# Studi Literatur : Ancaman *Cybercrime* di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital

**Nabila Aulia Agustin[1] dan Refania Meilani Firdos[2]**

[1,2]Teknik Informatika, Universitas Pelita Bangsa, Cikarang Selatan, Indonesia
Nabilaauliaagustin123@gmail.com[1],refaniameilanifirdos@gmail.com

## ABSTRAK

Meningkatkan Kesadaran akan Keamanan *Cyber* di Era *Digital*, Karena semakin banyaknya aktivitas yang dilakukan secara *Online*, keamanan *cyber* menjadi semakin penting. Studi tentang pengamanan *cyber* dapat meningkatkan pemahaman kita tentang jenis serangan *cyber*, teknik yang digunakan oleh penyerang, dan kerentanan sistem yang ada. Hal ini memiliki potensi untuk meningkatkan kesadaran dan kewaspadaan individu dan organisasi terhadap ancaman *cyber*. Beberapa cara untuk meningkatkan keamanan *cyber* termasuk meningkatkan kapasitas, membangun sistem pertahanan dan keamanan siber yang berbasis pada *cyber defence*, serta komunikasi dan sinergitas, koordinasi, jaringan, dan kerja sama teknis untuk membentuk komunitas keamanan siber. Selain itu, penelitian dapat dilakukan untuk mengukur kesadaran pengguna *E-commerce* dan media sosial Indonesia tentang keamanan *cyber*.

**Kata Kunci: *Cyber, Digital,* Sistem, Keamanan, Sosial**

## *ABSTRACT*

*Increasing awareness of cyber security in the digital age As more activities are being carried out Online, cybersecurity is becoming increasingly important. Studying cyber security can improve our understanding of the types of cyberattacks, the techniques used by attackers, and the vulnerabilities of existing systems. It has the potential to raise awareness and alertness of individuals and organizations to cyber threats. Some of the ways to enhance cyber security include enhancing capacity, building cyber defense-based defence and security systems, as well as communication and synergy, coordination, networking, and technical collaboration to form a cybersecurity community. In addition, research can be done to measure Indonesian E- commerce and social media users' awareness of cyber security.*

***Keywords: Cyber, Digital, Systems, Security, Social***

## PENDAHULUAN

Keamanan *cyber* adalah perlindungan terhadap serangan dan ancaman terhadap sistem, jaringan, dan data *digital*. Karena semakin banyaknya aktivitas yang dilakukan secara *Online*, keamanan *cyber* menjadi semakin penting di era *digital*. Oleh karena itu, penting untuk terus memperbarui sistem keamanan dan meningkatkan kesadaran pengguna internet akan ancaman *cybercrime*. Ancaman *cyber* termasuk pencurian data, serangan *Malware*, dan serangan *DDoS*. Selain itu, untuk membentuk komunitas keamanan siber, diperlukan kerja sama lintas negara dan strategi pengamanan *cyber*, seperti peningkatan kapasitas, pembentukan sistem pertahanan dan keamanan berbasis *cyber*, dan kerja sama teknis dan sinergitas. Studi tentang pengamanan *cyber* dapat

meningkatkan pemahaman kita tentang jenis serangan *cyber*, teknik yang digunakan oleh penyerang, dan kerentanan sistem yang ada.

Keamanan *cyber* menjadi semakin penting di era *digital*, di mana aktivitas *Online* semakin meluas. Untuk memahami dan mengatasi ancaman *cyber*, penting untuk terus memperbarui sistem keamanan dan meningkatkan kesadaran akan risiko *cybercrime* bagi pengguna internet.

Analisis terhadap berbagai studi kasus serangan *cyber* dapat memberikan pemahaman mendalam tentang jenis serangan, metode yang digunakan, dan kergentanan sistem, sehingga dapat meningkatkan kesadaran dan kewaspadaan terhadap ancaman *cyber* di kalangan individu dan organisasi.

Di Indonesia, strategi pengamanan *cyber* seperti capacity building, pembentukan sistem pertahanan berbasis *cyber* defence dan *cyber* security, serta sinergitas dan kerja sama teknis diperlukan untuk membentuk komunitas keamanan siber. Selain itu, pengetahuan dan kesadaran tentang *cyber* security juga penting dalam konteks *E-commerce*, di mana kesadaran ini dapat berperan dalam melindungi pelaku *E-commerce* dari ancaman *cyber*. Oleh karena itu, upaya untuk meningkatkan kesadaran akan keamanan *cyber* di era *digital* memiliki implikasi yang signifikan dalam melindungi individu, organisasi, dan infrastruktur *digital*.

