JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 6 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1554-1559

Ancaman Siber Di Era Digital: Mengenal Modus Kejahatan Teknologi Informasi dan Strategi Penanggulangannya

Lanang Patih Sadelih[1], Evy Nurmiati[2]

[1,2]Fakultas Sains dan Teknologi, Program Studi Sistem Informasi, UIN Syarif Hidayatullah Jakarta, Kota Tangerang Selatan, Indonesia
Email: [1]lanang.patih24@mhs.uinjkt.ac.id, [2]evy.nurmiati@uinjkt.ac.id

Abstrak−Transformasi digital yang masif di Indonesia membawa kemudahan luar biasa, tetapi sekaligus memperluas celah kerentanan keamanan informasi. Berdasarkan data Badan Siber dan Sandi Negara (BSSN), aktivitas serangan siber di Indonesia mengalami lonjakan drastis dalam beberapa tahun terakhir, mencapai 5,5 miliar serangan pada tahun 2025. Artikel ini membahas lanskap ancaman siber terkini, membedah berbagai modus kejahatan Teknologi Informasi (TI) seperti ransomware adaptif, phishing berbasis AI, kebocoran data, dan Distributed Denial of Service (DDoS), serta merumuskan strategi penanggulangan yang komprehensif dari aspek teknis, regulasi, dan edukasi publik. Metode kajian yang digunakan adalah studi pustaka kualitatif-konseptual yang menganalisis literatur sekunder dari laporan resmi pemerintah, regulasi perlindungan data pribadi, serta jurnal terakreditasi nasional dan internasional dari rentang tahun 2021-2026. Analisis mendalam difokuskan pada studi kasus serangan ransomware pada Pusat Data Nasional (PDN) 2024. Hasil kajian menekankan bahwa sinergi holistik dari arsitektur Zero Trust, penegakan hukum UU Perlindungan Data Pribadi (UU PDP), kolaborasi tim tanggap insiden (CSIRT) tingkat nasional, serta kampanye literasi siber secara berkelanjutan sangat krusial untuk mengamankan ekosistem digital nasional.

Kata Kunci: Keamanan siber; Kejahatan siber; Ransomware; Phishing; Zero Trust; Pusat Data Nasional

Abstract−*Indonesia's massive digital transformation has brought extraordinary convenience, but has also widened information security vulnerabilities. According to data from the National Cyber and Crypto Agency (BSSN), cyberattack activity in Indonesia has experienced a drastic spike in recent years, reaching 5.5 billion attacks by 2025. This article discusses the current cyberthreat landscape, dissecting various Information Technology (IT) crime modes such as adaptive ransomware, AI-based phishing, data breaches, and Distributed Denial of Service (DDoS), and formulating a comprehensive countermeasure strategy from technical, regulatory, and public education perspectives. The study method used is a qualitative-conceptual literature study that analyzes secondary literature from official government reports, personal data protection regulations, and national and international accredited journals from 2021-2026. The in-depth analysis focused on a case study of a ransomware attack on the National Data Center (PDN) in 2024. The study's findings emphasize that the holistic synergy of Zero Trust architecture, enforcement of the Personal Data Protection Law (PDP Law), collaboration of national-level incident response teams (CSIRTs), and ongoing cyber literacy campaigns are crucial to securing the national digital ecosystem.*

Keywords: Keamanan siber; Kejahatan siber; Ransomware; Phishing; Zero Trust; Pusat Data Nasional

1. PENDAHULUAN

Transformasi teknologi informasi dan komunikasi di Indonesia telah merambah hampir ke seluruh sektor kehidupan, mulai dari pelayanan publik, perbankan, hingga aktivitas perdagangan mikro. Berdasarkan data terbaru dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), tingkat penetrasi internet di Indonesia telah mencapai lebih dari 79% dari total populasi, yang setara dengan lebih dari 220 juta pengguna aktif. Di satu sisi, digitalisasi ini mendorong efisiensi, inklusi ekonomi, dan kemudahan akses layanan pemerintahan melalui Sistem Pemerintahan Berbasis Elektronik (SPBE). Di sisi lain, peningkatan ketergantungan yang masif pada ruang siber membuka celah kerentanan keamanan informasi yang semakin lebar (Safitri et al., 2026).

