DOI https://doi.org/10.33701/jk.v5i1.3208
P-ISSN: 2656-2383; E-ISSN: 2656-0925
Available Online at: http://ejournal.ipdn.ac.id/konstituen
Fakultas Perlindungan Masyarakat
Institut Pemerintahan Dalam Negeri

ANCAMAN *CYBERCRIME* DI INDONESIA
Sebuah Tinjauan Pustaka Sistematis

Rian Dwi Hapsari[1]*, Kuncoro Galih Pambayun[2]
rian_20@ipdn.ac.id, Institut Pemerintahan Dalam Negeri[1]
pambayun@ipdn.ac.id, Institut Pemerintahan Dalam Negeri[2]
Received: 10-03-2023, Accepted: 16-10-2023; Published Online: 26-10-2023

Corresponding Author

Abstrak

Perkembangan teknologi digital telah meningkatkan ancaman cybercrime secara signifikan, hingga berdampak terhadap pencurian identitas, kehilangan pekerjaan, dan gangguan infrastruktur kritis. Sementara itu pelaku *cybercrime* terus mengembangkan teknik dan strategi baru dalam melakukan tindakan kejahatan. Tujuan penelitian ini adalah untuk mendeskripsikan sejauhmana ancaman *cybercrime* yang terjadi di Indonesia. Penelitian ini menggunakan metode kajian *literatur review*, dilakukan dengan cara menelaah dan menganalisis literatur berkaitan dengan *cybercrime* di Indonesia. Temuan penelitian menunjukkan bahwa telah terjadinya evolusi publikasi tentang *cybercrime* di Indonesia dari fokus awal pada pemahaman dan regulasi hingga penekanan yang lebih besar pada teknologi, ancaman terbaru, dan dampaknya terhadap berbagai aspek kehidupan dan bisnis. Serangan *malware, denial of service (DoS), distributed denial of service (DDoS), dan phishing* menjadi ancaman yang sering terjadi, penyebabnya yakni kurangnya kesadaran dan edukasi tentang keamanan siber serta minimnya penegakan hukum kejahatan dunia maya. Penulis menyimpulkan bahwa ancaman *cybercrime* di Indonesia sekarang ini tergolong serius (sangat berbahaya) karena berpotensi sangat tinggi menimbulkan permasalahan nasional. Adapun upaya yang dapat dilakukan adalah dengan memperkuat penegakan hukum terhadap *cybercrime* dan meningkatkan edukasi terhadap masyarakat tentang cara melindungi diri dari kejahatan dunia maya.

Kata kunci: *Cybercrime*; Ancaman *Cybercrime*; *Literatur review*

Abstract

The advancement of digital technology has significantly increased the threat of cybercrime, leading to issues such as identity theft, job loss, and disruptions to critical infrastructure. Meanwhile, cybercriminals continue to develop new techniques and strategies in committing their criminal acts. The purpose to describe the extent of cybercrime threats in Indonesia. This study employs a literature review method, which involves examining and analyzing literature related to cybercrime in Indonesia. The findings indicate that there has been an evolution in publications concerning cybercrime in Indonesia, shifting from an initial focus on understanding and regulations to a greater emphasis on technology, emerging threats, and their impact on various aspects of life and business. Common cyber threats in Indonesia include malware attacks, denial of service (DoS), distributed denial of service (DDoS), and phishing. These threats are often exacerbated by a lack of awareness and education about cybersecurity and limited enforcement of cybercrime laws. In conclusion, cybercrime threats in Indonesia are currently considered serious and highly dangerous due to their potential to create national issues. Efforts to address this issue should include strengthening law enforcement against cybercrime and enhancing public education on protecting oneself from online threats.

Keywords: *Cybercrime; Cybercrime Threats; Literature Review*

PENDAHULUAN

Penggunaan internet di Indonesia terus meningkat dari tahun ke tahun seiring dengan semakin luasnya akses internet dan adopsi teknologi digital di berbagai sektor. Berdasarkan data yang dirilis oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2022, jumlah pengguna internet di Indonesia mencapai sekitar 210 juta orang atau sekitar 78,4% dari total populasi Indonesia yang mencapai 267,7 juta jiwa (Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), 2022). Penggunaan internet di Indonesia sangat beragam, mulai dari penggunaan untuk keperluan bisnis, pendidikan, hiburan, hingga komunikasi. Beberapa aktivitas yang paling umum dilakukan oleh pengguna internet di Indonesia yaitu untuk mengakses media sosial Sebagian besar pengguna internet di Indonesia menggunakan platform media sosial seperti *Facebook*, *Instagram*, *Twitter*, dan *YouTube* untuk berinteraksi dengan teman dan keluarga, mencari informasi, dan mengikuti konten yang diminati. Selain itu, email dan aplikasi chatting seperti *WhatsApp, Line*, dan *Telegram* digunakan untuk berkomunikasi dengan teman, keluarga, dan rekan kerja. *Browsing* atau pencarian informasi di internet juga menjadi kegiatan yang sangat umum dilakukan oleh masyarakat di Indonesia. Internet memudahkan akses informasi, komunikasi dengan orang lain, dan memfasilitasi kolaborasi dan inovasi (Carr, 2014). Setiap hari masyarakat juga melakukan belanja *online* melalui internet (Hermawansyah, 2022). Meskipun mempermudah akan tetapi tetap harus kritis dan bijak dalam memanfaatkannya (Lynch, 2016).

Penggunaan *e-commerce* semakin populer di Indonesia, di mana pengguna internet dapat membeli berbagai produk secara *online* melalui platform seperti Tokopedia, Bukalapak, Shopee, dan lainnya (Akbar & Alam, 2020). Aktivitas Gaming pun tidak kalah populer di kalangan pengguna internet di Indonesia, terutama bagi kalangan muda. Konten internet yang sering diakses oleh pengguna menurut hasil survey oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dari 7.568 koresponden yang dirilis Bulan Juni Tahun 2022 yaitu 89,15% mengakses sosial media, 73, 86% mengakses aplikasi chatting, 21,26% melakukan shopping *online*, mengakses game *online* 14,23%, *browsing* informasi 11,98%, mengakses transportasi *online* 9,27%, mengakses music *online* 8,49%, mengakses email 7,32%, mengakses aplikasi video/radio *online* 4,79%, melakukan meeting *online* 4,05%, belajar *online* 2,81% dan mengakses aplikasi dompet elektronik 1,37% (Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), 2022)

Berdasarkan laporan *We Are Social* dan *Hootsuite* pada tahun 2022, waktu orang Indonesia mengakses media digital cenderung bervariasi tergantung pada jenis media digital yang mereka gunakan (Aji, 2022). Mayoritas pengguna internet di Indonesia menghabiskan waktu sekitar 8 jam 36 menit dalam penggunaan internet, 2 jam 50 menit dalam menonton televisi, 3 jam 17 menit untuk menggunakan media sosial, 1 jam 30 menit untuk mendengarkan musik, dan 1 jam 19 menit untuk bermain game (We Are Social, 2021). Pola penggunaan media sosial cenderung sepanjang hari, dengan puncak penggunaan pada sore hingga malam. Pengguna YouTube cenderung mengaksesnya pada sore hingga malam hari, sementara pengguna e-commerce aktif pada pagi dan malam hari. Pola waktu penggunaan media digital dapat bervariasi berdasarkan faktor-faktor seperti usia, pekerjaan, dan pendidikan. Misalnya, remaja cenderung lebih aktif pada malam hari, sementara pekerja kantoran lebih sering mengaksesnya selama istirahat kerja (We Are Social, 2021).