Melalui berbagai program dan kebijakan, pemerintah Indonesia telah mendukung peningkatan akses internet. Selain itu, pemerintah Indonesia terus meluncurkan program-program seperti Gerakan Nasional
1000 *Start-Up Digital*, yang diluncurkan pada tahun 2016 oleh Kementerian Komunikasi dan Informatika (Kominfo). Program ini bertujuan untuk mendorong pertumbuhan ekonomi *digital* dan inovasi di Indonesia dengan menumbuhkan 1000 *Start-Up digital* yang sukses yang memiliki dampak positif pada ekonomi. Pelatihan, akses ke pasar, pembiayaan, pengembangan bisnis, dan infrastruktur teknologi adalah beberapa bentuk dukungan yang diberikan oleh program (Chusumastuti, 2020). Selain itu, ada Program Palapa Ring, yang bertujuan untuk membangun infrastruktur jaringan serat optik nasional yang melingkupi seluruh wilayah Indonesia. Diharapkan infrastruktur ini dapat meningkatkan akses internet di wilayah.

## METODE PENELITIAN

Dalam penelitian ini, metode literatur review digunakan untuk memeriksa dan menganalisis karya tulis atau literatur yang relevan dengan topik penelitian. Metode ini digunakan untuk mendapatkan pemahaman yang lebih baik tentang topik tertentu, menganalisis temuan penelitian sebelumnya, dan membuat kerangka teoretis yang solid untuk penelitian yang akan dilakukan (Fink, 2019). Peneliti mencari literatur tentang topik penelitian mereka dari berbagai sumber, seperti jurnal, buku, artikel, dan dokumen *Online*. Dalam kasus ini, penulis membatasi topik penelitian pada *cybercrime* yang ditemukan dalam database Google Scholar.

Karena kemudahan akses terbuka terhadap artikel, yang memudahkan pengumpulan data, database Google Scholar lebih disukai. Selanjutnya, penulis membaca dan menelaah literatur sebelumnya, mencatat informasi penting, dan mengorganisasi data secara sistematis. Kemudian, mereka menganalisis data dari literatur sebelumnya dan membuat sintesis atau rangkuman hasilnya. Pada tahap terakhir, penulis menulis laporan hasil penelitian dengan menggabungkan hasil analisis. Penulis membuat keputusan untuk menggunakan metode peninjauan literatur karena memiliki banyak kelebihan termasuk kemampuan untuk mengakses sejumlah besar informasi dari berbagai disiplin ilmu, menghemat waktu dan uang, dan dapat digunakan sebagai referensi saat menulis karya ilmiah.

## HASIL DAN PEMBAHASAN

*Cybercrime*, juga dikenal sebagai kejahatan dunia maya, adalah kejahatan yang dilakukan dengan menggunakan teknologi informasi dan komunikasi sebagai alat atau target dari kejahatan tersebut. *Cyber*crime termasuk kejahatan terhadap kerahasiaan, integritas, dan ketersediaan informasi (Rowe, 2019). Faktor-faktor seperti anonimitas di dunia *digital*, teknologi yang semakin canggih yang memudahkan kegiatan kejahatan siber, kesenjangan sosial yang mendorong orang untuk melakukan kejahatan siber, insentif finansial, dan kurangnya regulasi dan penegakan hukum yang memadai di banyak negara semuanya berkontribusi pada peningkatan kejadian *cyber*crime. Selain itu, penegakan hukum terhadap tindakan kejahatan siber juga terbatas oleh sumber daya dan kemampuan teknologi penegak hukum.

Kejahatan siber meningkat seiring dengan kemajuan teknologi *digital*. Ini dapat membahayakan korban secara finansial maupun nonfinansial. Kejahatan siber atau *cyber*crime tidak hanya terjadi di Indonesia tetapi juga di seluruh dunia, dan seringkali dilakukan secara lintas negara, membuat penanganan kejahatan siber semakin rumit dan kompleks. *Malware*, phishing, *DDoS (Distributed Denial of Service)*, *cyberstalking*, identitas palsu, *cyberbullying*, kejahatan finansial, dan serangan pada infrastruktur kritis adalah beberapa kejahatan *cyber* yang paling umum terjadi di Indonesia.

Penyebab utama pencurian data dan serangan internet. Berbagai faktor dapat menyebabkan kegagalan sistem keamanan, seperti kekurangan sumber daya, ketidaktahuan, dan kesalahan manusia. Selain itu, karena teknologi terus berkembang, serangan *cyber* semakin kompleks dan sangat sulit untuk diidentifikasi. Kejahatan siber juga menjadi masalah besar di Indonesia. *Malware*, *phishing*, dan lainnya adalah contoh kejahatan siber yang paling umum di Indonesia. *DDoS*, *cyberstalking*, intimidasi, kejahatan finansial, dan serangan pada infrastruktur sangat penting. Perlu terus memperbarui dan meningkatkan sistem keamanan. kesadaran akan bahaya yang dibawa oleh kejahatan internet kepada pengguna internet.