Menurut laporan resmi Badan Siber dan Sandi Negara (BSSN), eskalasi ancaman siber di Indonesia telah mencapai tahap yang mengkhawatirkan. Pada tahun 2025, tercatat sebanyak 5,5 miliar serangan siber yang menargetkan sistem pertahanan nasional maupun swasta. Angka ini merepresentasikan lonjakan sebesar 714% dari rata-rata tahunan pada periode 2020-2024. Bahkan, tren peningkatan ini berlanjut pada awal tahun 2026 dengan akumulasi mencapai 1,52 miliar serangan dalam periode Januari hingga pertengahan April. Kejadian fatal seperti serangan *ransomware* terhadap Pusat Data Nasional Sementara (PDNS) 2 pada Juni 2024 serta

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 6 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1554-1559

kebocoran data massal di berbagai lembaga negara memperjelas bahwa ancaman siber bukan lagi sekadar wacana teoritis, melainkan bahaya nyata yang dapat melumpuhkan infrastruktur kritis dan mengganggu pelayanan publik dalam skala nasional (Alfi et al., 2023).

Kerugian yang ditimbulkan dari kejahatan siber tidak lagi sebatas kerugian finansial individual seperti pembobolan rekening atau penipuan daring, melainkan telah menyentuh level kedaulatan data nasional. Transformasi digital yang terburu-buru tanpa disertai penguatan aspek keamanan (*security by design*) terbukti menjadi bumerang bagi ketahanan nasional (Aryapranata et al., 2024). Kelemahan ini sering kali dieksploitasi oleh kelompok peretas transnasional yang memanfaatkan taktik canggih untuk menyusup ke dalam server pemerintah maupun korporasi vital (Siregar et al., 2022).

Tantangan utama yang dihadapi Indonesia saat ini adalah kecepatan adaptasi pelaku kejahatan yang melampaui kesiapan sistem pertahanan siber domestik (Aryapranata et al., 2024). Modus operandi kejahatan teknologi informasi terus berkembang seiring dengan munculnya kecerdasan buatan (*Artificial Intelligence*) yang digunakan untuk mempermudah peretasan. Oleh sebab itu, tinjauan komprehensif mengenai modus kejahatan TI terbaru dan formulasi kebijakan penanggulangan yang integratif menjadi krusial untuk dibahas. Artikel ini bertujuan untuk memetakan modus-modus operandi kejahatan TI terkini, menganalisis studi kasus insiden keamanan siber nasional, mengidentifikasi faktor kerentanan internal, serta merumuskan rekomendasi strategi penanggulangan siber yang efektif dan dapat diterapkan di Indonesia.

Secara konseptual, kejahatan siber (*cybercrime*) didefinisikan sebagai tindakan ilegal yang melibatkan komputer, jaringan komputer, atau perangkat terhubung sebagai alat, target, atau tempat terjadinya kejahatan (Safitri et al., 2026). Kejahatan ini dibagi menjadi dua kategori utama: *cyber-dependent crimes* (kejahatan yang hanya bisa dilakukan menggunakan teknologi komputer, seperti penyebaran malware atau peretasan server) dan *cyber-enabled crimes* (kejahatan tradisional yang dipermudah oleh teknologi, seperti penipuan online, pencurian identitas, dan pelecehan siber) (Widiasari & Thalib, 2022). Kejahatan siber modern bersifat asimetris dan transnasional, sehingga penegakan hukumnya sering terkendala batas wilayah negara (*jurisdiction*) serta tingkat anonimitas yang tinggi dari para pelaku (Siregar et al., 2022). Dampak dari eskalasi kejahatan siber ini secara langsung mengancam privasi dan keamanan data sensitif pengguna, yang menuntut adanya mekanisme perlindungan hak-hak digital secara lebih proaktif (Ardhana & Nurmiati, 2026).