Pemerintah Indonesia telah memberikan dukungan untuk mendorong akses internet di Indonesia melalui beberapa program dan kebijakan. Pemerintah Indonesia juga terus mendorong akses internet dan teknologi digital ke seluruh wilayah Indonesia melalui program-program seperti Gerakan Nasional 1000 Startup Digital yang merupakan program yang diluncurkan oleh Kementerian Komunikasi dan Informatika (Kominfo) pada tahun 2016. Program ini bertujuan untuk mendorong pertumbuhan ekonomi digital dan inovasi di Indonesia dengan menumbuhkan 1000 startup digital yang sukses dan berdampak positif pada ekonomi. Program ini memberikan dukungan dalam bentuk pelatihan, pengembangan bisnis, akses ke pasar, pembiayaan, dan infrastruktur teknologi (Chusumastuti, 2020). Selanjutnya, Program Palapa Ring. Program ini bertujuan untuk membangun infrastruktur jaringan serat optik nasional yang melingkupi seluruh wilayah Indonesia. Dengan infrastruktur ini, diharapkan dapat meningkatkan akses internet di seluruh wilayah Indonesia, termasuk di daerah terpencil. Program Palapa Ring terdiri dari tiga paket proyek yaitu Palapa Ring Barat, Palapa Ring Tengah, dan Palapa Ring Timur yang terkoneksi melalui jalur laut dan darat. Palapa Ring Barat menghubungkan Sumatra, Jawa, Kalimantan, dan Nusa Tenggara Barat, Palapa Ring Tengah menghubungkan Nusa Tenggara Timur, Sulawesi, dan Maluku, sementara Palapa Ring Timur menghubungkan Maluku Utara, Papua Barat, dan Papua (Susanti & Juwono, 2019).

Selain itu pemerintah telah memberikan kebijakan bebas pajak untuk perusahaan yang berinvestasi di sektor telekomunikasi dan teknologi informasi. Kebijakan ini diharapkan dapat mendorong investasi dan perkembangan industri teknologi informasi di Indonesia. Kebijakan bebas pajak tersebut berlaku untuk perusahaan yang melakukan investasi pada proyek-proyek strategis di bidang teknologi informasi dan telekomunikasi, seperti pembangunan infrastruktur jaringan broadband, pengembangan perangkat lunak, riset dan pengembangan, dan pengembangan pusat data. Dengan memberikan insentif pajak kepada perusahaan-perusahaan tersebut, diharapkan mereka akan lebih tertarik untuk berinvestasi di Indonesia dan membantu meningkatkan pertumbuhan industri teknologi informasi di Indonesia (Indrajit, 2000). Ada juga program *WiFi*.id, program ini merupakan layanan internet gratis dari pemerintah yang tersedia di sejumlah tempat umum seperti bandara, stasiun, dan pusat perbelanjaan. Layanan ini diharapkan dapat memberikan akses internet yang mudah dan terjangkau bagi masyarakat. Layanan *WiFi*.id tersedia secara gratis bagi seluruh pengguna yang memiliki akun *WiFi*.id dan dapat diakses di seluruh wilayah Indonesia. Pengguna hanya perlu memilih jaringan *WiFi*.id yang tersedia di lokasi yang dituju dan memasukkan username dan *password* yang telah didaftarkan untuk mengakses layanan internet gratis. Program *WiFi*.id telah memberikan dampak positif dalam meningkatkan akses internet bagi masyarakat Indonesia, terutama di daerah-daerah yang sulit dijangkau oleh jaringan internet. Selain itu, program ini juga membantu meningkatkan produktivitas dan akses informasi bagi masyarakat serta mendukung pengembangan ekonomi digital di Indonesia (Purwadi & Calam, 2020). Masih ada beberapa program dan kebijakan yang disusun oleh pemerintah agar masyarakat melek internet seperti program desa digital, kebijakan penghapusan roaming internasional dan lainnya.

Teknologi digital yang berkembang pesat memiliki dampak positif dalam hal akses informasi, keterlibatan sosial, dan pemberdayaan ekonomi. Akan tetapi juga berisiko terhadap penyebaran informasi palsu dan ketergantungan pada teknologi. Perkembangan teknologi digital juga telah meningkatkan ancaman *cybercrime* secara signifikan, termasuk

serangan *malware*, *hacking*, dan pencurian data pribadi. Serangan *cybercrime* juga berdampak pada pencurian identitas, kehilangan pekerjaan, dan gangguan terhadap infrastruktur kritis. Masyarakat pada umumnya kurang sadar akan risiko *cybercrime* dan tidak memahami cara melindungi diri mereka sendiri secara efektif. Hukum dan regulasi seputar *cybercrime* juga terus berubah-ubah dalam ketidakpastian. Sementara itu pelaku *cybercrime* terus mengembangkan teknik dan strategi baru. Oleh karenanya penelitian ini penting untuk dilakukan untuk memahami perkembangan terkini dalam dunia *cybercrime*.

Penelitian berkaitan dengan ancaman *cybercrime* telah banyak dilakukan, misalnya saja penelitian oleh Hartati dan Muhammad melalui metode kualitatif deskriptif untuk menganalisis dampak kejahatan dunia maya di Indonesia dan peraturan dengan interkorelasi yang sangat tinggi (Hartati & Muhammad, 2023), penelitian oleh Soesanto et al. terkait keamanan data pribadi dalam sistem pembayaran via OVO terhadap ancaman dan pengelabuan (*cybercrime*) (Soesanto et al., 2023). Selanjutnya penelitian oleh Irfan et al. tentang ancaman *cybercrime* dan peran *cybersecurity* terkhusus pada bidang e-*commerce* yang menggunakan metode sama dengan yang dilakukan peneliti menemukan bahwa perlunya penanganan kejahatan siber pada e-*commerce* harus yang dilakukan secara kolektif oleh pelanggan dan perusahaan e-*commerce* (Irfan et al., 2023). Penelitian terakhir oleh Subandi et al tentang peningkatan keamanan pada simple network time protocol (SNTP) untuk mendeteksi *cybercrime* di dalam aktivitas jaringan yang menemukan bahwa perlunya migrasi *software sophos* ke *trend Micro* (Subandi et al., 2023). Dari beberapa penelitian sebelumya, penelitian ini tergolong baru dimana penelitian terkait ancaman *cybercrime* di Indonesia dilakukan dengan memilih publikasi nasional maupun internasional yang dianalisis berdasarkan tinjauan secara sistematis.

