Informatech: Jurnal Ilmiah Informatika dan Komputer
Volume 1, Nomor 2, Desember 2024, hlm 152-156 **E-ISSN: 3047-4752**

Menghadapi Tantangan Dan Solusi *Cybercrime* Di Era Digital

Virginia Valentine[1], Clara Sinta Septiani[2], Jadiaman Parshusip[3]
Universitas Palangka Raya, Jl. Yos Sudarso Palangka Kec. Jekan Raya Kota Palangka Raya 74874
[*1]*email : virginiavalent11@mhs.eng.upr.ac.id*
[2]*email : clarasinta@mhs.eng.upr.ac.id*
[3]*email : parhusip.jadiaman@it.upr.ac.id*

(Naskah diterima: *15 Nopember 2024*; Naskah direvisi: *4 Desember 2024*; Naskah diterbitkan: *5 Desember 2024*)

ABSTRAK *– Cybercrime merupakan ancaman terbesar di era digital yang terus berkembang seiring pesatnya teknologi informasi dan komunikasi, memberikan dampak kompleks terhadap individu hingga infrastruktur nasional. Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif-analitis untuk mengidentifikasi tantangan utama dalam menghadapi cybercrime, dengan fokus pada dinamika keamanan siber global. Saai ini menunjukkan peningkatan pemanfaatan kecerdasan buatan dan analitik data besar dalam sistem pertahanan siber. Namun, masih terdapat pada integrasi lintas sektor, regulasi adaptif, serta pendekatan edukatif yang efektif dalam meningkatkan kesadaran publik. Kajian dilakukan terhadap faktor-faktor seperti cepatnya transformasi digital, rendahnya literasi keamanan siber, keterbatasan regulasi, dan defisit tenaga ahli. Penanganan cybercrime membutuhkan pendekatan komprehensif yang menggabungkan teknologi, hukum, pendidikan, dan kerja sama internasional. Solusi strategis mencakup penguatan infrastruktur, edukasi publik, kolaborasi global, pengembangan SDM, dan pemanfaatan AI dalam deteksi serta pencegahan ancaman secara proaktif.*

Kata Kunci *– Edukasi Keamanan, Kejahatan Siber, Keamanan Digital, Teknologi Informasi*

Facing Cybercrime Challenges And Solutions In The Digital Era

ABSTRACT *– Cybercrime is the biggest threat in the digital era that continues to grow along with the rapid development of information and communication technology, giving complex impacts on individuals to national infrastructure. This study uses a qualitative method with a descriptive-analytical approach to identify the main challenges in dealing with cybercrime, with a focus on the dynamics of global cybersecurity. Currently, it shows an increase in the use of artificial intelligence and big data analytics in cyber defense systems. However, there are still cross-sector integration, adaptive regulations, and educational approaches that are effective in increasing public awareness. The study was conducted on factors such as the rapid digital transformation, low cybersecurity literacy, limited regulations, and a deficit of experts. Handling cybercrime requires a comprehensive approach that combines technology, law, education, and international cooperation. Strategic solutions include strengthening infrastructure, public education, global collaboration, human resource development, and the use of AI in proactive threat detection and prevention.*

Keywords *– Cyber Security Education, Cybercrime, Digital Security, Information Technology*

1. PENDAHULUAN

Seiring dengan pesatnya perkembangan sebuah teknologi informasi dan komunikasi membawa perubahan besar dalam cara manusia berinteraksi, berbisnis, dan mengakses informasi. Masyarakat kini lebih bergantung pada pencipataan teknologi untuk berbagai aspek kehidupan. Kemajuan ini memberikan banyak manfaat, seperti kemudahan akses data, efisiensi proses, dan konektivitas global. Namun, di balik kemajuan teknologi informasi ini, muncul pula sebuah tantangan besar, salah satunya adalah meningkatnya insiden kejahatan siber atau *cybercrime*. *Cybercrime* mencakup berbagai bentuk aktivitas ilegal yang melibatkan teknologi informasi, seperti peretasan, pencurian data, penyebaran malware, hingga manipulasi digital untuk tujuan penipuan atau penghancuran reputasi [1] [2].