Pemerintah Indonesia telah mengupayakan instrumen regulasi guna meminimalkan dampak kejahatan siber dan kebocoran data. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua atas UU Informasi dan Transaksi Elektronik (UU ITE) merupakan pilar utama regulasi siber nasional (Kristianti & Kurniasi, 2024). UU PDP secara spesifik mengatur hak-hak subjek data, kewajiban pengendali data, penunjukan *Data Protection Officer* (DPO), serta sanksi administratif berupa denda hingga 2% dari pendapatan tahunan bagi korporasi yang lalai, serta sanksi pidana bagi pihak yang secara ilegal mengumpulkan atau memalsukan data pribadi (Ramadhan, 2025). Sementara itu, UU ITE berfokus pada legalitas transaksi elektronik dan sanksi pidana bagi akses ilegal (*unauthorized access*) terhadap sistem komputer (Kristianti & Kurniasi, 2024).

Sistem keamanan perimeter tradisional yang mengandalkan konsep benteng pertahanan seperti *firewall* dan VPN kini dianggap tidak lagi memadai untuk menahan serangan siber modern. Sebagai gantinya, konsep *Zero Trust Architecture* (ZTA) yang merujuk pada standar NIST SP 800-207 diusulkan sebagai paradigma baru. Konsep ini menekankan prinsip "jangan pernah percaya, selalu verifikasi" (*never trust, always verify*). Dalam model *Zero Trust*, tidak ada pengguna atau perangkat yang dipercaya secara bawaan, baik berada di dalam maupun di luar jaringan internal. Setiap permintaan akses wajib melalui proses autentikasi ketat, otorisasi dinamis, enkripsi menyeluruh, dan inspeksi perilaku berkelanjutan untuk meminimalkan dampak eksploitasi lateral jika peretas berhasil menembus satu titik pertahanan (Siregar et al., 2022).

Keamanan informasi tidak hanya diselesaikan melalui solusi teknologi, tetapi juga memerlukan manajemen risiko yang terstruktur. Organisasi internasional telah menetapkan standar sertifikasi seperti ISO/IEC 27001 Sistem Manajemen Keamanan Informasi (SMKI) (Alfi et al., 2023). Standar ini memandu organisasi dalam mengidentifikasi aset informasi, menganalisis risiko ancaman, mengimplementasikan kontrol keamanan yang sesuai (seperti manajemen akses, enkripsi, keamanan fisik, dan kelangsungan bisnis), serta melakukan evaluasi berkala untuk perbaikan

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 6 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1554-1559

berkelanjutan. Penerapan standar ini sangat krusial bagi instansi yang mengelola infrastruktur penting nasional guna meminimalkan peluang terjadinya kegagalan sistem (Aryapranata et al., 2024).

2. METODE

2.1. Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif-konseptual dengan metode studi kepustakaan (*library research*). Desain konseptual ini bertujuan untuk memetakan risiko keamanan siber di Indonesia dan merumuskan strategi mitigasi penanggulangan secara integratif dengan membandingkan landasan teori, regulasi, dan data insiden riil.

2.2. Teknik Pengumpulan Data

Data yang digunakan dalam penelitian ini adalah data sekunder. Proses pengumpulan data dilakukan dengan mengompilasi laporan berkala mengenai serangan siber nasional dari BSSN, dokumen regulasi nasional (UU PDP dan UU ITE), serta artikel jurnal ilmiah terakreditasi nasional maupun internasional yang dipublikasikan dalam rentang waktu lima tahun terakhir (2021–2026). Pencarian literatur dilakukan melalui pangkalan data akademis Google Scholar dan portal SINTA dengan kata kunci penelusuran: "keamanan siber", "cybersecurity", "modus kejahatan TI", "ransomware Indonesia", dan "perlindungan data pribadi".

