.v10i2.590.
[24] S. Jannah and M. Naufal, "Penegakan Hukum Cyber Ditinjau dari Hukum Positif," vol. XII, no. 1, pp. 69–84.
[25] A. Marsehan, M. I. Herdiansyah, A. H. Mirza, and D. Antoni, "Penilaian Resiko Kejahatan Illegal Content Menggunakan Framework Nist 800-30," Paradig. - J. Komput. dan Inform., vol. 22, no. 2, pp. 215–224, 2020, doi: 10.31294/p.v22i2.8913.