Fenomena ini menimbulkan kekhawatiran besar bagi masyarakat, organisasi, dan pemerintah terkait dengan keamanan data dan integritas informasi. Dalam beberapa tahun terakhir, banyak terjadi kasus *cybercrime* yang dapat merugikan baik secara finansial maupun reputasi, yang menunjukkan

bahwa ancaman ini tidak bisa dianggap sepele [3] [4]. Oleh karena itu, penting untuk memahami berbagai tantangan yang akan dihadapi dalam memerangi kejahatan di dunia maya dan sebagai solusi yang bisa diterapkan untuk mengatasinya.

2. TINJAUAN PUSTAKA

Cybercrime adalah sebuah tindakan kejahatan yang dilakukan melalui internet atau komputer yang terhubung ke jaringan internet [5][6] [7] [8]. Tindakan kejahatan ini bisa berupa pencurian data, pengambil alihan akun, perusakan sistem, penyebaran virus, dan lain sebagainya. *Cybercrime* menjadi semakin umum, karena kemajuan teknologi dan semakin banyak orang yang menggunakan internet. *Cybercrime* merupakan kejahatan yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi (TIK), sedangkan *cybersecurity* ditujukan sebagai upaya untuk melindungi sistem komputer dari berbagai ancaman atau akses ilegal [9] [10] [11].

Cyberattack atau serangan siber adalah serangan yang dilakukan oleh pelaku kejahatan siber dengan menggunakan satu atau lebih komputer terhadap satu atau beberapa komputer atau jaringan [12] [13] [14]. Hal ini menjadi perhatian serius bagi individu, perusahaan, dan pemerintah. Indonesia tidak terlepas dari berbagai serangan siber. 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 [15] [16]. 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. Kejahatan siber telah marak terjadi di Indonesia yang menjadi ancaman bagi pertahanan dan keamanan negara [17] . Akibat dari permasalahan ini adalah bocornya data pribadi, data perusahaan, maupun data negara yang ditampilkan secara umum oleh pihak-pihak yang tidak bertanggung jawab. Berdasarkan permasalahan tersebut, kelompok akan melakukan kegiatan penelitian mengenai pertahanan dan keamanan siber di era digital dengan para mahasiswa. Melalui penelitian yang dilakukan oleh kelompok, diharapkan dapat mendapatkan pengetahuan dan pemahaman yang lebih dalam mengenai tantangan menghadapi keamanan siber di Indonesia. Dengan penelitian ini juga diharapkan kelompok beserta para responden yang berisi mahasiswa dapat mendapatkan pemahaman mengenai upaya dalam mengatasi tantangan keamanan siber tersebut dan dapat menemukan solusi yang efektif untuk mencapai tujuan dari ditingkatkannya pertahanan dan keamanan siber. Jumlah kasus cybercrime yang meningkat di negara Indonesia yang telah mendorong pemerintah untuk membuat undang-undang yang kuat untuk menjerat beberapa pelaku *cybercrime*. Pemerintah Indonesia memasukkan UU *Cybercrime* (UU Siber) ke dalam Undang-Undang Nomor 19 Tahun 2016 dan Kode Hukum Pidana sebagai revisi dari UU ITE Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun, penanggulangan tindak pidana cybercrime masih menghadapi kendala-kendala yang signifikan, seperti keterbatasan sumber daya manusia, fasilitas yang belum memadai, serta anggaran yang terbatas. Hal ini memerlukan sebuah perhatian lebih lanjut dari para pemerintah demi kemajuan kinerja aparat penegak hukum.