METODE

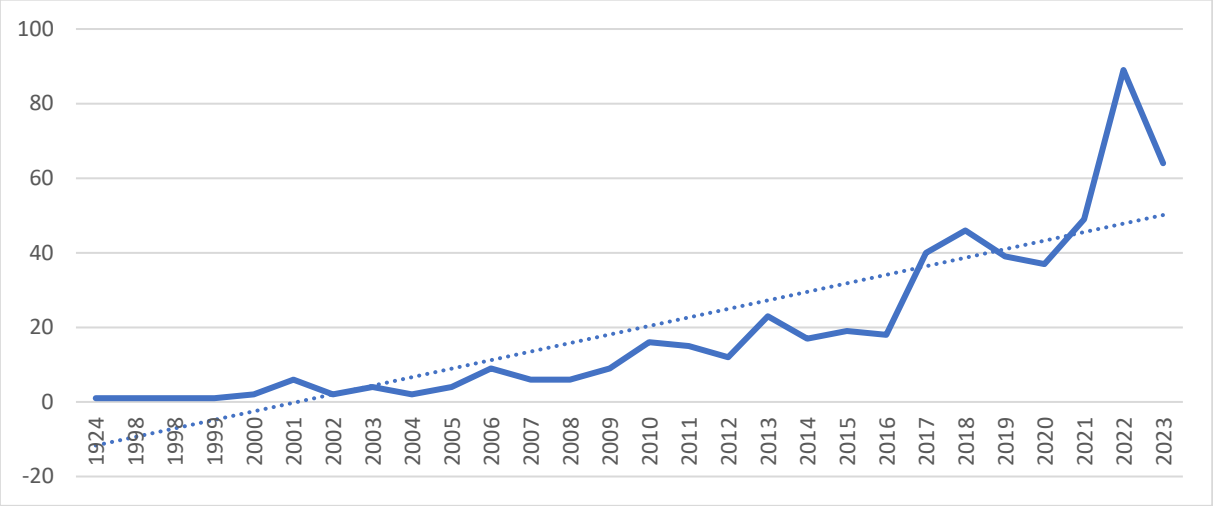
Penelitian ini menggunakan metode *literatur review*. Metodologi *literatur review* dilakukan dengan cara menelaah dan menganalisis literatur atau karya tulis yang berkaitan dengan topik atau masalah yang akan diteliti. Metode ini digunakan untuk memperoleh pemahaman yang mendalam tentang topik tertentu, menganalisis kesimpulan yang diambil dari penelitian terdahulu, dan menyusun kerangka teoretis yang kuat untuk penelitian yang akan dilakukan (Fink, 2019). Setelah peneliti menentukan topik penelitian, selanjutnya mencari literatur yang berkaitan dengan topik penelitian dari berbagai sumber seperti jurnal, buku, artikel, dan dokumen *online*, dalam hal ini penulis membatasi topik penelitian berkaitan dengan *cybercrime* yang terdapat pada database *Google Scholar*. Pemilihan database *Google Scholar* lebih dikarenakan karena kemudahan open akses terhadap artikel yang dapat dilakukan oleh siapa saja untuk mempermudah pengumpulan data. Penulis selanjutnya membaca dan menelaah literatur yang sudah terkumpul, mencatat informasi penting, serta mengorganisasi data secara sistematis. Lalu menganalisis data dari literatur yang sudah terkumpul dan membuat sintesis atau rangkuman dari temuan-temuan yang ditemukan. Pada tahap terakhir, penulis menulis laporan hasil penelitian dengan memasukkan kesimpulan dari analisis yang telah dilakukan. Penulis memilih metode *literatur review* karena memiliki kelebihan yaitu waktu dan biaya yang relatif murah, dapat mengakses banyak sumber informasi dari berbagai disiplin ilmu, serta dapat digunakan sebagai bahan referensi dalam penulisan karya ilmiah.

HASIL DAN PEMBAHASAN

A. Hasil Pencarian Artikel Bertema *Cybercrime* di Indonesia

Pencarian di *Google Scholar* dengan kata kunci "*cybercrime*" dan "Indonesia" menghasilkan 581 artikel, dengan artikel tertua yang diterbitkan pada tahun 1924. Selanjutnya, dari hasil tersebut dilakukan seleksi artikel yang sesuai dengan database *online* yang bereputasi, seperti *Academic Search Complete, Wiley Online Library, Taylor & Francis, Springer, IGI Global, IEEE Xplore, Hein Online, Emerald, Elsevier, Cybercrime Journal, Atlantis-press*, dan *Proquest*. Perkembangan jumlah artikel yang relevan dengan topik "*cybercrime*" di Indonesia dari tahun 1924 hingga 2023 dapat dilihat dari grafik frekuensi artikel berdasarkan tahun terbit berikut.

Grafik 1. Frekuensi Artikel Berdasarkan Tahun Terbit



Sumber: Data Penelitian 2023

Grafik 1 menunjukkan bahwa jumlah artikel yang relevan dengan topik "*cybercrime*" di Indonesia mengalami peningkatan yang signifikan seiring berjalannya waktu. Tren ini semakin kuat pada tahun 2010-an dan 2020-an. Terdapat titik balik pada tahun 1999, ketika jumlah artikel yang relevan mulai meningkat. Mungkin ada peristiwa atau perkembangan penting terkait dengan *cybercrime* di Indonesia pada tahun tersebut yang menjadi pemicu peningkatan ini. Jumlah artikel mencapai puncaknya pada tahun 2022 dengan 89 artikel. Ini mungkin mencerminkan peningkatan kesadaran dan minat terhadap isu *cybercrime* di Indonesia. Jumlah artikel yang terus bertambah dari tahun ke tahun juga mencerminkan peran aktif akademisi dan peneliti dalam memahami, mengidentifikasi, dan memecahkan masalah terkait *cybercrime* di Indonesia. Data tahun 2023 yang tercatat sebanyak 64 artikel menunjukkan bahwa penelitian tentang topik ini masih berlanjut dan relevan. Hal ini menekankan pentingnya mengikuti perkembangan terkini dalam bidang *cybercrime*. Analisis ini memberikan gambaran tentang bagaimana topik "*cybercrime*" di Indonesia telah berkembang seiring waktu dan masih menjadi isu yang signifikan dan menarik perhatian para peneliti.

Berdasarkan hasil pemilihan artikel tersebut, penulis memilih sejumlah 81 artikel yang relevan dengan topik, berasal dari berbagai sumber database *online* bereputasi, dengan beragam tahun terbit, metode penelitian yang digunakan, serta subtopik yang membahas tentang *cybercrime* di Indonesia, dimana tergambar pada Tabel 1 berikut.

Tabel 1. Klasifikasi Artikel Dipilih Berdasarkan Sumber *Online*

Sumber *Online*	**Jumlah**
Academic Search Complete	3
Wiley *Online* Library	2
Taylor & Francis	4
Springer	25
IGI Global	4
IEEE Xplore	6
Hein *Online*	9
Emerald	5
Elsevier	6
***Cybercrime* Journal**	9
Atlantis-press	5
Proquest	3
TOTAL	81

Sumber: Data Penelitian 2023

Berdasarkan Tabel 1 dapat tergambar bahwa Springer menjadi sumber utama artikel terkait "*cybercrime*" di Indonesia dengan 25 artikel, menunjukkan bahwa banyak penelitian tentang topik ini dapat ditemukan di platform ini. "*Cybercrime* Journal" juga menjadi sumber yang signifikan dengan 9 artikel, menunjukkan bahwa jurnal ini memiliki fokus khusus pada topik "*cybercrime*."Data menunjukkan bahwa artikel terkait "*cybercrime*" dapat ditemukan di berbagai sumber *online* terkemuka, seperti IEEE Xplore, Hein *Online*, Taylor & Francis, dan Elsevier. Ini menunjukkan keragaman sumber informasi yang tersedia untuk penelitian tentang topik ini. Beberapa sumber, seperti Academic Search Complete dan Proquest, memiliki jumlah artikel yang lebih sedikit (3 artikel masing-masing). Meskipun demikian, mereka masih menyumbang informasi yang berguna untuk penelitian. Total keseluruhan artikel yang ditemukan dari semua sumber adalah 81 artikel. Ini mencerminkan jumlah yang signifikan dan menunjukkan minat yang kuat dalam topik "*cybercrime*" di Indonesia. Analisis data ini memberikan gambaran tentang sebaran dan dominasi artikel berdasarkan sumber *online*

Berdasarkan tema penelitian yang penulis teliti, dapat kita identifikasi beberapa kelompok topik atau fokus utama yang berkaitan dengan masalah *cybercrime* di Indonesia, dan dapat dipetakan berdasarkan tahun publikasinya sebagai berikut.

Tabel 2. Tema Penelitian Berdasarkan Periode Penelitian Tentang *Cybercrime* di Indonesia pada Periode Sebelum Tahun 2010 dan Periode Setelah Tahun 2010

Tahun	**Fokus utama penelitian *cybercrime* di Indonesia**
2010-Sekarang	ancaman dan keamanan data, peran teknologi untuk tindakan preventif, kerjasama internasional, dampak terhadap bisnis, perlindungan korban, literasi digital, keamanan dalam perilaku pembelian, internet banking, *cyberbullying*, pencurian dan penyalahgunaan data, perkembangan teknologi forensik digital, penyalahgunaan telepon seluler dan media sosial, keamanan nasional, teknologi informasi.

Sebelum 2010	pengaruh dan implikasi *cybercrime*, *cybercrime* dalam konteks global, perlawanan terhadap *cybercrime*, pengaturan hukum, penegakan hukum, aspek sosial dan pendidikan, kebijakan *cybercrime*.