2.3. Prosedur Analisis dan Sintesis Data

Langkah-langkah analisis data yang diterapkan adalah sebagai berikut: a. Analisis Kasus & Komparatif: Memetakan efektivitas pertahanan siber di berbagai organisasi melalui evaluasi studi kasus insiden keamanan siber besar di Indonesia, secara spesifik serangan ransomware *Brain Cipher* yang melumpuhkan Pusat Data Nasional (PDN) pada Juni 2024. b. Sintesis Strategi: Mengaitkan celah-celah keamanan yang ditemukan dengan standar manajemen internasional (seperti ISO/IEC 27001) dan konsep arsitektur keamanan siber terbaru (*Zero Trust*) untuk merumuskan usulan solusi strategis yang komprehensif bagi ekosistem digital nasional.

3. ANALISA DAN PEMBAHASAN

3.1. Analisis Modus Kejahatan Teknologi Informasi Terkini

Pelaku kejahatan TI kini memanfaatkan teknologi mutakhir seperti kecerdasan buatan (*Artificial Intelligence*) untuk memperlancar serangan mereka. Beberapa modus utama yang diidentifikasi dijabarkan pada Tabel 1.

Tabel 1. Karakteristik Modus Kejahatan TI Terkini di Indonesia

Modus Kejahatan	**Deskripsi Teknis**	**Dampak Utama**	**Keterlibatan AI**
Ransomware Adaptif	Enkripsi database sistem target dengan tuntutan uang tebusan crypto.	Penghentian operasional layanan publik dan kerugian finansial skala besar.	AI digunakan untuk memutasi kode malware secara otomatis guna menghindari antivirus.
Phishing & Social Eng.	Manipulasi psikologis korban melalui tautan/pesan palsu.	Pencurian kredensial akun, pembobolan akses admin, dan transfer dana ilegal.	Penggunaan Deepfake Voice dan teks generatif untuk meniru identitas otoritas.
Kebocoran Data	Eksploitasi kerentanan database untuk mengunduh data pribadi pengguna.	Penjualan data di dark web dan peningkatan kasus penipuan pinjaman online.	Automasi pemindaian celah keamanan port database secara massal.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 6 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1554-1559

DDoS	Pembobolan lalu lintas server menggunakan botnet secara simultan.	Layanan online lumpuh total (downtime) dalam periode waktu tertentu.	Botnet terkoordinasi secara cerdas berdasarkan beban traffic server sasaran.

Sumber: Data diolah dari laporan BSSN dan analisis literatur (Alfi et al., 2023; Safitri et al., 2026; Siregar et al., 2022).

Selain penipuan finansial, kemunculan teknologi deepfake juga memicu ancaman baru berupa pelecehan siber (*cyber harassment*) berbasis manipulasi visual dan suara di media sosial, yang mengharuskan penerapan etika profesi yang ketat di kalangan pengembang AI (Nurmiati & Rizqi, 2026). Di sisi lain, pembobolan data pribadi pengguna di Indonesia terus menjadi komoditas bernilai tinggi di pasar gelap. Lemahnya perlindungan pada basis data instansi pemerintah maupun korporasi swasta menjadi penyebab utama tingginya keberhasilan eksploitasi data siber (Kristianti & Kurniasi, 2024).

3.2. Studi Kasus: Insiden Ransomware Pusat Data Nasional (PDN) 2024

Pada Juni 2024, Indonesia dikejutkan oleh insiden lumpuhnya Pusat Data Nasional Sementara (PDNS) 2 yang berlokasi di Surabaya. Serangan ini disebabkan oleh ransomware varian baru bernama *Brain Cipher*, yang merupakan pengembangan dari strain *LockBit 3.0* (Siregar et al., 2022). Insiden ini melumpuhkan lebih dari 282 instansi pemerintah pusat dan daerah, termasuk sistem keimigrasian di bandara internasional, sistem pendaftaran beasiswa pendidikan, serta portal perizinan ekspor-impor.

