**SAMMAJIVA : Jurnal Penelitian Bisnis dan Manajemen**
**Vol.1, No.2 Juni 2023**
e-ISSN: 2985-9611; p-ISSN: 2986-0415, Hal 172-191
DOI: https://doi.org/10.47861/sammajiva.v1i2.226

# Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File

**(1)Edy Soesanto, (2) Achmad Romadhon, (3 Bima Dwi Mardika, (4 Moch Fahmi Setiawan**

(1)Teknik Perminyakan, Universitas Bhayangkara Jakarta Raya
(2)Manajemen, Universitas Bhayangkara Jakarta Raya
(3)Manajemen, Universitas Bhayangkara Jakarta Raya
(4)Manajemen, Universitas Bhayangkara Jakarta Raya

*Korespondensi penulis: edy.soesanto@dsn.ubharajaya.ac.id*

**Abstrak**

Ancaman terhadap objek vital dan keamanan file berkembang pesat. Penjahat dunia maya menjadi lebih licik dan terampil dalam mengeksploitasi kerentanan keamanan dalam sistem digital. Untuk meningkatkan keamanan siber, diperlukan analisis menyeluruh terhadap ancaman yang dihadapi di lingkungan digital dan solusi yang dapat diterapkan. Tujuan penelitian ini adalah menganalisis objek vital, mengidentifikasi tantangan utama dalam melindunginya dari serangan dunia maya, mengevaluasi dan mengusulkan langkah dan strategi untuk meningkatkan keamanan file, dan mengkaji studi kasus terkait ancaman dan solusi di lingkungan digital. pendekatan kualitatif dengan menggunakan teknik wawancara dan observasi. Potensi ancaman cybercrime di Indonesia antara lain hacking, cracking, cyber sabotage, dan spyware. Proses manajemen risiko melibatkan identifikasi, penilaian, penanganan, dan pengendalian risiko. Untuk mengantisipasi ancaman tersebut, diperlukan tenaga ahli teknologi yang mendukung pengembangan sistem pertahanan negara tingkat lanjut dan mendirikan pusat komando keamanan siber.

**Kata Kunci**: Manajemen Risiko, Keamanan Siber, Potensi Ancaman

***Abstract***

*The threat to vital objects and file security is rapidly evolving. Cybercriminals are becoming more cunning and skilled at exploiting security vulnerabilities in digital systems. In order to enhance cybersecurity, a thorough analysis of the threats faced in the digital environment and the applicable solutions is necessary. The objectives of this research are to analyze vital objects, identify key challenges in protecting them from cyber attacks, evaluate and propose measures and strategies to improve file security, and examine case studies related to threats and solutions in the digital environment.This research adopts a qualitative approach using interview and observation techniques. Potential cybercrime threats in Indonesia include hacking, cracking, cyber sabotage, and spyware. The risk management process involves identifying, assessing, treating, and controlling risks. To anticipate these threats, it is essential to have technology experts who support the development of advanced national defense systems and establish a cybersecurity command center.*

*Received April 30, 2023; Revised Mei 02, 2023; Accepted Juni 07, 2023*
* Edy Soesanto, edy.soesanto@dsn.ubharajaya.ac.id

***Keywords:*** *Risk Management, Cybersecutity, Potential Threats*

## PENDAHULUAN

Dalam pesatnya perkembangan era digital, objek vital dan pengamanan file menjadi perhatian utama dalam konteks keamanan cyber. Objek vital, seperti infrastruktur kritis, data sensitif, dan sistem penting lainnya, memiliki nilai strategis yang tinggi dan rentan terhadap serangan cyber yang dapat menyebabkan kerugian yang signifikan. Pengamanan file juga menjadi krusial dalam lingkungan digital, karena file-file tersebut sering kali mengandung informasi penting dan rahasia yang harus dilindungi dari akses yang tidak sah.

Ancaman terhadap objek vital dan keamanan file semakin berkembang dengan cepat. Penjahat cyber semakin cerdik dan terampil dalam mengeksploitasi celah keamanan dalam sistem digital, termasuk serangan malware, peretasan, dan serangan jaringan yang kompleks. Selain itu, dengan semakin banyaknya data yang dikirim dan disimpan secara elektronik, tantangan dalam mengamankan file juga semakin kompleks.

Oleh karena itu, diperlukan analisis mendalam tentang ancaman yang dihadapi dalam lingkungan digital dan solusi yang dapat diterapkan untuk meningkatkan keamanan cyber. Studi kasus tentang serangan yang pernah terjadi dan langkah-langkah yang diambil untuk mengatasinya menjadi sangat penting dalam memahami kompleksitas dan tantangan yang dihadapi dalam pengamanan objek vital dan file.

kami akan menganalisis berbagai ancaman yang ada dalam lingkungan digital dan menggali solusi yang dapat diterapkan untuk meningkatkan keamanan cyber. Kami juga akan menggunakan beberapa studi kasus nyata untuk memperoleh wawasan praktis tentang bagaimana serangan cyber terjadi serta cara atau langkah dalam menangani serangan ini. Melalui penelitian ini, diharapkan meningkatkan pemahaman dan ilmu mendalam pentingnya pengamanan objek vital dan file dalam lingkungan digital, serta upaya yang dapat dilakukan untuk meningkatkan keamanan cyber secara keseluruhan.

Berikut adalah tiga rumusan masalah yang relevan untuk penelitian tentang pengamanan cyber yang diperlukan:

1. Apa saja objek vital yang perlu diamankan dalam lingkungan digital, dan apa tantangan utama yang dihadapi dalam melindungi objek vital tersebut dari serangan cyber
2. Bagaimana pengamanan file dapat ditingkatkan dalam lingkungan digital untuk melindungi informasi sensitif dan rahasia dari akses yang tidak sah?
3. Bagaimana analisis terhadap studi kasus ancaman dan solusi dalam lingkungan digital dapat memberikan wawasan praktis dalam meningkatkan keamanan cyber secara efektif dan efisien?