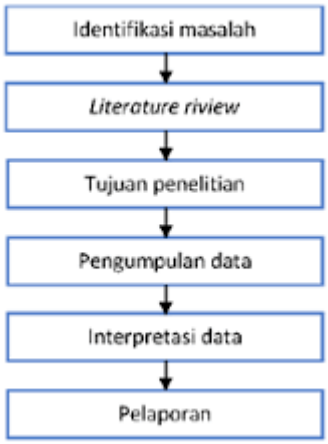
Tabel 1. Jumlah Korban Insiden dan Serangan Digital pada Periode Januari-Maret 2024

Nama Data	Nilai
Mahasiswa dan pelajar	17
Warga umum	11
Lembaga publik	9
Ormas sipil	6
Staf LSM dan aktivis	4
Jurnalis & pekerja media	4
Akademisi	3
Pegawai swasta	3

Tabel 1 merupakan contoh data terkait korban insiden dan serangan digital pada periode Januari-Maret 2024. Data tersebut menunjukkan berbagai kelompok yang menjadi target serangan siber, mulai dari mahasiswa dan pelajar hingga pegawai pemerintah. Insiden ini mencerminkan bagaimana serangan siber tidak hanya menyasar institusi besar atau perusahaan, tetapi juga individu dan kelompok masyarakat yang lebih luas. Dengan banyaknya korban dari berbagai latar belakang, data ini menyoroti betapa luasnya dampak serangan digital dan perlunya perhatian lebih terhadap keamanan siber di berbagai sektor.

3. METODE PENELITIAN

Penelitian ini menggunakan sebuah pendekatan kualitatif dengan metode atau teknik deskriptif untuk mengidentifikasi tantangan dan solusi dalam menghadapi *cybercrime* di era digital [18] [19]. Data dikumpulkan melalui studi literatur dari jurnal ilmiah, laporan kasus, buku, dan artikel terpercaya yang membahas *cybercrime [20]*.



Gambar 1. Metode Penelitian

Pada gambar 1 merupakan tahapan penelitian antara lain tahapan Identifikasi Masalah. Langkah pertama adalah menentukan masalah atau isu utama yang akan menjadi fokus penelitian. Masalah utama adalah meningkatnya ancaman cybercrime yang semakin kompleks seiring dengan pesatnya perkembangan teknologi. Kecepatan perkembangan teknologi melebihi kemampuan regulasi yang ada, menciptakan celah keamanan yang dimanfaatkan oleh pelaku kejahatan siber. Identifikasi masalah ini juga melibatkan tantangan seperti kurangnya kesadaran masyarakat tentang pentingnya menjaga data pribadi, serta keterbatasan tenaga ahli di bidang keamanan siber.

Tahap selanjutnya adalah Literature Review. Pada tahap ini, peneliti mempelajari berbagai sumber informasi. Data dikumpulkan dari jurnal ilmiah, laporan kasus, buku, dan artikel yang membahas masalah dan solusi terkait dengan kejahatan siber. Proses Literature review membantu memperkaya pemahaman peneliti tentang topik yang diteliti dan menjadi dasar untuk analisis lebih lanjut.

Tahapan ketiga adalah mendefinisikan Tujuan Penelitian. Berdasarkan identifikasi masalah dan hasil kajian literatur, peneliti merumuskan tujuan penelitian. Tujuan penelitian ini adalah untuk mengidentifikasi tantangan utama penelitian dalam menghadapi cybercrime dan mencari solusi yang efektif untuk mengurangi dampak dan frekuensi insiden *cybercrime*. Tujuan ini juga mencakup upaya memahami dinamika perkembangan teknologi yang dapat memperburuk ancaman siber serta mencari langkah-langkah pencegahan yang lebih baik.

Tahapan selanjutnya adalah sebuah proses Pengumpulan Data. Data yang dibutuhkan untuk menjawab pertanyaan penelitian dikumpulkan menggunakan studi literatur. Peneliti menganalisis berbagai sumber informasi yang relevan, termasuk laporan kasus yang mendokumentasikan insiden cybercrime, buku yang membahas teori terkait, dan artikel yang memberikan perspektif terkini mengenai ancaman siber. Metode pengumpulan data ini fokus pada sumber sekunder yang dapat memberikan informasi valid terkait cybercrime.