Berikut adalah laporan kasus kejahatan siber dari Januari-September 2021


Gambar 1. Laporan Kejahatan *Cyber*, Januari-September 2021

Karena Indonesia menjadi salah satu korban terbesar serangan siber, kejahatan dunia maya semakin memprihatinkan. Jumlah kebocoran data internet di Indonesia meningkat 143% dari kuartal pertama 2022 hingga kuartal kedua 2022, dengan 1,04 juta akun membocorkan data. Kasus kejahatan dunia maya telah berdampak pada orang dan lembaga pemerintah. Berikut adalah beberapa kasus kejahatan dunia maya di Indonesia.


Gambar 2. Kasus Kejahatan Dunia Maya di Indonesia

Pada tahun 2004, situs web Komisi Pemilihan Umum (KPU) Indonesia diretas, sehingga

informasinya tersebar luas. Dani Firmansyah, seorang hacker, ditahan pada 22 April 2004. Setelah pejabat KPU menyatakan bahwa sistem teknologinya kuat dan tidak mungkin diretas, ia menyatakan bahwa itu sulit untuk diretas. Peristiwa itu terjadi pada tanggal 17 April 2004 di Pusat Tabulasi Pemilu Hotel KPU Borobudur di Jakarta Pusat. Dani menguji sistem keamanan server tnp.kpu.go.id di gedung PT Danar dengan menggunakan *Cross Site Scripting (XSS)* dan *SQL Injection*. Berita peretasan menunjukkan betapa pentingnya mengambil tindakan untuk menjaga keamanan situs web pemerintah. Untuk mencegah kejahatan dunia maya, KPU telah memberlakukan peraturan TIK. Namun demikian, kelemahan sistem keamanan TI masih dapat dimanfaatkan oleh pencuri (Effendi, 2022).

Tuduhan bahwa pemerintah Australia memata-matai pemerintah Indonesia memicu perang dunia maya 2013 antara Indonesia dan Australia. Antara 8 dan 11 November, peretas Indonesia yang berafiliasi dengan Anonymous melakukan serangan ke sejumlah situs web Australia, termasuk situs web *Australian Secret Intelligence Service (ASIS)*. Pada 15 November, warga Australia diharapkan akan memberikan tanggapan. Ketidaksepakatan antara Indonesia dan Australia tentang pencari suaka dan fakta bahwa Australia menyadap pejabat Indonesia memicu perang dunia maya (Lestari, 2021). Perang dunia maya 2013 antara Indonesia dan Australia adalah contoh bagaimana keamanan dunia maya dapat memengaruhi hubungan internasional. Sejak saat itu, kedua negara bekerja sama dalam keamanan siber melalui diskusi kebijakan untuk menghindari perselisihan.

Kasus terkait Tiket.com dan Citilink adalah hasil dari serangan hacker oleh sekelompok remaja dan satu individu berusia 27 tahun. Hacker ini berhasil membobol akun situs jual beli tiket Tiket.com di server Citilink. Mereka melakukannya dengan meretas situs Tiket.com dan memasuki server Citilink. Tiket.com mengalami kerugian sebesar Rp 4.124.000.982 dan Citilink mengalami kerugian sebesar Rp 1.973.784.434 sebagai akibat dari serangan ini, mereka menjual tiket pesawat melalui akun Facebook pribadi mereka dengan harga diskon 30 hingga 40 persen. Pelaku menghasilkan keuntungan hingga 1 milyar rupiah.

Kasus keempat adalah kebocoran data BPJS Kesehatan pada Mei 2021, yang melibatkan penyebaran 279 juta catatan warga negara Indonesia di forum *Online*. BPJS Kesehatan segera menghentikan semua kolaborasi pertukaran data setelah diberitahu tentang pelanggaran di media sosial. Polisi, BSSN (Badan Siber dan Sandi Negara), dan tim sistem operasi keamanan memulai investigasi untuk melacak sumber kebocoran (*e*-Media DPR RI, 2021). Kekhawatiran tentang keamanan nasional telah muncul karena pelanggaran data. Selain itu, Dewan Pengawas BPJS Kesehatan telah menyatakan keprihatinan mereka atas masalah tersebut.