Analisis forensik digital pascainsiden mengidentifikasi beberapa kelemahan teknis yang fatal di balik keberhasilan serangan tersebut (Ferian Fajar et al., 2025):

a. **Ketiadaan Backup yang Redundan**: Ditemukan bahwa hanya sekitar 2% dari total data yang disimpan di PDNS 2 yang memiliki sistem pencadangan otomatis (*backups*) di Pusat Data Nasional cadangan di Batam. Ketiadaan *cold backup* yang terisolasi secara fisik dari jaringan utama membuat data yang terenkripsi tidak dapat dipulihkan secara instan tanpa membayar tebusan.
b. **Kelemahan Tata Kelola Akses (Identity Access Management)**: Penyerang masuk menggunakan kredensial administratif yang bocor melalui metode phishing atau eksploitasi *Remote Desktop Protocol* (RDP) yang terbuka di jaringan internet publik tanpa otentikasi ganda (MFA).
c. **Absennya Deteksi Ancaman Aktif (Threat Hunting)**: Aktivitas mencurigakan di dalam sistem terdeteksi terlambat. Penyerang telah berada di dalam jaringan selama berminggu-minggu (*lateral movement*) sebelum akhirnya mengeksekusi enkripsi data secara massal.

Dampak dari insiden PDNS 2024 tidak hanya berupa kerugian material, tetapi juga merusak reputasi pemerintah dalam hal kedaulatan data dan perlindungan privasi hak asasi warga negara (Nurrohmah & Nur, 2026). Kejadian ini menjadi momentum penting yang menegaskan bahwa pengonsolidasian data nasional ke dalam satu server fisik tanpa protokol keamanan bertaraf internasional justru menciptakan *Single Point of Failure* yang sangat berbahaya.

3.3. Faktor Pemicu Kerentanan Keamanan Siber Nasional

Berdasarkan kajian literatur dan evaluasi insiden PDN, kelemahan pertahanan siber di Indonesia dipicu oleh interaksi tiga faktor utama yang saling berkaitan:

3.3.1. Faktor Manusia (*People*)

Tingkat literasi digital masyarakat Indonesia yang rendah menjadi celah psikologis yang paling sering dieksploitasi oleh peretas melalui taktik rekayasa sosial. Pengguna internet cenderung mudah mengklik tautan tidak dikenal atau menginstal aplikasi bajakan yang disusupi malware. Di level organisasi, terdapat kekurangan akut terhadap tenaga ahli keamanan siber bersertifikasi internasional (seperti CISSP atau CEH). Banyak instansi menugaskan staf TI umum yang tidak memiliki kompetensi khusus untuk mengelola sistem keamanan informasi yang kompleks. Selain itu, etika profesi praktisi TI memegang peranan krusial dalam pencegahan insiden

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 6 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1554-1559

kebocoran data internal, di mana pelanggaran etika dan kelalaian prosedur sering menjadi celah masuk utama serangan siber (Suci Anugrah et al., 2025).

3.3.2. Faktor Proses (*Process*)

Ketiadaan standar operasional keamanan siber yang seragam di kementerian dan lembaga menyebabkan koordinasi penanganan insiden berjalan lambat. Protokol mitigasi bencana teknologi informasi umumnya hanya tertulis di atas kertas tanpa pernah diuji coba melalui latihan simulasi serangan secara berkala (*cyber drill*). Ketiadaan audit keamanan siber secara berkala dan independen membuat kerentanan sistem baru diketahui setelah serangan berhasil terjadi (Alfi et al., 2023).

3.3.3. Faktor Teknologi (*Technology*)

Penggunaan perangkat lunak bajakan dan sistem operasi yang sudah usang tanpa dukungan pembaruan keamanan (*end-of-life systems*) masih marak digunakan di lingkungan administrasi pemerintahan (Aryapranata et al., 2024). Selain itu, tidak diterapkannya enkripsi yang kuat pada basis data pribadi warga negara membuat peretas dapat dengan mudah membaca dan memperjualbelikan data curian tersebut tanpa hambatan teknis yang berarti (Kristianti & Kurniasi, 2024; Widiasari & Thalib, 2022).