Sumber: Data Penelitian 2023

Berdasarkan Tabel 2 dapat dijelaskan bahwa penelitian berkaitan dengan tema besar *cybercrime* di Indonesia pada periode sebelum tahun 2010 antara lain berfokus pada pengaruh dan implikasi *cybercrime*, menunjukkan ketertarikan awal dalam memahami dampaknya. Penelitian mencakup isu-isu global terkait *cybercrime* juga menunjukkan bahwa *cybercrime* telah diakui sebagai masalah global. Terdapat penekanan pada aspek perlawanan dan penegakan hukum, menunjukkan upaya awal untuk mengatasi *cybercrime* dari sudut pandang hukum dan penegakan hukum. Aspek sosial dan pendidikan juga menjadi perhatian, dimana hal ini menunjukkan kesadaran akan pentingnya literasi digital dan pendidikan terkait keamanan siber. Beberapa penelitian lainnya juga membahas terkait kebijakan *cybercrime*, menyoroti upaya awal dalam mengembangkan kerangka regulasi.

Adapun pada Periode yang lebih modern tahun 2010-Sekarang (periode terkini) menunjukkan bahwa terjadinya pergeseran fokus utama penelitian ke ancaman dan keamanan data, menunjukkan bahwa perkembangan teknologi telah meningkatkan kompleksitas kejahatan siber. Penelitian juga lebih memusatkan perhatian pada peran teknologi untuk tindakan preventif, menunjukkan pemahaman bahwa teknologi dapat digunakan sebagai alat untuk mencegah *cybercrime*. Terdapat peningkatan kerjasama internasional dalam penelitian, yang mencerminkan sifat lintas-batas *cybercrime*. Dampak *cybercrime* terhadap bisnis juga menjadi fokus utama, menunjukkan bahwa bisnis menghadapi risiko yang cukup signifikan dari serangan siber. Selain itu, penelitian dengan tema perlindungan korban *cybercrime* dan literasi digital adalah aspek penting dalam penelitian saat ini. Internet banking, *cyberbullying*, pencurian dan penyalahgunaan data, serta perkembangan teknologi forensik digital semuanya menjadi topik penelitian yang penting pada periode ini. Penyalahgunaan telepon seluler dan media sosial juga terus menjadi perhatian seiring dengan meningkatnya penggunaan perangkat mobile. Keamanan nasional dan teknologi informasi tetap menjadi perhatian utama.

Analisa peneliti menunjukkan bahwa terjadinya evolusi penelitian tentang *cybercrime* di Indonesia dari fokus awal pada pemahaman dan regulasi hingga penekanan yang lebih besar pada teknologi, ancaman terbaru, dan dampaknya terhadap berbagai aspek kehidupan dan bisnis. Hal ini juga mencerminkan pentingnya literasi digital dan upaya kerjasama internasional dalam mengatasi masalah *cybercrime* yang semakin kompleks.

B. Kejahatan Siber Global

Cybercrime atau kejahatan dunia maya adalah kejahatan yang dilakukan dengan menggunakan teknologi informasi dan komunikasi sebagai alat atau target dari kejahatan tersebut. *Cybercrime* adalah kejahatan yang dilakukan dengan menggunakan teknologi informasi dan komunikasi, termasuk kejahatan terhadap kerahasiaan, integritas, dan ketersediaan informasi (Rowe, 2019). Meningkatnya kejadian *cybercrime* disebabkan oleh faktor-faktor seperti anonimitas di dunia digital, teknologi yang semakin canggih memudahkan kegiatan kejahatan siber, kesenjangan sosial yang mendorong individu untuk melakukan tindakan kriminal, insentif finansial, dan kurangnya regulasi serta penegakan hukum yang memadai di banyak negara. Selain itu, penegakan hukum terhadap tindakan

kejahatan siber juga masih terbatas oleh keterbatasan sumber daya dan kemampuan teknologi yang dimiliki oleh pihak penegak hukum (Bowker, 2012).

Kejahatan siber semakin berkembang seiring dengan semakin canggihnya teknologi digital, dan dapat memiliki dampak yang merugikan baik secara finansial maupun non-finansial bagi korban. Kejahatan siber atau *cybercrime* tidak hanya terjadi di seluruh dunia namun juga terjadi di Indonesia. Bahkan, kejahatan siber seringkali dilakukan secara lintas negara, sehingga membuat penanganan kejahatan siber menjadi semakin rumit dan kompleks. Kejahatan *cyber* di Indonesia yang sering terjadi antara lain *malware*, *phishing*, DDoS (*Distributed Denial of Service*), *cyberstalking*, identitas palsu, *cyberbullying*, kejahatan finansial, dan serangan pada infrastruktur kritis.

Beberapa *cybercrime* yang terjadi di beberapa negara yaitu serangan *Ransomware WannaCry* yang terjadi pada bulan Mei tahun 2017, serangan *ransomware WannaCry* menyerang lebih dari 200.000 komputer di 150 negara di seluruh dunia. Serangan ini menyerang sistem operasi Windows yang tidak diupdate dengan patch terbaru dan menggunakan teknik *exploit EternalBlue* yang dikembangkan oleh NSA. Setelah sistem terinfeksi, ransomware akan mengenkripsi file dan meminta pembayaran dalam bentuk bitcoin untuk mendapatkan kunci dekripsi. *Serangan WannaCry* menyebar dengan cepat dan menyerang banyak organisasi, termasuk rumah sakit, pabrik, dan perusahaan di seluruh dunia. Serangan ini menyebabkan gangguan besar-besaran dan kerugian finansial yang signifikan. *Serangan WannaCry* memunculkan kekhawatiran tentang keamanan siber global dan menyoroti pentingnya patching sistem dan tindakan keamanan yang tepat untuk mencegah serangan *ransomware* dan serangan siber lainnya (Syafira, 2020).

Serangan Jaringan Target pada tahun 2013, perusahaan retail AS Target mengalami serangan siber yang mengakibatkan pencurian data pribadi 110 juta nasabah. Serangan tersebut terjadi selama beberapa minggu pada bulan November dan Desember 2013, dan mengakibatkan informasi pribadi dari sekitar 110 juta nasabah Target dicuri oleh para peretas. Informasi yang dicuri termasuk nomor kartu kredit, tanggal kedaluwarsa, dan kode keamanan dari nasabah yang melakukan transaksi di toko-toko Target pada periode tertentu. Serangan ini dianggap sebagai salah satu serangan jaringan terbesar dalam sejarah dan mengakibatkan Target mengeluarkan dana yang besar untuk memperbaiki sistem keamanan mereka dan memberikan kompensasi kepada nasabah yang terkena dampak serangan tersebut (Smith et al., 2019).

Serangan *cyber* pada *Sony Pictures Entertainment* pada tahun 2014 adalah salah satu kejadian *cybercrime* terbesar yang pernah terjadi di dunia. Pada waktu itu, perusahaan tersebut mengalami serangan dari grup hacker yang mengklaim diri sebagai Guardians of Peace (GOP). Serangan tersebut menyebabkan pencurian data pribadi karyawan Sony Pictures, termasuk informasi yang berhubungan dengan gaji, data identitas, dan informasi medis. Selain itu, informasi bisnis rahasia, seperti naskah film, kontrak, dan email perusahaan juga dicuri oleh para hacker. Akibatnya, beberapa film yang diproduksi oleh *Sony Pictures*, seperti *The Interview*, bocor ke internet sebelum dirilis secara resmi. Serangan ini menyebabkan kerugian finansial yang besar bagi perusahaan, termasuk biaya untuk memperbaiki sistem keamanan dan mengembalikan layanan IT yang terkena dampak serangan. Serangan tersebut juga mengakibatkan kerugian citra bagi perusahaan (Setiaji, 2016).