Tahapan selanjutnya adalah Interpretasi Data yakni Data yang telah dikumpulkan dianalisis untuk menemukan pola, tantangan utama, dan solusi yang dapat diterapkan untuk menangani masalah cybercrime. Peneliti akan menganalisis faktor-faktor seperti cepatnya perkembangan teknologi, kesadaran masyarakat yang rendah terhadap risiko keamanan, serta keterbatasan tenaga ahli di bidang keamanan siber. Interpretasi data juga mencakup perbandingan situasi di Indonesia pada tahun 2023 dan 2024 mengenai insiden cybercrime, termasuk motif politik yang mempengaruhi jenis serangan.

Tahapan terakhir yaitu pelaporan. Setelah analisis data selesai, hasil penelitian disusun dan dipresentasikan dalam bentuk laporan. Laporan ini menyajikan pemahaman yang diperoleh mengenai tantangan dan permasalahan serta menciptakan solusi dalam menghadapi permasalahan cybercrime, serta merekomendasikan langkah-langkah strategis yang dapat diambil. Rekomendasi ini mencakup penguatan infrastruktur keamanan digital, peningkatan edukasi masyarakat, regulasi yang lebih ketat, serta kerja sama internasional dalam menangani kejahatan siber lintas negara.

4. HASIL DAN PEMBAHASAN

Tantangan dalam menghadapi cybercrime sangat beragam, terutama dengan pesatnya perkembangan teknologi. Salah satu tantangan terbesar adalah kecepatan teknologi yang melebihi perkembangan regulasi yang ada, menciptakan celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan siber. [7]. Teknologi baru, seperti kecerdasan buatan dan *Internet of Things* (IoT), sering kali diadopsi tanpa pertimbangan keamanan yang matang, sehingga meningkatkan risiko. Selain itu, banyak masyarakat yang masih kurang sadar akan pentingnya menjaga keamanan data mereka. Kebiasaan menggunakan kata sandi yang lemah atau mudah ditebak, serta tidak mengenali ancaman phishing, menjadi salah satu penyebab utama tingginya insiden cybercrime. Solusi atau pemecahan untuk mengatasi masalah cybercrime tidak hanya bergantung pada teknologi, tetapi juga memerlukan upaya untuk meningkatkan kesadaran publik. Edukasi melalui kampanye dan pelatihan menjadi penting untuk memperkenalkan konsep dasar keamanan digital kepada masyarakat luas . Selain itu, kerja sama internasional yang sangat diperlukan untuk menghadapi tantangan ini, mengingat sifat cybercrime yang sering kali lintas batas negara. Kerja sama antarnegara dalam rangka

untuk menyusun regulasi global yang seragam dan efisien akan mempermudah penegakan hukum dalam kasus cybercrime lintas yurisdiksi. Di sisi lain, pengembangan teknologi seperti enkripsi data dan sistem deteksi intrusi secara real-time dapat membantu mencegah serangan siber sebelum terjadi kerugian yang lebih besar.

Namun, tantangan terbesar mungkin terletak pada keterbatasan tenaga ahli di bidang keamanan siber. Permintaan terhadap tenaga profesional keamanan jauh melebihi ketersediaan yang ada, sehingga banyak organisasi yang kesulitan untuk menjaga infrastruktur mereka dari ancaman digital. Oleh karena itu, penting bagi pemerintah dan institusi pendidikan untuk berinvestasi dalam pengembangan kurikulum yang mendukung peningkatan kompetensi di bidang keamanan siber. Secara keseluruhan, pendekatan yang holistik, mencakup peningkatan teknologi, regulasi hukum yang ketat, edukasi publik, serta kerja sama global, merupakan kunci dalam menangani ancaman cybercrime yang terus berkembang.