Kemudian pada Juli 2021, terjadi kebocoran data pada aplikasi *e*-HAC, kartu elektronik yang dibutuhkan selama pandemi Covid-19. Protokol keamanan yang tidak ketat menyebabkan kebocoran data. Pembobolan data tersebut berdampak pada sekitar 1,3 juta pengguna aplikasi *e*- HAC Kemenkes, dengan jumlah data yang bocor sekitar 2 GB. Selain itu, bocoran tersebut mengungkap data tentang 226 rumah sakit di Indonesia, termasuk nama, alamat, dan kapasitasnya (Direktorat Sistem Informasi dan Teknologi UNIDA, 2021). Pada 24 Agustus, BSSN memverifikasi laporan dan mematikan server *e*-HAC. Pada 25 Agustus,

Kemenkes mendiskusikan masalah keamanan pada aplikasi *e*-HAC. VPNMentor menemukan bahwa pembobolan data mencakup pengguna aplikasi eHAC dan seluruh infrastruktur terkait *e*-HAC yang digunakan oleh Kemenkes, rumah sakit, dan pejabat.

Kejahatan dunia maya dapat berdampak besar pada orang dan perusahaan. Kejahatan dunia maya seperti pencurian identitas, penipuan, dan pelanggaran data dapat menyebabkan tekanan emosional, kerusakan finansial, dan reputasi yang buruk. Selain itu, bisnis rentan terhadap kejahatan dunia maya, yang dapat menyebabkan kerugian finansial. Pencurian data atau serangan ransomware. Selain itu, perusahaan dapat dikenakan denda oleh lembaga pemerintah. Jika mereka tidak mengikuti peraturan perlindungan data (Nugroho & Chandrawulan, 2022).

Akibatnya, individu dan organisasi harus mengambil tindakan untuk melindungi diri dari aktivitas ilegal di internet. Di Indonesia, kejahatan siber telah mencatat banyak peristiwa penting yang menekankan efek negatifnya, seperti kehilangan uang dan masalah diplomatik. Pemahaman masyarakat tentang hak privasi dan penggunaan kata sandi yang kuat adalah beberapa dari banyak rekomendasi pencegahan yang telah dilakukan. Selain itu, karena tantangan keamanan siber akan terus meningkat seiring dengan kemajuan teknologi, pembahasan ini menggarisbawahi pentingnya pembaruan terus-menerus dalam keamanan siber untuk melindungi data dan sistem di internet.

## SIMPULAN

Dengan semakin meluasnya aktivitas *Online*, kesadaran akan keamanan *cyber* menjadi sangat penting. Studi dan pemahaman mendalam tentang jenis serangan, teknik yang digunakan oleh penyerang, dan kerentanan sistem menjadi kunci dalam meningkatkan kesadaran dan kewaspadaan individu serta organisasi terhadap ancaman *cyber*. Negara ini mengalami berbagai kasus serangan *cyber*, termasuk pencurian data, serangan *Malware*, *DDoS*, dan lainnya. Kurangnya penegakan hukum yang memadai, kompleksitas serangan, dan kesenjangan sosial merupakan faktor-faktor utama yang menyebabkan meningkatnya kasus *cyber*crime. Kejahatan *cyber* seperti pencurian identitas, penipuan, dan pelanggaran data dapat menyebabkan kerugian finansial, reputasi buruk, dan kerugian emosional pada individu dan perusahaan.

Kesimpulannya, perlunya meningkatkan kesadaran, pengetahuan, serta upaya kolaboratif yang kuat dalam bidang keamanan *cyber* menjadi esensial untuk melindungi masyarakat dan infrastruktur *digital* di era *digital* saat ini.

## DAFTAR PUSTAKA

Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan *cyber* security guna mewujudkan keamanan nasional di era society 5. 0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234. https://doi.org/10.54706/senastindo .v3.2021.141

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman *cyber*crime di indonesia: Sebuah tinjauan pustaka sistematis. *Jurnal Konstituen*, *5*(1), 1–17. https://doi.org/10.33701/jk.v5i1.32 08

Rosyidi, A. F. (2018). *Ambiguitas politik HAM di Papua: Laporan kondisi hak asasi manusia di Papua tahun 2016*. Publikasi Masyarakat Setara.

Wibawa, S. (2023). Analisis chatbot otomatisasi tugas administratif dan manajemen dalam lingkungan *digital* dengan menggunakan python. *INSANTEK*, *4*(1), 25–31. https://doi.org/10.31294/insantek.v 4i1.2190

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. bjm.ac.id/index.php/JRIMK/article/view/86/0

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

Rowe, N. C. (2019). Honeypot deception tactics. Autonomous *Cyber* Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings, 35–45.

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

Nugroho, A., & Chandrawulan, A. A. (2022). Research synthesis of *cyber*crime 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

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