Beberapa serangan serupa juga terjadi pada perusahaan Yahoo pada tahun 2013 dan 2014 yang menyebabkan informasi pribadi lebih dari 1 miliar akun pengguna dicuri. Serangan keamanan siber pada *Democratic National Committee (DNC)* pada tahun 2016 yang diduga dilakukan oleh peretas yang berhubungan dengan pemerintah Rusia, dan mengakibatkan informasi pribadi dan rahasia partai tersebut terbongkar. Serangan keamanan siber pada Equifax pada tahun 2017, di mana data pribadi dari hampir 150 juta orang Amerika dicuri oleh peretas. Serangan ransomware pada *Colonial Pipeline* pada tahun 2021 yang mengakibatkan penutupan jalur pipa bahan bakar minyak yang menghubungkan Selatan dan Timur Amerika Serikat, dan menimbulkan krisis pasokan bahan bakar. Serangan ransomware pada JBS, perusahaan daging terbesar di dunia, pada tahun 2021 yang menyebabkan pemadaman sementara operasi perusahaan dan mengancam pasokan daging di seluruh dunia.

Kelemahan dalam sistem keamanan menjadi penyebab utama pencurian data dan serangan cyber. Sistem keamanan tidak selalu sempurna dan dapat disebabkan oleh berbagai faktor, termasuk kekurangan sumber daya, ketidaktahuan, dan kesalahan manusia. Teknologi yang terus berkembang juga membuat serangan cyber semakin kompleks dan sulit untuk dideteksi. Dalam konteks Indonesia, kejahatan siber juga menjadi masalah serius. Jenis-jenis kejahatan siber yang sering terjadi di Indonesia mencakup *malware*, *phishing*, DDoS, cyberstalking, identitas palsu, cyberbullying, kejahatan finansial, dan serangan pada infrastruktur kritis. Penting untuk terus memperbarui sistem keamanan dan meningkatkan kesadaran akan risiko *cybercrime* bagi pengguna internet. Selain itu, kerjasama lintas negara juga penting untuk mengatasi kejahatan siber yang sering melibatkan pelaku dari berbagai negara. Penanganan kejahatan siber menjadi semakin kompleks dan memerlukan upaya yang terkoordinasi dari berbagai pihak. Dalam era digital yang semakin maju, penting bagi individu, perusahaan, dan pemerintah untuk mengambil tindakan yang serius dalam melindungi diri dari ancaman *cybercrime* dan bekerja sama untuk menciptakan lingkungan *online* yang lebih aman.

Serangan-serangan siber yang telah terjadi, seperti WannaCry, Jaringan Target, dan Sony Pictures Entertainment menunjukkan dampak serius yang dapat ditimbulkan oleh kejahatan dunia maya. Serangan-serangan ini menggarisbawahi pentingnya perbarui sistem keamanan, perlindungan data pribadi, dan kerjasama lintas negara dalam mengatasi ancaman *cybercrime*. Keamanan siber merupakan masalah global yang memerlukan upaya bersama dari berbagai pihak untuk melindungi infrastruktur digital dan menjaga keamanan data dari serangan yang dapat mengakibatkan kerusakan besar.

C. Kejahatan Siber di Indonesia dan Upaya Menghadapinya

Indonesia digempur 1,225 miliar serangan siber setiap harinya berdasarkan data Kementerian Komunikasi dan Informatika yang diperkuat oleh Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan, seperti tertulis dalam siaran pers dari Eset Indonesia. Dari miliaran serangan itu, perusahaan keamanan siber, Eset, menyebut bahwa ransomware masih jadi momok bagi keamanan siber berbagai perusahaan di 2018 (Rachmadie, 2020). Berdasarkan kajian dan analisis yang dilakukan melalui DAKA Advisori, kerugian yang diperkirakan akibat *cybercrime* di Indonesia adalah USD 895 miliar, yang berarti mencapai 1,20% dari total kerugian yang diperkirakan akibat *cybercrime* global, yaitu USD 71,620 miliar.

Indonesia menduduki peringkat kedua dunia untuk kejahatan dunia maya setelah Ukraina (Kominfo, 2015). *Cybercrime* merupakan jenis kejahatan baru yang melibatkan teknologi komputer dalam pelaksanaannya. *Cybercrime* mencakup berbagai jenis kejahatan seperti hacking, *phishing*, pornografi, penipuan *online*, dan pencurian nomor kartu kredit. Kejahatan dunia maya yang paling banyak terjadi di Indonesia adalah penyebaran konten provokatif dan penipuan *online*. Pada tahun 2022, terdapat 8.831 kasus kejahatan dunia maya yang dilaporkan oleh Polri dari Januari hingga Desember (Pusiknas Polri, 2022)

Kejahatan dunia maya di Indonesia meliputi pembajakan perangkat lunak, terorisme dunia maya, penipuan (termasuk penipuan berbasis dunia maya dan pelanggaran hukum transaksi elektronik), peretasan, manipulasi data, *web phishing*, dan serangan dunia maya terhadap sistem keamanan digital (Saragih & Siahaan, 2016). Penipuan saat ini merupakan jenis kejahatan yang paling banyak terjadi di Indonesia. Ledakan e-commerce telah berkontribusi pada peningkatan kasus penipuan.

Pemerintah Indonesia telah mengambil langkah untuk memerangi kejahatan dunia maya dengan memberlakukan undang-undang seperti Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Meskipun ada undang-undang keamanan siber di Indonesia, banyak kasus kejahatan siber telah disaksikan selama Covid-19. Kerentanan data pribadi publik Indonesia juga terungkap pada tahun 2020. Pakar keamanan dunia maya memperkirakan bahwa jumlah kejahatan dunia maya dan serangan mungkin meningkat hampir dua kali lipat karena teknologi komputerisasi modern dan keterampilan teknis perangkat lunak yang berbeda membuat individu melakukan kejahatan dunia maya (Nugroho & Chandrawulan, 2022).

Polisi juga telah membentuk unit khusus untuk menyelidiki kasus kejahatan dunia maya dan memiliki laboratorium forensik digital untuk mendukung penyelidikan mereka. Direktorat Tindak Pidana Siber (Dittipidsiber) di bawah Badan Reserse Kriminal (Bareskrim Polri) bertugas menegakkan hukum terhadap kejahatan dunia maya di Indonesia. Mereka menangani dua kategori kejahatan dunia maya: kejahatan komputer dan kejahatan terkait komputer. Kejahatan komputer menggunakan komputer sebagai alat utama operasi kejahatan seperti peretasan, manipulasi data, *phishing* web, dan serangan dunia maya terhadap sistem keamanan digital. Kejahatan terkait komputer menggunakan komputer sebagai fasilitator kejahatan. Polisi Siber berpatroli di dunia maya untuk mencari, mengamati, memantau, dan memprediksi potensi ancaman yang dapat mengganggu ketentraman dan keamanan masyarakat Indonesia (Center for Digital Society Fisipol UGM, 2021).

Secara umum ada tiga faktor utama yang menyebabkan kejahatan dunia maya di Indonesia. Faktor pertama adalah *human error*, yang mengacu pada ketidaksadaran pengguna dalam mengambil tindakan di dunia maya yang dapat membuat sistem mereka rentan terhadap peretasan. Misalnya, menggunakan kata sandi yang lemah atau mengklik tautan yang mencurigakan. Faktor kedua adalah kerentanan atau kelemahan sistem, yang dapat dimanfaatkan oleh penjahat dunia maya untuk mendapatkan akses tidak sah ke informasi sensitif. Faktor ketiga adalah penggunaan *malware* dan berbagai serangan dunia maya lainnya oleh peretas dunia maya profesional terorganisir yang meluncurkan berbagai serangan dunia maya menggunakan teknik dan alat canggih (Telkom, 2022). Salah satu pemicu terjadinya pencurian data adalah kelemahan sistem keamanan. Sistem keamanan

pada suatu *website* atau perangkat lunak tidak selalu sempurna sehingga dapat memungkinkan terjadinya kebocoran data atau serangan dari luar. Hal ini bisa disebabkan oleh beberapa faktor seperti kekurangan sumber daya, ketidaktahuan, kurangnya pelatihan, atau bahkan kesalahan manusia. Selain itu, teknologi juga terus berkembang she ingga serangan *cybercrime* juga semakin kompleks dan sulit untuk dideteksi dan dicegah. Oleh karena itu, penting untuk terus memperbarui sistem keamanan dan meningkatkan kesadaran akan risiko *cybercrime* bagi pengguna internet (Prabowo et al., 2020).