Pada tahun 2024, Indonesia mengalami peningkatan signifikan dalam insiden cybercrime. Berdasarkan laporan dari SAFEnet, terdapat 61 insiden keamanan digital yang tercatat pada kuartal pertama tahun ini, hampir dua kali lipat dari periode yang sama pada 2023, di mana hanya ada 33 insiden. Peningkatan ini setara dengan tambahan 28 insiden lebih banyak dibandingkan tahun sebelumnya, rata-rata bulanan insiden pada 2023 adalah 11, sementara pada 2024 meningkat menjadi 16,25 insiden per bulan. Insiden besar termasuk serangan ransomware yang melibatkan 130 serangan, serta 4.046 serangan phishing yang menargetkan sektor layanan informasi dan infrastruktur kritis. Ancaman ini meningkat menjelang Pemilu 2024, dengan motif politik menjadi salah satu faktor utama serangan digital tersebut.

Tabel 2. Perbandingan Insiden Cybercrime di Indonesia antara Kuartal Pertama Tahun 2023 dan 2024

Tahun	Jumlah Insiden (Total)	Rata-rata Bulanan	Jenis Insiden Utama	Motif Utama
2023	33	11	Phishing, Ransomware	Umum, tanpa motif politik dominan
2024	61	16,25	Phishing, Ransomware	Politik, terkait Pemilu 2024

Menurut data yang di dapatkan dari databoks yang digambarkan pada tabel 2, pada kuartal pertama 2024, terdapat 61 insiden, hampir dua kali lipat dari 33 insiden yang tercatat pada periode yang sama tahun 2023. Rata-rata insiden bulanan juga meningkat dari 11 insiden per bulan pada 2023 menjadi 16,25 insiden per bulan pada 2024. Jenis serangan yang paling dominan di kedua tahun tersebut adalah phishing dan ransomware, dengan peningkatan yang didorong oleh motif politik di tahun 2024, terutama menjelang Pemilu.

5. SIMPULAN

Cybercrime merupakan ancaman besar yang semakin meningkat seiring dengan pesatnya perkembangan teknologi yang sulit diimbangi oleh regulasi yang ada. Ancaman ini tidak hanya menyerang sektor bisnis besar, tetapi juga individu dan organisasi kecil. Solusi yang diperlukan untuk menghadapi cybercrime adalah pendekatan yang komprehensif, mencakup penguatan infrastruktur keamanan digital, edukasi masyarakat, regulasi yang lebih ketat, serta kerja sama internasional. Pengembangan tenaga ahli dan investasi dalam teknologi canggih, seperti kecerdasan buatan, juga menjadi kunci penting dalam memperkuat ketahanan terhadap serangan digital. Namun, meskipun penelitian ini memberikan gambaran umum yang komprehensif, masih diperlukan penelitian lebih lanjut mengenai efektivitas regulasi yang ada dan dampaknya terhadap pengurangan kasus cybercrime. Saran untuk penelitian selanjutnya adalah fokus pada pengembangan kebijakan yang adaptif terhadap perubahan teknologi dan peningkatan kolaborasi antar negara dalam menghadapi kejahatan siber global.

DAFTAR PUSTAKA

[1] R. S. Deora dan D. Chudasama, "Brief study of cybercrime on an internet," *Journal of communication engineering & Systems*, vol. 11, no. 1, hlm. 1–6, 2021.

[2] S. Monteith, M. Bauer, M. Alda, J. Geddes, P. C. Whybrow, dan T. Glenn, "Increasing cybercrime since the pandemic: Concerns for psychiatry," *Curr Psychiatry Rep*, vol. 23, hlm. 1–9, 2021.

[3] G. Sarkar dan S. K. Shukla, "Behavioral analysis of cybercrime: Paving the way for effective policing strategies," *Journal of Economic Criminology*, vol. 2, hlm. 100034, 2023.

[4] S. Chen *dkk.*, "Exploring the global geography of cybercrime and its driving forces," *Humanit Soc Sci Commun*, vol. 10, no. 1, hlm. 1–10, 2023.

[5] O. v Sviatun, O. v Goncharuk, C. Roman, O. Kuzmenko, dan I. V Kozych, "Combating cybercrime: economic and legal aspects,"

WSEAS Transactions on Business and Economics, vol. 18, hlm. 751–762, 2021.