3.4. Startegi Penanggulangan Siber Intergratif

Mengacu pada kelemahan sistemik yang telah dijabarkan, dirumuskan strategi penanggulangan siber nasional yang bertumpu pada empat pilar utama:

3.4.1. Penerapan Teknologi Pertahanan Modern (Zero Trust & Kriptografi)

Setiap pengelola infrastruktur kritis wajib mengadopsi arsitektur *Zero Trust* guna mencegah pergerakan lateral peretas di dalam sistem (Siregar et al., 2022). Penggunaan enkripsi kuat pada level database dan jalur komunikasi data (*kriptografi*) harus distandardisasi di bawah pengawasan BSSN (Kristianti & Kurniasi, 2024). Di samping itu, implementasi strategi pencadangan data dengan formula 3-2-1 (3 salinan data, disimpan pada 2 jenis media berbeda, dengan 1 salinan disimpan secara offline di lokasi terpisah) harus diwajibkan bagi seluruh pengelola data publik untuk mengantisipasi serangan ransomware.

3.4.2. Penegakan Kepatuhan Regulasi UU Perlindungan Data Pribadi (UU PDP)

Pemerintah harus mempercepat pembentukan Lembaga Pengawas PDP independen yang bertugas mengawasi jalannya kepatuhan organisasi terhadap UU PDP (Ramadhan, 2025). Lembaga ini harus diberikan kewenangan untuk melakukan audit kepatuhan secara acak, menjatuhkan sanksi administratif berupa denda finansial yang signifikan bagi instansi pemerintah maupun swasta yang lalai, serta menuntut akuntabilitas publik dari pengelola data pascainsiden kebocoran data terjadi.

3.4.3. Penguatan Infrastruktur Tanggap Insiden (CSIRT)

Pembentukan *Computer Security Incident Response Team* (CSIRT) harus dipercepat hingga ke tingkat pemerintah daerah kabupaten/kota dan kementerian sektoral (Aji, 2023). Tim ini harus dibekali alat pemantauan lalu lintas data aktif (*Security Operations Center*/SOC) dan memiliki wewenang penuh untuk melakukan isolasi jaringan secara instan begitu terdeteksi adanya anomali traffic atau aktivitas peretasan (Ramadhan, 2025).

3.4.4. Program Literasi Siber dan Sertifikasi SDM Nasional

BSSN bersama Kementerian Komunikasi dan Informatika perlu menggalakkan kampanye kebersihan siber (*cyber hygiene*) secara masif kepada masyarakat luas, mencakup edukasi penggunaan pengelola kata sandi (*password manager*), aktivasi otentikasi ganda (MFA), dan pengenalan taktik phishing. Di sisi lain, program beasiswa sertifikasi profesi keamanan siber bagi aparatur sipil negara dan lulusan perguruan tinggi perlu ditingkatkan guna mengisi kekosongan SDM ahli di bidang pertahanan siber.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 6 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1554-1559

4. KESIMPULAN

Ancaman siber di Indonesia telah berkembang ke tingkat yang sangat mengkhawatirkan dengan pola serangan yang semakin canggih memanfaatkan kecerdasan buatan. Modus operandi seperti ransomware adaptif dan phishing berbasis AI tidak lagi hanya menyasar kerugian finansial personal, melainkan kedaulatan data nasional. Penanggulangan ancaman ini membutuhkan sinergi yang berkelanjutan antara penguatan teknis melalui arsitektur Zero Trust, penegakan kepatuhan terhadap regulasi UU Perlindungan Data Pribadi (UU PDP), pembentukan tim tanggap insiden CSIRT yang responsif, serta peningkatan literasi siber bagi masyarakat umum. Keamanan siber tidak boleh lagi dipandang sebagai sekadar urusan teknis divisi TI, melainkan pilar utama ketahanan nasional di era digital.