Berdasarkan rumusan masalah tersebut maka tujuan penelitian ini adalah sebagai berikut:

1. Menganalisis objek vital yang perlu diamankan dalam lingkungan digital untuk memahami pentingnya perlindungan terhadap mereka dan mengidentifikasi tantangan utama yang dihadapi dalam melindungi objek vital tersebut dari serangan cyber.
2. Mengevaluasi dan mengusulkan langkah-langkah dan strategi untuk meningkatkan pengamanan file dalam lingkungan digital guna melindungi informasi sensitif dan rahasia dari akses yang tidak sah.
3. Mengkaji studi kasus terkait ancaman dan solusi dalam lingkungan digital untuk memperoleh wawasan praktis tentang serangan cyber yang pernah terjadi serta langkah-langkah yang diambil untuk mengatasi mereka, dengan tujuan memperoleh pemahaman yang lebih baik tentang cara meningkatkan keamanan cyber secara keseluruhan.

Berikut adalah beberapa manfaat penelitian tentang pengamanan cyber:

1. Meningkatkan kesadaran dan pemahaman tentang ancaman cyber: Penelitian ini berkontribusi menambah pengetahuan mengenai jenis-jenis serangan cyber, metode yang digunakan oleh penyerang, dan kerentanan yang ada dalam sistem. Hal ini membantu meningkatkan kesadaran dan kewaspadaan terhadap ancaman cyber di kalangan individu, organisasi, dan masyarakat pada umumnya.
2. Meningkatkan keamanan sistem dan data: Penelitian ini dapat menghasilkan penemuan baru dalam hal keamanan cyber dan memberikan wawasan tentang praktik terbaik dalam melindungi sistem dan data dari serangan cyber. Ini dapat membantu organisasi mengidentifikasi celah keamanan serta cara atau langkah yang dibutuhkan untuk meningkatkan keamanan mereka, sehingga mengurangi risiko serangan dan kebocoran data.

3. Mendukung pengembangan kebijakan keamanan cyber: Penelitian ini dapat memberikan dasar pengetahuan yang diperlukan untuk merumuskan kebijakan keamanan cyber yang efektif. Dengan memahami ancaman dan tantangan yang dihadapi, kebijakan dapat dirancang untuk melindungi infrastruktur teknologi informasi, mendorong praktik keamanan yang baik, dan meningkatkan koordinasi antara pihak-pihak yang terlibat dalam pengamanan cyber.
4. Mendorong inovasi dan pengembangan solusi baru: Penelitian ini dapat merangsang inovasi dalam pengembangan teknologi dan solusi baru untuk menghadapi ancaman cyber. Temuan penelitian dapat digunakan untuk mengembangkan alat dan metode baru dalam mendeteksi, mencegah, dan merespons serangan cyber. Hal ini dapat memperkuat kemampuan organisasi dalam menghadapi ancaman yang terus berkembang di dunia cyber.
5. Menjaga kepercayaan publik: Dengan meningkatkan keamanan cyber, penelitian ini dapat membantu menjaga kepercayaan publik terhadap sistem dan layanan digital. Dengan adanya perlindungan yang lebih baik terhadap data pribadi dan informasi sensitif, masyarakat dapat merasa lebih aman dan percaya dalam menggunakan teknologi digital dan berpartisipasi dalam dunia online.

## KAJIAN PUSTAKA

Tabel 1. Penelitian Terdahulu yang Relevan

| No. | Author dan Tahun | Hasil Riset | Persamaan | Perbedaan |
|---|---|---|---|---|
| 1. | Sari, N. W. (2018) | kemajuan teknologi informasi berbasis komputer telah mengakibatkan munculnya tindakan kejahatan cyber yang melibatkan penggunaan data atau informasi yang dikirim melalui internet | Persamaan Penelitian ini menganalisis kejahatan teknologi informasi dengan metode observasi | Perbedaan: analisis regulasi hukum yang berkaitan dengan kejahatan cyber dalam konteks teknologi informasi. |

| No. | Author dan Tahun | Hasil Riset | Persamaan | Perbedaan |
|---|---|---|---|---|
| 2. | Li, Y., & Liu, Q. (2021) | Cyberspace dan teknologi terkait merupakan salah satu sumber kekuatan yang paling penting di milenium ketiga. Karakteristik dari dunia maya, seperti biaya masuk yang rendah, anonimitas, kerentanan, dan ketidaksimetrisan, telah menciptakan fenomena penyebaran kekuatan, yang berarti jika pemerintah sejauh ini telah membagi permainan kekuasaan di antara mereka, maka harus ada aktor lain, seperti perusahaan swasta, kelompok teroris terorganisir, dan individu, | Analisis survei dan tinjauan menyeluruh terhadap perkembangan standar yang disajikan dalam bidang keamanan siber dan menyelidiki tantang yang dihadapi | Perbedaaan analisis terbatas pada ancaman dan tidak membahas pada manajemen resiko dan langkah yang dilakukan |
| 3. | Connolly, L. Y., & Wall, D. S. (2019) | Respons terhadap crypto-ransomware menjadi lebih kompleks oleh hubungan nuansa antara aspek teknis (malware yang mengenkripsi) dan aspek manusia (rekayasa sosial yang masih menjadi penyebab utama infeksi). Akibatnya, tidak ada 'senjata ajaib' teknologi sederhana yang akan | Menggunakan analisis wawancara dan dokumen dalam ancaman keamanan cyber | Fokus pada pengamanan crypto-ransomware |