[6] K. Phillips, J. C. Davidson, R. R. Farr, C. Burkhardt, S. Caneppele, dan M. P. Aiken, "Conceptualizing cybercrime: Definitions, typologies and taxonomies," *Forensic sciences*, vol. 2, no. 2, hlm. 379–398, 2022.

[7] D. S. Gojali, "Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective," *International Journal of Cyber Criminology*, vol. 17, no. 1, hlm. 1–11, 2023.

[8] M. M. Mijwil, M. Aljanabi, dan C. ChatGPT, "Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime," *Iraqi Journal For Computer Science and Mathematics*, vol. 4, no. 1, hlm. 8, 2023.

[9] M. E. Fauzi, M. Zakiansyah, D. T. Al Ariiq, dan T. Sutabri, "TRANSFORMASI TEKNOLOGI DIGITAL DI BIDANG PERBANKAN," *Kohesi: Jurnal Sains dan Teknologi*, vol. 1, no. 8, hlm. 91–100, 2023.

[10] A. Ali, M. Fahminuddin, dan S. Hidayatullah, "FINANSIAL TEKNOLOGI SYARIAH DAN BANK DIGITAL," *Zhafir: Journal of Islamic Economics, Finance, and Banking*, vol. 4, no. 1, hlm. 61–90, 2022.

[11] S. C. Simamora, V. Gaffar, dan M. Arief, "Systematic Literatur Review Dengan Metode Prisma: Dampak Teknologi Blockchain Terhadap Periklanan Digital," *Jurnal Ilmiah M-Progress*, vol. 14, no. 1, hlm. 1–11, 2024.

[12] D. Surya, D. Setiawan, Y. A. Aryani, dan T. Arifin, "Cyberattacks on the accounting profession: a literatur review," *Media Riset Akuntansi, Auditing & Informasi*, vol. 24, no. 2, hlm. 255–272, 2024.

[13] A. D. Samsoerizal, E. R. Hidayat, dan A. Sukendro, "Analytical study of indonesian cybersecurity: lesson learned from estonian cyberattacks in 2007," *International Journal of Arts and Social Science*, vol. 5, no. 2, hlm. 32–33, 2022.

[14] T. Sutikno dan D. Stiawan, "Cyberattacks and data breaches in Indonesia by Bjorka: hacker or data collector?," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 6, hlm. 2989–2994, 2022.

[15] N. B. Mulya, K. D. N. Pradnyani, A. L. Wangi, A. A. Nugraha, dan T. D. Rimadhani, "Analisis Peningkatan Jumlah Kasus Cyber Attack Di Indonesia Pada Masa Pandemi Covid-19," dalam *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, 2021, hlm. 241–247.

[16] R. Fitriani, R. Subagiyo, dan B. N. Asiyah, "Mitigating IT Risk of Bank Syariah Indonesia: A Study of Cyber Attack on May 8, 2023," *Al-Amwal: Jurnal Ekonomi dan Perbankan Syari'ah*, vol. 15, no. 1, hlm. 86–100, 2023.

[17] B. A. Tatara, B. Abdurachman, D. L. Mustofa, dan D. Yacobus, "The Potential of Cyber Attacks in Indonesia's Digital Economy Transformation," *NUANSA: Jurnal Penelitian Ilmu Sosial dan Keagamaan Islam*, vol. 20, no. 1, hlm. 19–37, 2023.

[18] H. Shabri, "Transformasi digital industri perbankan syariah Indonesia," *El-Kahfi | Journal of Islamic Economics*, vol. 3, no. 02, hlm. 228–234, 2022.

[19] Y. Ngamal dan M. A. Perajaka, "Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia," *Jurnal Manajemen Risiko*, vol. 2, no. 2, hlm. 59–74, 2022.

[20] S. N. Mareta, D. T. K. Wardani, A. L. Hanim, D. C. Rahmawati, N. P. Puspitasari, dan S. N. A. C. Darsono, "Peran Transformasi Digital Terhadap Kepuasan Nasabah Green Banking," *Journal of Waqf and Islamic Economic Philanthropy*, vol. 1, no. 3, hlm. 1–11, 2024.