Kejahatan dunia maya semakin memprihatinkan di Indonesia, dimana Indonesia menjadi salah satu korban terbesar serangan siber. Terdapat 1,04 juta akun membocorkan data di Indonesia pada kuartal kedua tahun 2022 saja. Jumlah kebocoran data internet di Indonesia meningkat 143% dari kuartal pertama 2022 ke kuartal kedua. Kasus kejahatan dunia maya telah memengaruhi individu dan institusi pemerintah. Berikut adalah beberapa kasus kejahatan dunia maya yang terjadi di Indonesia.

Gambar 1. Kasus Kejahatan Dunia Maya yang Menyerang Website Pemerintah

Situs Komisi Pemilihan Umum (KPU) Indonesia diretas dan informasinya bocor pada tahun 2004. Sang hacker, Dani Firmansyah, ditangkap pada 22 April 2004. Ia mengaku tertantang untuk meretas situs tersebut setelah pejabat KPU menyatakan bahwa sistem teknologinya kuat dan tidak mungkin diretas. Peristiwa itu terjadi di Pusat Tabulasi Pemilu Hotel KPU Borobudur Jakarta Pusat pada 17 April 2004. Dani menggunakan *Cross Site Scripting (XSS)* dan *SQL Injection* untuk menguji sistem keamanan server tnp.kpu.go.id di gedung PT Danar. Insiden peretasan menyoroti pentingnya langkah-langkah keamanan dunia maya untuk situs web pemerintah. KPU telah menerapkan regulasi Teknologi Informasi dan Komunikasi (TIK) untuk mencegah kejahatan dunia maya. Namun demikian, masih terdapat kelemahan pada sistem keamanan teknologi informasi yang dapat dimanfaatkan oleh para hacker (Effendi, 2022).

Selanjutnya pada tahun 2013 terjadi serangan siber antara Indonesia dan Australia. Serangan tersebut diprakarsai oleh seorang hacker Indonesia yang bertanggung jawab atas serangan tersebut dan menuntut permintaan maaf dari Australia. Peretas menargetkan situs web pemerintah Australia dan bank sentral. Menanggapi hal tersebut, Kementerian Komunikasi dan Informatika (Kemkominfo) RI mengeluarkan pernyataan yang menghimbau para hacker Indonesia untuk tidak menyerang Australia. Namun, peretas melanjutkan serangannya hingga Australia meminta maaf kepada Indonesia. Insiden

tersebut menyebabkan ketegangan antara kedua negara dan menimbulkan kekhawatiran bahwa hal itu dapat menyebabkan perang dunia maya antara Indonesia dan Australia (Kominfo, 2013). Perang dunia maya antara Indonesia dan Australia pada tahun 2013 dipicu oleh tuduhan bahwa pemerintah Australia memata-matai pemerintah Indonesia. Konflik meningkat ketika peretas Indonesia yang berafiliasi dengan Anonymous menyerang sejumlah situs web yang berbasis di Australia, termasuk situs web *Australian Secret Intelligence Service (ASIS)*, antara 8 dan 11 November. Warga Australia diduga membalas pada 15 November. Perang dunia maya terjadi di tengah ketidaksepakatan antara Indonesia dan Australia atas pencari suaka dan terungkapnya penyadapan pejabat Indonesia oleh Australia (Lestari, 2021). Perang dunia maya antara Indonesia dan Australia pada tahun 2013 merupakan contoh bagaimana keamanan dunia maya dapat berdampak pada hubungan internasional. Sejak saat itu, kedua negara menjalin kerja sama keamanan siber melalui dialog kebijakan untuk mencegah konflik di masa depan.

Kasus selanjutnya adalah Tiket.com dan Citilink yang diserang oleh sekelompok *hacker* remaja dan satu orang berusia 27 tahun. Hacker ini berhasil membobol akun situs jual beli tiket *online* Tiket.com di server Citilink. Mereka menggunakan username dan *password* yang didapatkan dengan cara meretas situs Tiket.com untuk memasuki server Citilink. Setelah mendapatkan kode booking tiket pesawat, mereka menjualnya melalui akun Facebook pribadi mereka dengan harga diskon 30-40%. Akibat dari serangan ini, Tiket.com mengalami kerugian sebesar Rp 4.124.000.982 dan Citilink merugi Rp 1.973.784.434. Pelaku telah meraup keuntungan sampai Rp 1 milyar rupiah (CNN Indonesia, 2017)

Kasus keempat, pada Mei 2021 BPJS Kesehatan, kebocoran data di mana 279 juta catatan warga negara Indonesia bocor dan dijual di forum *online*. Pelanggaran tersebut pertama kali dilaporkan di media sosial dan BPJS Kesehatan segera merespons dengan menangguhkan semua kemitraan pertukaran data. Investigasi diluncurkan oleh polisi, BSSN (Badan Siber dan Sandi Negara), dan tim sistem operasi keamanan untuk melacak sumber kebocoran (e-Media DPR RI, 2021). Pelanggaran data telah menimbulkan kekhawatiran tentang risiko keamanan nasional. Dewan Pengawas BPJS Kesehatan juga telah menyatakan keprihatinan atas masalah tersebut.

Kemudian pada Juli 2021, ditemukan kebocoran data pada aplikasi e-HAC, yaitu kartu elektronik yang diperlukan untuk bepergian selama pandemi Covid-19. Kebocoran tersebut disebabkan oleh lemahnya protokol keamanan. Diperkirakan 1,3 juta pengguna aplikasi e-HAC Kemenkes terkena dampak pembobolan data tersebut, dengan data yang bocor sekitar 2 GB. Bocoran tersebut juga mengungkap data dari 226 rumah sakit di Indonesia, termasuk nama, alamat, dan kapasitasnya (Direktorat Sistem Informasi dan Teknologi UNIDA, 2021). Pada 24 Agustus, BSSN melakukan verifikasi laporan dan mematikan server e-HAC. Pada 25 Agustus lalu, Kemenkes membahas celah keamanan pada aplikasi e-HAC. VPNMentor menemukan bahwa tidak hanya pengguna aplikasi e-HAC yang terkena pembobolan data, tetapi juga seluruh infrastruktur terkait e-HAC Kemenkes, rumah sakit, dan pejabat yang menggunakan aplikasi tersebut. Data yang bocor tersebut antara lain informasi penumpang seperti dokumen identitas, nomor paspor, dan foto serta nomor KTP Elektronik yang digunakan saat pembelian tiket dan tujuan hotel. Namun, pada 9 September, penyelidikan polisi tidak menemukan bukti data pengguna diambil dari server eHAC. Kepala Pusat Data dan Informasi Kementerian Kesehatan menyatakan data

pengguna aman dan terlindungi dalam aplikasi PeduliLindungi yang telah terintegrasi dengan sistem eHAC (Kominfo, 2021).

Selanjutnya situs Sekretariat Kabinet Republik Indonesia setkab.go.id diretas pada 30 Juli 2021. Peretas adalah dua remaja yang ditangkap polisi pada 5-6 Agustus 2021. Para peretas adalah anggota komunitas bernama Padang BlackHat dan telah meretas sekitar 650 situs secara total. Motif meretas situs Sekretariat adalah untuk mencari keuntungan dengan menjual skrip pintu belakang dari situs yang ditargetkan. Kedua hacker tersebut dijerat dengan pasal 46 ayat (1) UU No.11/2008 tentang Informasi dan Transaksi Elektronik (ITE) dengan ancaman hukuman maksimal enam tahun penjara dan/atau denda Rp 1 miliar (USD). 69.000). Namun, mereka dialihkan ke program rehabilitasi alih-alih dituntut karena masih di bawah umur. Sekretariat menegaskan bahwa tidak ada dokumen rahasia di situsnya dan hanya berisi informasi tentang kegiatan presiden dan pemerintah (Maharani, 2021).