| No. | Author dan Tahun | Hasil Riset | Persamaan | Perbedaan |
|---|---|---|---|---|
| | | menghapus ancaman crypto-ransomware. Sebaliknya, diperlukan pendekatan berlapis yang terdiri dari langkah-langkah sosio-teknis, manajer garis depan yang berdedikasi, dan dukungan aktif dari manajemen senior | | |
| 4. | Fatani, A., Dahou, A., Al-Qaness, M. A., Lu, S., & Abd Elaziz, M. (2022) | Performa tinggi menggunakan algoritma SI yang baru dikembangkan, Aquila optimizer (AQU). Selain itu, untuk menilai kualitas pendekatan IDS yang dikembangkan, empat dataset publik yang terkenal, yaitu CIC2017, NSL-KDD, BoT-IoT, dan KDD99 | Persamaan penelitian ini adalah analisis pengembangan keamanan cyber s | Perbedaannya adlah fokus pada Aquila optimizer (AQU) untuk metode pengembangan |
| 5. | Kuzmenko, O. V., Dotsenko, T. V., & Skrynka, L. O. (2021). | Hasil dari penelitian ini menganalisis efektivitas sistem nasional dalam mengatasi kejahatan siber dan legalisasi dana ilegal berdasarkan metode Kaplan-Meier. Efektivitas sistem nasional dalam mengatasi kejahatan siber dan legalisasi dana | Analisis efektivitas sistem nasional dalam mengatasi kejahatan siber | Perbedaan penelitian pengendalian legalisasi dana ilegal dengan membangun peta kata kunci bibliometrik menggunakan |

| No. | Author dan Tahun | Hasil Riset | Persamaan | Perbedaan |
|---|---|---|---|---|
| | | ilegal bergantung pada rentang waktu setelah terdeteksinya pelanggaran. Signifikansi praktis dari penerapan model yang dikembangkan adalah membentuk dasar analitis untuk pengambilan keputusan manajemen lebih lanjut oleh Bank Nasional Ukraina, Layanan Pemantauan Keuangan Negara, dan Pelayanan Keamanan Ukraina dalam konteks efektivitas sistem nasional dalam mengatasi kejahatan siber dan legalisasi dana ilegal, serta kebutuhan untuk penyesuaian | | perangkat lunak VOSviewer |

Teori yang dikaji dalam penelitian ini adalah sebagai berikut :

a. Objek Vital

Dalam pengamanan cyber, objek vital merujuk pada sistem atau infrastruktur yang memiliki nilai strategis dan sensitif, seperti sistem keuangan, instalasi kelistrikan, atau data penting yang terkait dengan keamanan nasional. Untuk melindungi objek vital ini, berbagai strategi dan teknologi telah dikembangkan. Contohnya, sistem deteksi intrusi yang canggih, pembaruan keamanan yang teratur, dan segmentasi jaringan untuk mengisolasi objek vital dari lingkungan yang tidak aman. Penelitian terkait perlindungan objek vital ini penting untuk memahami tantangan dan solusi yang terkait dalam konteks pengamanan file dan keamanan cyber