Pemerintah disarankan untuk segera mempercepat pembentukan Komisi Pengawas Perlindungan Data Pribadi independen dan mewajibkan audit sistem manajemen keamanan informasi berbasis ISO/IEC 27001 secara tahunan bagi seluruh pengelola data publik. Bagi peneliti selanjutnya, disarankan untuk mengkaji lebih dalam mengenai pemanfaatan teknologi *Machine Learning* untuk deteksi dini serangan ransomware pada server cloud pemerintahan guna memperkuat sistem pertahanan otomatis nasional.

REFERENCES

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2). https://doi.org/10.7454/jkskn.v6i2.10082

Ardhana, R. K., & Nurmiati, E. (2026). *Analisis Dampak Cyber Crime terhadap Keamanan dan Privasi Data Pengguna Teknologi Informasi di Era*. *04*(02), 890–897.

Aryapranata, A., Al Rasyid, Y., Agsena, Y. P., & Hermanto, S. (2024). Keamanan Siber dalam Era Digital: Tantangan dan Solusi. *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi Dan Sistem Komputer*, *8*(2), 109–114. https://doi.org/10.55886/infokom.v8i2.932

Ferian Fajar, H., Fadhila, A., & Yades, M. K. (2025). REDESAIN KEBIJAKAN HUKUM KEAMANAN DAN KETAHANAN SIBER: STUDI KASUS SERANGAN SIBER PADA PUSAT DATA NASIONAL TAHUN 2024. *Jurnal Rechtsvinding*, *14*(2), 285–314. https://www.tempo.co/politik/kronologi-pusat-data-nasional-jebol-hingga-desakan-menkominfo-budi-arie-

Novera Kristianti, & Ririn Kurniasi. (2024). Peraturan dan Regulasi Keamanan Siber di Era Digital. *Satya Dharma : Jurnal Ilmu Hukum*, *7*(1), 297–310. https://ejournal.iahntp.ac.id/index.php/satya-dharma/article/view/1243

Nurmiati, E., & Rizqi, F. N. (2026). *Tinjauan Etika Profesi Teknologi Informasi Terhadap Deepfake Harassment di Media Sosial : Systematic Literature Review*. (2025), 368–376.

Nurrohmah, A., & Nur, H. (2026). *Analisis Yuridis Kebocoran Data pada Pusat Data Nasional Sementara (PDNS) dalam Perspektif Undang-Undang Perlindungan Data Pribadi*. *1*, 239–245.

Ramadhan, G. (2025). Analisis Strategi Keamanan Nasional Indonesia dalam Menghadapi alam Menghadapi Ancaman Siber. *Jurnal Hukum, Administrasi Publik, Dan Ilmu Komunikasi*, *2*(April), 257–266. https://ejournal.appihi.or.id/index.php/Konstitusi/article/view/722?

Safitri, A. N., Qamar, N., & Ilham, M. A. (2026). *Kejahatan Siber Ancaman Nyata di Era Digial Indonesia*. *I*(2).

Siregar, M., Fitria, S., & Ema, D. (2022). *Pengaruh Self-Management Terhadap Prokrastinasi Akademik Pada Mahasiswa Tingkat Akhir* (Vol. 4).

Suci Anugrah, Muhammad Zaky Himawan, Nabila Raihana Qalby, & Evy Nurmiati. (2025). Pengaruh Etika Profesi Terhadap Keamanan Informasi dalam Konteks Kebocoran Data BSI (Bank Syariah Indonesia): Studi Literatur Sistematis. *Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi*, *11*(2), 106–112. https://doi.org/10.34010/jtk3ti.v11i2.17033

Widiasari, N. K. N., & Thalib, E. F. (2022). The Impact of Information Technology Development on Cybercrime Rate in Indonesia. *Journal of Digital Law and Policy*, *1*(2), 73–86. https://doi.org/10.58982/jdlp.v1i2.165