Kejahatan dunia maya dapat berdampak signifikan pada individu dan bisnis. Kejahatan dunia maya seperti pencurian identitas, penipuan, dan pelanggaran data dapat menyebabkan kerugian finansial, kerusakan reputasi, dan tekanan emosional bagi individu. Bisnis juga rentan terhadap kejahatan dunia maya, dengan potensi kerugian finansial akibat pencurian data atau serangan ransomware. Selain itu, bisnis dapat dikenai denda peraturan jika gagal mematuhi undang-undang perlindungan data (Nugroho & Chandrawulan, 2022). Karena itu, penting bagi individu dan bisnis untuk mengambil langkah-langkah untuk melindungi diri dari kejahatan dunia maya.

Beberapa upaya yang dapat dilakukan sebagai langkah preventif untuk menghindari *cybercrime*. Pertama, penting untuk menggunakan *password* yang kuat dan berbeda untuk setiap akun, serta menghindari berbagi informasi pribadi secara publik di media sosial atau forum *online*. Kedua, instal program antivirus dan *firewall* yang andal di komputer dan perangkat seluler untuk melindungi dari *malware* dan serangan hacker. Selanjutnya, selalu periksa URL sebelum mengklik tautan untuk memastikan keamanannya, terutama dalam pesan email atau pesan teks yang mencurigakan. Penggunaan jaringan *WiFi* yang aman juga dianjurkan, terutama saat melakukan transaksi keuangan atau mengakses informasi pribadi. Waspada terhadap pesan *phishing* yang meminta informasi pribadi, serta perbarui perangkat lunak secara teratur untuk mengatasi kelemahan keamanan. Pilihan untuk menggunakan layanan keamanan *online* juga dapat dipertimbangkan. Terakhir, penting untuk memahami hak privasi dan aturan privasi yang berlaku untuk layanan *online* yang digunakan agar dapat mengontrol dan melindungi data pribadi dengan lebih baik.

Meskipun pemerintah Indonesia telah mengambil langkah-langkah untuk mengatasi masalah ini, masalah ini tetap menjadi tantangan bagi semua negara seiring kemajuan teknologi. Ada beberapa tindakan yang dapat diambil untuk mencegah kejadian serupa di masa depan. Salah satu cara paling efektif untuk melindungi situs web dari peretas adalah dengan selalu memperbarui perangkat lunak. Perusahaan harus menginstal SSL dan plugin keamanan, memiliki perangkat lunak keamanan terbaru, dan menggunakan HTTPS. Penting juga untuk berinvestasi dalam pencadangan otomatis. Sekalipun semua tindakan lain diambil, masih ada risiko kehilangan segalanya karena peretasan situs web. Mencadangkan informasi secara teratur dapat membantu mencegah hal ini. Cara lain untuk melindungi situs web dari peretas adalah dengan berhati-hati saat menerima unggahan file melalui situs. Saat seseorang memiliki opsi untuk mengunggah sesuatu ke situs web, mereka dapat menyalahgunakan hak istimewa tersebut dengan memuat file berbahaya atau menimpa file

penting yang sudah ada untuk situs web tersebut. Oleh karena itu, penting untuk memeriksa file sebelum mengunggahnya (Casey Rowland, 2021).

Baik pemerintah maupun personal juga harus memeriksa kata sandi secara teratur. Kata sandi harus kuat dan unik untuk setiap akun. Penting juga untuk memantau log aktivitas secara teratur karena membantu memberi sinyal perubahan sehingga aktivitas yang tidak sah dapat dihentikan sejak awal. Terakhir, pemerintah atau personal perlu menyadari bahwa melindungi situs web mereka dari peretas dan serangan berbahaya adalah proses yang berkelanjutan. Mereka perlu menyadari perubahan ancaman dan mengambil langkah proaktif menuju keamanan (Nirvana, 2021).

Kejahatan siber di Indonesia telah mencatat berbagai peristiwa penting yang menitikberatkan terhadap dampak negatif yang ditimbulkannya, misalnya saja kerugian finansial, permasalahan diplomasi. Berbagai saran dan upaya pencegahan juga telah dilakukan diantaranya terkait penggunaan kata sandi kuat dan pemahaman tentang hak privasi kepada masyarakat. Pembahasan ini juga menggarisbawahi tentang pentingnya pembaruan secara terus-menerus dalam keamanan siber untuk melindungi data dan sistem *online*, karena tantangan ini akan terus meningkat seiring dengan perkembangan teknologi.

KESIMPULAN

Penulis penulis menyimpulkan bahwa ancaman *cybercrime* di Indonesia sekarang ini tergolong serius (berbahaya) karena berpotensi tinggi menimbulkan permasalahan nasional. Ancaman tersebut meliputi serangan *malware* atau perangkat lunak berbahaya yang dapat merusak data, mencuri informasi sensitif, atau bahkan mengambil alih sistem komputer secara keseluruhan. Ancaman selanjutnya yakni serangan DoS (*denial of service*) yang menyebabkan terganggunya akses pengguna terhadap layanan atau bahkan hingga terjadinya pemadaman layanan dan atau dalam skala yang lebih besar disebut dengan serangan DDoS (*distributed denial of service*). Serangan *phishing* juga menjadi ancaman serius karena dapat menyebabkan kebocoran informasi pribadi, seperti kata sandi dan informasi keuangan yang selanjutnya digunakan sebagai serangan pesan palsu untuk target yang lebih terarah melalui data/informasi pribadi yang telah ditemukan sebelumnya (*spear phishing*).

Indonesia menghadapi tantangan dalam menerapkan hukum siber melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Masalah utama adalah terminologi yang mempengaruhi interpretasi dan kontroversi terkait UU ITE. Meskipun UU ITE telah digunakan untuk menangani kejahatan siber seperti penyebaran konten negatif dan hoax, penerapannya kontroversial karena dianggap terlalu luas dan berpotensi mengekang kebebasan berekspresi. Masih ada kendala dalam penegakan hukum siber di Indonesia karena kurangnya SDM dan teknologi yang memadai. Oleh karena itu, perlu peningkatan kesadaran keamanan siber, edukasi, dan penegakan hukum yang lebih efektif untuk mengatasi ancaman *cybercrime*. Ancaman-ancaman ini dapat merusak data, mencuri informasi sensitif, mengganggu layanan, dan bahkan membahayakan keamanan nasional.

Sebagai saran dari penelitian ini bahwa perlunya keseriusan pemerintah dalam memperkuat penegakan hukum pelaku *cybercrime* di Indonesia dan perlunya peningkatan edukasi terhadap masyarakat tentang cara melindungi diri dari kejahatan dunia maya. Langkah preventif agar Masyarakat terhindar dari *cybercrime* meliputi penggunaan *password* yang kuat, instalasi antivirus dan *firewall*, pemeriksaan URL sebelum mengklik

tautan, penggunaan jaringan *WiFi* aman, waspada terhadap pesan *phishing*, pembaruan perangkat lunak, pertimbangan penggunaan layanan keamanan *online*, dan pemahaman aturan privasi yang berlaku guna melindungi data pribadi dan mengurangi risiko terhadap serangan siber.

Adapun beberapa saran untuk penelitian lanjutan (*future work*) yakni memperluas cakupan topik yang telah diselidiki dalam artikel ini, mengadopsi pendekatan *literatur review* dengan database yang lebih luas, atau melakukan penelitian empiris guna memvalidasi temuan yang telah diperoleh dalam penelitian ini.