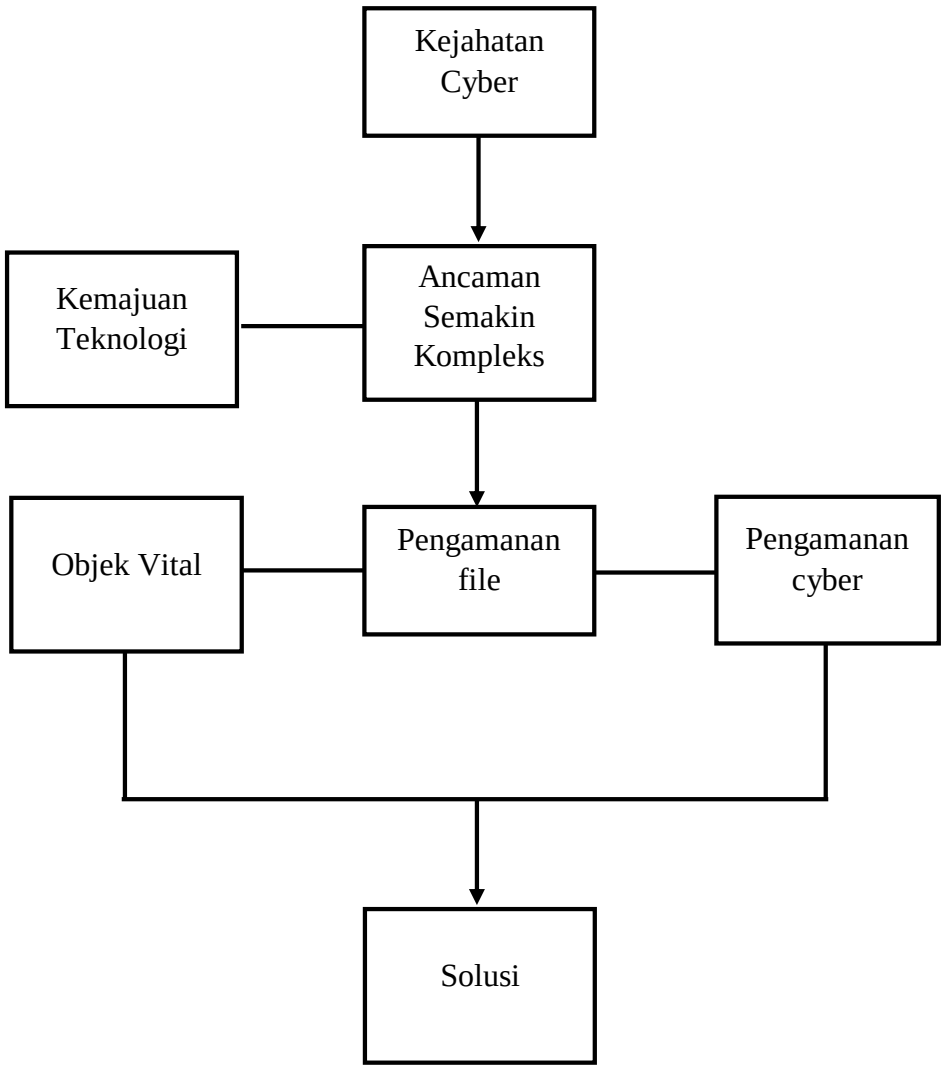
b. Pengamanan File

Pengamanan file dalam lingkungan digital melibatkan perlindungan informasi sensitif dan rahasia dari akses yang tidak sah. Langkah-langkah yang dapat diambil termasuk enkripsi data, penggunaan otentikasi yang kuat, pengawasan akses, dan kebijakan keamanan yang ketat. Penting untuk melakukan penelitian tentang metode dan teknologi pengamanan file yang efektif, serta kebijakan dan praktik terbaik dalam pengelolaan dan perlindungan file digital. Dalam konteks pengamanan file, analisis ancaman yang mungkin timbul, seperti serangan ransomware atau pencurian data, dapat memberikan wawasan tentang langkah-langkah yang perlu diambil untuk melindungi file-file tersebut

c. Analisis dan peningkatan keamanan Cyber

Studi kasus terkait ancaman dan solusi dalam lingkungan digital memberikan wawasan praktis tentang serangan yang pernah terjadi dan tindakan yang diambil untuk mengatasi mereka. Dalam penelitian ini, analisis terhadap berbagai studi kasus serangan cyber dapat memberikan pemahaman mendalam tentang taktik dan strategi yang berhasil dalam melawan serangan cyber. Dari sini, dapat ditemukan solusi efektif untuk meningkatkan keamanan cyber secara keseluruhan, termasuk upaya identifikasi ancaman yang lebih baik, peningkatan kesadaran pengguna tentang kebijakan keamanan, dan pengembangan sistem deteksi dini yang kuat.

## KERANGKA PEMIKIRAN




## HIPOTESIS

1. Objek vital dalam lingkungan digital, seperti infrastruktur kritis dan data sensitif, rentan terhadap serangan cyber yang dapat menyebabkan kerugian yang signifikan. Dengan penerapan langkah-langkah pengamanan yang tepat, seperti sistem deteksi intrusi yang canggih dan pembaruan keamanan yang teratur, objek vital tersebut dapat dilindungi dengan lebih efektif.

2. Dengan menerapkan tindakan pengamanan yang tepat, seperti enkripsi data, penggunaan otentikasi yang kuat, dan kesadaran terhadap kebijakan keamanan, pengamanan file dalam lingkungan digital dapat ditingkatkan, sehingga informasi sensitif dan rahasia dapat terlindungi dari akses yang tidak sah.
3. Melalui analisis studi kasus tentang ancaman dan solusi dalam lingkungan digital, dapat ditemukan wawasan praktis tentang taktik dan strategi yang berhasil digunakan dalam menghadapi serangan cyber. Dengan mempelajari pengalaman orang lain dalam menghadapi serangan, dapat dikembangkan pendekatan yang lebih efektif untuk meningkatkan keamanan cyber secara keseluruhan.

## METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif yang bertujuan untuk mendapatkan pemahaman mendalam tentang ancaman keamanan cyber yang ada di lingkungan digital serta mengidentifikasi solusi yang efektif untuk meningkatkan keamanan tersebut.

Pertama, dalam proses pengumpulan data, peneliti menggunakan teknik wawancara dengan melibatkan ahli keamanan cyber, pengguna internet, dan pihak terkait dalam lingkungan digital. Wawancara ini dilakukan secara langsung atau melalui telepon, dan tujuannya adalah untuk mendapatkan pandangan dan pengetahuan ahli tentang jenis-jenis ancaman keamanan cyber yang sering terjadi, teknik yang digunakan oleh penyerang, serta dampak yang ditimbulkan oleh ancaman tersebut. Selain itu, wawancara juga dilakukan dengan pengguna internet untuk memahami pengalaman mereka dalam menghadapi ancaman keamanan cyber dan tindakan yang mereka lakukan untuk melindungi diri.

Selain wawancara, penelitimenggunakan teknik observasi. Observasi dilakukan dengan mengamati perilaku pengguna dalam menghadapi ancaman keamanan cyber di lingkungan digital. Peneliti mengamati bagaimana pengguna berinteraksi dengan perangkat dan aplikasi, tindakan yang mereka lakukan untuk menjaga keamanan data pribadi, serta respon mereka terhadap ancaman yang muncul.

Selanjutnya, peneliti melakukan analisis dokumen. Data dikumpulkan dari berbagai sumber terkait seperti laporan keamanan cyber, studi kasus, dan artikel ilmiah yang berkaitan dengan ancaman keamanan cyber dan solusi yang telah diterapkan. Data dari sumber-sumber ini dianalisis

agar memperoleh suatu informasi mendalam tentang karakteristik dan dampak dari ancaman keamanan cyber, serta solusi yang telah ada atau diusulkan untuk meningkatkan keamanan di lingkungan digital.

Setelah data terkumpul, peneliti melakukan analisis kualitatif terhadap data tersebut. Data dari wawancara, observasi, dan analisis dokumen dianalisis secara tematik untuk mengidentifikasi pola, tema, dan hubungan antara ancaman keamanan cyber yang ada, karakteristik dan dampaknya, serta solusi yang dapat diterapkan.

Penelitian ini memiliki fokus pada studi kasus tentang ancaman keamanan cyber di lingkungan digital. Dengan menggunakan metode kualitatif dan melibatkan berbagai sumber data, diharapkan penelitian ini memberikan kontribusi pengetahuan mendalam membahas cyber yang dihadapi dan solusi yang efektif untuk meningkatkan keamanan di lingkungan digital.

Penelitian ini menggunakan analisis data mendalam untuk memperoleh informasi dan data. analisis yang digunakan dalam penelitian ini adalah :

1. Transkripsi Wawancara: Jika telah dilakukan wawancara dengan ahli keamanan cyber, pengguna internet, dan pihak terkait, langkah pertama adalah mentranskripsikan rekaman wawancara tersebut ke dalam teks. Transkripsi ini memungkinkan untuk melihat secara rinci apa yang dibahas dalam wawancara dan mempermudah analisis data selanjutnya.
2. Analisis Tematik: Pada tahap ini, data dari transkripsi wawancara, catatan observasi, dan dokumen yang terkumpul dianalisis secara tematik. Tema-tema utama dan sub-tema yang muncul dalam data diidentifikasi dan dikategorikan. Contohnya, tema-tema seperti "jenis ancaman keamanan cyber", "dampak ancaman keamanan cyber", "solusi yang telah diterapkan", dan "saran untuk peningkatan keamanan cyber" dapat muncul dalam analisis ini.
3. Koding Data: Setelah tema-tema dan sub-tema diidentifikasi, langkah selanjutnya adalah memberikan kode pada bagian-bagian data yang relevan dengan tema tersebut. Koding dapat dilakukan dengan memberikan label atau tanda pada potongan teks yang mencerminkan tema atau sub-tema yang telah diidentifikasi sebelumnya. Hal ini memungkinkan untuk mengumpulkan dan mengorganisir data yang relevan dengan tema tertentu.
4. Pembentukan Kategori dan Sub-Kategori: Setelah proses koding selesai, kategori dan sub-kategori dapat dibentuk berdasarkan temuan dalam data. Kategori adalah pengelompokan

tema yang lebih luas, sementara sub-kategori merupakan pengelompokan yang lebih spesifik. Contoh kategori mungkin termasuk "Ancaman Fisik", "Ancaman Jaringan", atau "Ancaman Sosial", sementara sub-kategori dapat mencakup detail seperti "Malware", "Serangan DDoS", atau "Phishing".

5. Analisis Silang: Dalam analisis silang, peneliti melihat keterkaitan antara tema atau kategori yang berbeda dalam data. Misalnya, dapat dianalisis bagaimana solusi tertentu telah diterapkan untuk mengatasi jenis ancaman keamanan cyber yang spesifik, atau bagaimana pengguna mengalami dampak dari ancaman tertentu dan mengambil tindakan pencegahan yang sesuai.
6. Penafsiran dan Interpretasi: Pada tahap ini, peneliti memberikan penafsiran dan interpretasi terhadap data yang telah dikodekan dan dikategorikan. Hal ini melibatkan menganalisis pola, perbedaan, dan kesamaan dalam data, serta mengaitkan temuan dengan teori atau kerangka konseptual yang relevan. Penafsiran ini memberikan pemahaman mendalam tentang ancaman keamanan cyber yang ada, karakteristik dan dampaknya, serta solusi yang dapat diterapkan.
7. Penyusunan Laporan: Langkah terakhir adalah penyusunan laporan penelitian yang mencakup hasil analisis data, temuan, kesimpulan, dan rekomendasi. Laporan penelitian harus disusun dengan jelas dan logis, menggambarkan dengan rinci temuan-temuan yang relevan dengan tujuan penelitian.

Metode analisis data yang disebutkan di atas dapat disesuaikan dengan kebutuhan penelitian dan karakteristik data yang dikumpulkan. Dalam penelitian kualitatif, fleksibilitas dan kemampuan untuk menemukan pola-pola baru dalam data sangat penting untuk menghasilkan pemahaman yang mendalam tentang subjek penelitian.

Penelitian ini menggunakan beberapa tahap untuk memperoleh informasi dan data. Tahapan penelitian yang digunakan dalam penelitian ini adalah

1. Tahap Perencanaan: a. Menetapkan tujuan penelitian: Menentukan tujuan penelitian yang mencakup analisis ancaman keamanan cyber, karakteristik dan dampaknya, serta pengembangan solusi yang efektif. b. Merumuskan pertanyaan penelitian: Merumuskan pertanyaan penelitian yang relevan dengan tujuan penelitian, misalnya, "Apa saja jenis ancaman keamanan cyber yang sering terjadi di lingkungan digital?" c. Menyusun kerangka

teoritis: Membuat kerangka teoritis yang mendukung penelitian dan memberikan pemahaman tentang konsep dan teori terkait keamanan cyber. d. Merancang desain penelitian: Memilih pendekatan penelitian kualitatif, menentukan teknik pengumpulan data, dan mengidentifikasi populasi atau subjek penelitian yang relevan.