DAFTAR PUSTAKA

Aji, V. B. S. (2022). Tinjauan Mekanisme Pengenaan Pajak Pertambahan Nilai Atas Transaksi Digital Game *Online*. *Jurnal Acitya Ardana*, *2*(1), 62–78. https://jurnal.pknstan.ac.id/index.php/JAA/article/view/1643

Akbar, M. A., & Alam, S. N. (2020). *E-COMMERCE: Dasar Teori Dalam Bisnis Digital*. Yayasan Kita Menulis.

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). *No Title*. Survei Profil Internet Indonesia 2022.

Bowker, A. (2012). *The Cybercrime Handbook for Community Corrections: Managing Offender Risk in the 21st Century*. Charles C Thomas Publisher.

Carr, N. (2014). *The Shallows: Internet mendangkalkan cara berfikir kita*. Mizan Pustaka.

Casey Rowland. (2021). *How to Secure a Website from Hackers [13-Step Guide]*.

Center for Digital Society Fisipol UGM. (2021). *The Existence of Indonesia Cyber Police: What does it mean for Us Netizens?*

Chusumastuti, D. (2020). Pengaruh Pemanfaatan Media *Online* Terhadap Minat Berwirausaha pada Mahasiswa (Studi Kasus di Sekolah Tinggi Multi Media "MMTC" Yogyakarta). *Jurnal Riset Inspirasi Manajemen Dan Kewirausahaan*, *4*(2), 77–85. https://ejurnal.stimi-bjm.ac.id/index.php/JRIMK/article/view/86/0

CNN Indonesia. (2017). *Begini Cara Hacker Bobol Situs Tiket.com*.

Direktorat Sistem Informasi dan Teknologi UNIDA. (2021). *Merunut Kebocoran Data E-HAC Kemenkes, dari Kronologi hingga Hapus Aplikasi*. https://www.cnnindonesia.com/teknologi/20170331145137-185-204065/begini-cara-hacker-bobol-situs-tiketcom

e-Media DPR RI. (2021). *Data BPJS Kesehatan Bocor, Tanggung Jawab Siapa?*

Effendi, D. R. N. (2022). *Hukum Pers dan Etika Jurnalistik di Era Digital* (Vol. 1). UPPM Universitas Malahayati.

Fink, A. (2019). *Conducting research literature reviews: From the internet to paper*. Sage publications.

Hartati, C. S., & Muhammad, A. (2023). Combating *Cybercrime* and Cyberterrorism in Indonesia. *Jurnal Hubungan Internasional*, *11*(2), 45–56. https://doi.org/10.18196/jhi.v11i2.15647

Hermawansyah, A. (2022). *Analisis Profil Dan Karakteristik Pengguna Media Sosial Di Indonesia*.

Indrajit, R. E. (2000). Manajemen sistem informasi dan teknologi informasi. *Jakarta: PT Elex Media Komputindo*.

Irfan, M., Elvia, M., & Dania, S. (2023). Ancaman *Cybercrime* dan Peran Cybersecurity pada E-commerce: Systematic Literature Review. *JURSIMA (Jurnal Sistem Informasi Dan Manajemen)*, *11*(1), 110–121. https://ejournal.indobarunasional.ac.id/index.php/jursima/article/view/567

Kominfo. (2013). *Kominfo serukan hacker Indonesia tahan serangan ke Australia*.

Kominfo. (2015). *Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber*.

Kominfo. (2021). *Kominfo Tangani Dugaan Kebocoran Data Aplikasi E-Hac*.

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. Springer.

Lestari, E. A. P. (2021). Complex Interdependence Between Indonesia-Australia Through Cybersecurity Cooperation Post Indonesia Australia Cyber War in 2013. *Jurnal Hubungan Internasional UMY*, *9*(2).

Lynch, M. P. (2016). *The internet of us: Knowing more and understanding less in the age of big data*. WW Norton & Company.

Maharani, T. (2021). *Kronologi dan Motif Peretasan Situs Setkab oleh Dua Remaja*.

Nirvana. (2021). *How to Protect & Secure Website From Hackers? (Website Protection Guide)*.

Nugroho, A., & Chandrawulan, A. A. (2022). Research synthesis of *cybercrime* laws and COVID-19 in Indonesia: lessons for developed and developing countries. *Security Journal*, 1–20. https://link.springer.com/article/10.1057/s41284-022-00357-y

Prabowo, W., Wibawa, S., & Azmi, F. (2020). Perlindungan Data Personal Siber di Indonesia. *Padjadjaran Journal of International Relations*, *1*(3), 218–239. http://jurnal.unpad.ac.id/padjir/article/view/22138

Purwadi, P., & Calam, A. (2020). Sistem Pendukung Keputusan Untuk Menentukan Pemasangan Lokasi Strategis *WiFi*. Id Pada Telkom (Studi Kasus Pada Pemsangan *WiFi*. Id Di Beberapa Lokasi Medan Menggunakan Metode Oreste. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer)*, *19*(1), 110–121. https://ojs.trigunadharma.ac.id/index.php/jis/article/view/231

Pusiknas Polri. (2022). *Kejahatan Siber di Indonesia Naik Berkali-kali Lipat*.

Rachmadie, D. T. (2020). Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana *Malware* Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016. *RECIDIVE*, *9*(2), 128–156. https://jurnal.uns.ac.id/recidive/article/view/47400

Rowe, N. C. (2019). Honeypot deception tactics. *Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings*, 35–45. https://www.researchgate.net/publication/330084850_Honeypot_Deception_Tactics_Reasoning_Adaptive_Planning_and_Evaluation_of_HoneyThings

Saragih, Y. M., & Siahaan, A. P. U. (2016). Cyber crime prevention strategy in Indonesia. *SSRG Int. J. Humanit. Soc. Sci*, *3*(6), 22–26. https://www.internationaljournalssrg.org/IJHSS/2016/Volume3-Issue6/IJHSS-V3I6P106.pdf

Setiaji, H. A. (2016). Tinjauan Hukum Internasional Terhadap Kasus Hacking Sony Pictures Entertainment. *Tidak Dipublikasikan). Universitas Hasanuddin*.

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of *cybercrime* and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society*, *17*(1), 42–60. https://www.emerald.com/insight/content/doi/10.1108/JICES-02-2018-0010/full/html

Soesanto, E., Utami, A. S., Chantica, J. A., Nabila, R. A., & Ricki, T. S. (2023). Keamanan Data Pribadi Dalam Sistem Pembayaran Via OVO Terhadap Ancaman dan Pengelabuan (*Cybercrime*). *IJM: Indonesian Journal of Multidisciplinary*, *1*(2), 424–435. https://journal.csspublishing.com/index.php/ijm/article/download/154/97

Subandi, K., Sugara, V. I., & Aryani, A. S. (2023). Peningkatan Keamanan pada Simple Network Time Protocol (SNTP) untuk Mendeteksi *Cybercrime* di dalam Aktivitas Jaringan. *Jurnal Asiimetrik: Jurnal Ilmiah Rekayasa Dan Inovasi*, 93–100. https://doi.org/10.35814/asiimetrik.v5i1.4113

Susanti, S. O., & Juwono, V. (2019). Collaborative Governance: Proyek Penyelenggaraan Jaringan Tulang Punggung Serat Optik Palapa Ring di Indonesia Tahun 2016-

2019. *Publik (Jurnal Ilmu Administrasi)*, *8*(1), 12–23. https://scholar.ui.ac.id/en/publications/collaborative-governance-proyek-penyelenggaraan-jaringan-tulang-p

SYAFIRA, A. (2020). *Upaya Sekuritisasi Pemerintah Inggris Dalam Kebijakan Kejahatan Cyber Wannacry Tahun 2017*.

Telkom. (2022). *The Most Common Causes of Cyber Crime in Indonesia*.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

We Are Social. (2021). *No Title*. Digital 2022: Another Year Of Bumper Growth.

Zittrain, J. (2008). *The future of the internet--and how to stop it*. Yale University Press.