2. Tahap Pengumpulan Data: a. Wawancara: Melakukan wawancara dengan ahli keamanan cyber, pengguna internet, dan pihak terkait untuk mendapatkan pemahaman mendalam tentang ancaman keamanan cyber dan solusi yang telah ada. b. Observasi: Mengamati perilaku pengguna dalam menghadapi ancaman keamanan cyber di lingkungan digital. c. Analisis Dokumen: Mengumpulkan laporan keamanan cyber, studi kasus, dan artikel ilmiah terkait untuk mendapatkan data yang relevan.
3. Tahap Analisis Data: a. Transkripsi: Mentranskripsikan rekaman wawancara ke dalam teks jika diperlukan. b. Analisis Tematik: Mengidentifikasi tema-tema utama dan sub-tema yang muncul dalam data yang telah terkumpul. c. Koding Data: Memberikan kode pada potongan data yang relevan dengan tema dan sub-tema yang telah diidentifikasi. d. Pembentukan Kategori dan Sub-Kategori: Mengelompokkan kode-kode yang serupa menjadi kategori dan sub-kategori yang lebih luas dan spesifik. e. Analisis Silang: Menganalisis keterkaitan antara tema, kategori, dan sub-kategori yang berbeda dalam data. f. Penafsiran dan Interpretasi: Memberikan penafsiran dan interpretasi terhadap temuan dalam data dengan mengaitkan dengan teori atau kerangka konseptual yang relevan.
4. Tahap Penyusunan Laporan: a. Menyusun laporan penelitian yang mencakup pengantar, tujuan penelitian, kerangka teoritis, metodologi penelitian, temuan, kesimpulan, dan rekomendasi. b. Menulis dengan jelas dan sistematis untuk menjelaskan temuan-temuan yang relevan dengan tujuan penelitian. c. Melakukan revisi dan penyempurnaan laporan penelitian berdasarkan umpan balik dan saran dari pihak yang berkompeten.

Tahapan penelitian ini dapat disesuaikan dengan kebutuhan penelitian Anda, namun secara umum, tahapan tersebut mencakup perencanaan, pengumpulan data, analisis data, dan penyusunan laporan.

Lokasi Penelitian: Penelitian ini dapat dilakukan di beberapa lokasi yang relevan, seperti:

1. Institusi keamanan cyber, seperti lembaga keamanan cyber nasional atau perusahaan keamanan cyber yang memiliki ahli di bidang keamanan digital.

2. Organisasi atau perusahaan dengan sistem digital yang rentan terhadap ancaman keamanan cyber.
3. Tempat-tempat di mana pengguna internet aktif berinteraksi dengan lingkungan digital, seperti pusat perbelanjaan, ruang kerja bersama, atau sekolah/lembaga pendidikan.

Waktu Penelitian: Waktu penelitian dapat disesuaikan dengan kompleksitas dan ruang lingkup penelitian yang diinginkan. Namun, disarankan untuk mengalokasikan waktu yang memadai untuk setiap tahapan penelitian, seperti:

1. Tahap Perencanaan: Biasanya membutuhkan beberapa minggu untuk merumuskan pertanyaan penelitian, menyusun kerangka teoritis, dan merancang desain penelitian.
2. Tahap Pengumpulan Data: Bergantung pada jumlah responden dan ketersediaan mereka, tahap pengumpulan data dapat memakan waktu beberapa minggu hingga beberapa bulan.
3. Tahap Analisis Data: Analisis data kualitatif biasanya membutuhkan waktu yang cukup, tergantung pada jumlah data yang terkumpul. Ini dapat memakan waktu beberapa minggu hingga beberapa bulan.
4. Tahap Penyusunan Laporan: Menulis dan menyusun laporan penelitian biasanya membutuhkan waktu beberapa minggu.

## PEMBAHASAN

Perkembangan globalisasi serta kemajuan teknologi informasi berperan dalam perubahan kehidupan manusia yang signifikan. Teknologi informasi memungkinkan komunikasi antar individu serta negara menjadi lebih mudah dan cepat, tanpa terpengaruh batasan ruang dan waktu (Scholte, 2000). Teknologi informasi berkontribusi pada negara memberikan dua hal yang m yang menjadikan kontribusi penting teknologi informasi untukmendorong pertumbuhan ekonomi global. Pertama, teknologi informasi meningkatkan permintaan terhadap produk-produk teknologi informasi itu sendiri. Permintaan yang tinggi terhadap produk-produk ini berdampak positif pada pertumbuhan industri teknologi informasi serta mendorong inovasi dan pengembangan lebih lanjut dalam sektor ini.Kedua, teknologi informasi mempermudah transaksi bisnis, terutama dalam bidang keuangan dan bisnis secara umum. Kemajuan dalam teknologi informasi telah mengubah cara transaksi dilakukan, dengan adanya sistem pembayaran elektronik, e-commerce, dan layanan

perbankan online. Hal ini memungkinkan perusahaan untuk melakukan bisnis secara efisien dan efektif, serta membuka peluang baru untuk ekspansi pasar global. (Raharjo 2002).

Indonesia termasuk dalam lima negara terbesar dalam penggunaan media sosial, yang memiliki potensi positif (kekuatan) dan potensi negatif (kerentanan/kelemahan) terkait adanya perang siber. Penggunaan oleh masyarakat dalam media sosial dapat menjadi ancaman terhadap kedaulatan negara. Namun, media sosial dapat menjadi sumber pengetahuan tentang teknologi informasi, komunikasi, dan digital, yang memungkinkan masyarakat menjadi terampil dalam dunia digital. Kegiatan penggunaan tehnologi digital di Indonesia adalah potensi dalam perang siber. Penggunaan teknologi informasi dapat mudah disusupi hacker atau cracker berbagai negara, yang mengakibatkan kerawanan informasi, terutama dalam hal transmisi informasi intelijen melalui dunia maya.Indonesia memiliki posisi yang signifikan dalam penggunaan media sosial, yang memiliki implikasi positif dalam peningkatan pemahaman masyarakat tentang dunia digital. Namun, hal ini juga membawa kerentanan terhadap serangan siber yang dapat mengancam kedaulatan negara dan keamanan informasi yang dikirim melalui platform digital.

Potensi ancaman kejahatan siber (cyber crime) dapat berdampak pada perang siber. Berikut ini adalah beberapa potensi ancaman kejahatan siber di Indonesia:

- Hacking

  Salah satu penyebab terjadinya serangan siber, mulai dari niat iseng untuk menguji keamanan hingga penolakan terhadap pemerintah. Contoh kasus saat pemilihan presiden tahun 2014 adalah penyebaran kabar bahwa situs KPU telah mengalami peretasan disebabkan hacker. Indikasinya adalah situs KPU mengalami gangguan akses yang menyebabkan tidak bisa diakses sementara waktu.
- Cracking

  Di Indonesia, terjadi kasus peretasan yang dilakukan oleh individu yang dikenal sebagai "carder". Mereka menggunakan metode ini untuk mencuri informasi kartu kredit yaitu mengintip data kartu kredit para nasabah. Setelah mendapatkan akses ke informasi tersebut, para peretas kemudian mencoba untuk mengakses data sensitif serta harta simpanan nasabah pada bank untuk suatu keuntungan pelaku.
- Cyber Sabotage

Cyber sabotage adalah tindakan secara sengaja untuk mengganggu, merusak, atau menghancurkan data atau sistem jaringan komputer sedang dihubungkan internet. Tindakan ini merupakan metode paling ditakuti banyak perusahaan besar di seluruh dunia.

- Spyware

  Program tersebut merujuk pada perangkat lunak yang merekam secara diam-diam penggunaan online yaitu merekam data cookies atau registry. Data berhasil terekam kemudian dapat dikirim atau dijual kepada perusahaan atau individu tertentu, kemudian dapat menggunakan informasi tersebut untuk mengirim iklan yang tidak diinginkan atau menyebarkan virus berbahaya. Sayangnya, di Indonesia telah terjadi 24 kasus infeksi malware yang terkait dengan penggunaan perbankan online oleh masyarakat.

Sebaiknya dilakukan identifikasi risiko kejahatan siber secara teratur untuk mengidentifikasi faktor pemicu terjadinya kejahatan siber. Dalam prosesnya berbagai aspek berpotensi dalam memicu kejahatan siber perlu dievaluasi. Kemajuan teknologi penyadapan secara cepat dalam meretas media sosial menjadi ancaman signifikan dalam era perang siber. Menurut Abdul Wahid dan Mohammad Labib, ada dua jenis utama kejahatan siber, yaitu Pertama, kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas: Ini mengacu pada kejahatan di mana pelaku menggunakan TI sebagai alat atau sarana untuk melancarkan tindakan kriminal. Contoh-contohnya termasuk serangan siber, penipuan online, pencurian identitas, penyebaran malware, atau kegiatan ilegal lainnya yang memanfaatkan teknologi informasi sebagai alat pelaksanaan. Kedua kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (TI) sebagai sasaran: Ini mengacu pada kejahatan yang ditujukan langsung pada sistem dan fasilitas TI itu sendiri. Contohnya termasuk serangan siber terhadap infrastruktur TI, pencurian data, sabotase terhadap jaringan komputer, atau eksploitasi kelemahan dalam sistem keamanan TI.

Dengan berbagai kasus kejahatan siber di Indonesia, stabilitas keamanan dan ketertiban nasional menghadapi ancaman signifikan. Eskalasi kejahatan siber telah mencapai tingkat yang cukup tinggi. Penanganan tindakan melawan hukum dalam dunia maya tidaklah mudah hanya dengan hukum positif konvensional. Hal ini disebabkan hubungan yang kompleks antara lima faktor terkait, yaitu pelaku kejahatan, korban kejahatan, reaksi sosial terhadap kejahatan, dan hukum.Meskipun hukum memiliki peran penting untuk pencegahan serta penanggulangan kejahatan, menciptakan regulasi hukum yang responsif berbagai bidang hukum merubah dengan

cepat seperti teknologi informasi bukanlah tugas yang mudahDalam menghadapi tantangan kejahatan siber, perlu adanya kerja sama lintas sektor, termasuk pemerintah, lembaga penegak hukum, sektor swasta, dan masyarakat secara keseluruhan. Selain itu, pengembangan kerangka hukum yang adaptif dan penggunaan teknologi keamanan siber yang canggih menjadi penting dalam memerangi kejahatan siber yang terus berkembang. (Suhariyanto 2022).

Menurut Rahmawati (2017), terdapat beberapa tahapan proses manajemen risiko dalam menghadapi ancaman kejahatan siber (cyber crime) yang dapat diterapkan, yang dijelaskan sebagai berikut:

- Identify

  Identifikasi risiko kejahatan siber dengan berkala untuk mengidentifikasi penyebab terjadinya kejahatan siber. Dalam proses ini, semua aspek yang memiliki potensi menyebabkan kerugian harus diidentifikasi secara seksama. Setelah identifikasi dilakukan, seluruh risiko yang telah teridentifikasi kemudian diukur. Pengukuran risiko pada ancaman kejahatan siber mengacu pada dua ukuran utama, yaitu probabilitas dan dampak.
- Assess

  Penilaian risiko atau Assess pada dasarnya bertujuan untuk mengevaluasi tingkat risiko yang timbul dari kejahatan siber dan dampaknya terhadap berbagai aspek kehidupan, termasuk pertahanan negara. Penilaian risiko kejahatan siber tidak dapat dilakukan secara langsung, tetapi dapat menggunakan tabel matriks untuk pengukuran risiko.Dalam penilaian risiko kejahatan siber, tabel matriks menggambarkan tingkat probabilitas serta dampak dari ancaman kejahatan siber yang teridentifikasi.
- Treat

  Memutuskan tindakan dan respons terhadap risiko kejahatan siber melibatkan menentukan risiko tersebut akan diterima, dialihkan, diminimalisir, atau dihindari. Dalam kasus pencurian informasi dan data terjadi individu maupun lembaga, upaya minimalisir risiko adalah penting.
- Control

  Dalam rangka mengevaluasi keberhasilan manajemen risiko, adalah penting untuk terus melakukan pemantauan dan penyesuaian. Dalam proses pemantauan tersebut, disarankan adanya mekanisme peringatan dini bagi pihak yang bertanggung jawab atas keamanan, seperti

Kementerian Pertahanan Republik Indonesia, sehingga mampu mengambil tindakan yang dibutuhkan dalam mengantisipasi ancaman kejahatan siber.

Untuk mengantisipasi kejahatan siber, penting untuk melibatkan ahli teknologi memiliki kemampuan mendukung pengembangan sistem pertahanan negara yang canggih serta modern. Perlu adanya suatu kerja sama industri pertahanan Indonesia diperlukan untuk menciptakan program sistem informasi dan komunikasi yang memiliki daya saing dengan negara lain. Pengembangan sistem pertahanan siber di Indonesia dipengaruhi oleh dua faktor, yaitu regulasi dan keberadaan pusat komando siber. Pemerintah perlu membuat regulasi yang baik dan sesuai untuk mengatur pengembangan keamanan siber nasional.

Salah satu hal penting lainnya adalah membangun pusat komando keamanan pertahanan siber. Pemerintah Indonesia berencana untuk melaksanakan cyber operation command yang bertujuan menjadi pusat komando pertahanan siber di Indonesia. Dengan beroperasinya pusat komando tersebut, diharapkan bangsa Indonesia akan lebih siap dalam mengantisipasi ancaman nontradisional, yaitu kejahatan siber (cyber crime) yang semakin meningkat dampaknya terhadap kedaulatan NKRI. Ini merupakan langkah besar yang perlu terus diperkuat agar dapat berfungsi secara optimal. Diperlukan regulasi yang tepat dan kemampuan dalam hal sistem pertahanan negara, jaringan, aplikasi, serta kebijakan yang terkait dengan keamanan siber.

## KESIMPULAN

Pencurian informasi dan data yang bersifat rahasia sebagai ancaman kejahatan siber ditujukan untuk menyerang individu, instansi pemerintah, dan militer yang dapat mengancam pertahanan suatu negara. Oleh karena itu, penting untuk memiliki manajemen risiko yang terkait dengan informasi dan komunikasi guna mengurangi kerentanan terhadap penyalahgunaan informasi dan data di ruang siber (cyberspace), yang dapat berdampak pada banyak warga negara dan informasi yang bersifat rahasia. Selain memiliki pertahanan negara yang kuat, juga dibutuhkan dukungan hukum yang saling terkait dan saling mempengaruhi dalam menghadapi ancaman kejahatan siber..

## SARAN

Pemerintah perlu terus menyosialisasikan penggunaan teknologi informasi dengan benar. Selain itu, pemerintah harus memberlakukan sanksi hukum bagi siapa pun yang melakukan kejahatan di dunia maya yang berbasis teknologi informasi. Aparat terkait, seperti aparat hukum yang ada, harus memiliki pemahaman yang maksimal tentang hukum cyber. Mengingat kejahatan dalam lingkungan teknologi informasi terus berkembang dengan modus dan bentuk yang beragam, hal ini menjadi penting agar kejahatan siber tidak semakin meluas dan tumbuh subur dalam masyarakat

## DAFTAR PUSTAKA

Anderson, R., & Moore, T. (2019). Why Crypto Tokens Matter: How to Ensure Security in the Internet of Things. Harvard Business Review. Retrieved from https://hbr.org/2019/01/why-crypto-tokens-matter

Buchholz, R. A. (2019). Secure Coding in C and C++. CRC Press.

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures.Computers & Security,87, 101568.

Denning, D. E. (2016). The Ethics of Cyber Conflict. Journal of Military Ethics, 15(4), 299-314.

Dhillon, G., & Backhouse, J. (2001). Information system security management in the new millennium. Communications of the ACM, 44(4), 125-128.

Duffield, A., Whitty, M. T., & Greenhill, A. (2019). Cyber Threats and Cyber Self-Defence for the Individual. Computers & Security, 83, 259-273.

Fatani, A., Dahou, A., Al-Qaness, M. A., Lu, S., & Abd Elaziz, M. (2022). Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system.Sensors,22(1), 140.

Goel, S., & Chen, Y. (2019). Machine Learning for Cybersecurity. CRC Press.

Khan, K., & Malluhi, Q. M. (2017). Cybersecurity: The Essential Body of Knowledge. CRC Press.

Kuzmenko, O. V., Dotsenko, T. V., & Skrynka, L. O. (2021). Economic and Mathematical Modelling of the Effectiveness of the National System for Countering Cyber Fraud and Criminal Proceeds Legalisation Based on Survival Analysis Methods. Scientific Bulletin of Mukachevo State University. Series "Economics, 8(1), 144-153.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments.Energy Reports,7, 8176-8186.

Luiijf, E., & Nieuwenhuis, L. J. M. (2019). Cyber Security as Competitive Advantage. Journal of Cyber Policy, 4(2), 161-178.

Mitnick, K. D., & Simon, W. L. (2017). The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. Little, Brown and Company.

Moore, T., & Chatterjee, S. (2018). The Quantified Employee: A Study of Employee Monitoring in the Digital Workplace. European Journal of Information Systems, 27(3), 251-267.

Ponemon Institute. (2020). Cost of a Data Breach Report 2020. Retrieved from https://www.ibm.com/security/data-breach

Sari, N. W. (2018). Kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer. Jurnal Surya Kencana Data Dinamika Masalah Hukum dan Keadilan. 5(2): 577-592

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

Solms, R. V., & Solms, K. (2020). An Analysis of the Human Aspect of Cybersecurity in Organizations: An Exploratory Study. Computers & Security, 95, 101889.

Symantec Corporation. (2020). Internet Security Threat Report 2020. Retrieved from https://www.symantec.com/security-center/threat-report