INSOLOGI: Jurnal Sains dan Teknologi
https://journal.literasisains.id/index.php/INSOLOGI
ISSN 2828-4984 (Media Online) | ISSN 2828-4992 (Media Cetak)
Vol. 2 No. 6 (Desember 2023) 1124-1130
DOI: 10.55123/insologi.v2i6.2847
Submitted: 19-11-2023 | Accepted: 02-12-2023 | Published: 28-12-2023

Strategi Pengamanan Cyber: Lingkup Kerjasama dalam Menghadapi Ancaman Cyber

Chintya Pradilla Putri[1], Widya Anggraini[2*], Yuda Mahendra Hasibuan[3], Nurbaiti[4]
[1,2*,3,4]Universitas Islam Negeri Sumatera Utara
Email: [1]chintya.pradilla2003@gmail.com, [2*]anggraini312@gmail.com, [3]yudahsb201@gmail.com, [4]nutbaiti@uinsu.ac.id

Abstract

Threats to the security of important objects and files are growing rapidly. In the rapid development of the digital era, the security of goods and files has become very important, which is a big problem in terms of cyber security. Cybercriminals are more clever and skilled at exploiting information security gaps in digital systems. Improving cyber security requires a thorough analysis of the threats faced in the digital environment and the solutions that can be implemented. The aim of this research is to analyze the main targets, identify the main challenges to protect them from cyber attacks, evaluate and recommend measures and strategies to improve file security, explore case studies related to threats and solutions in the digital environment. The qualitative approach uses data collection methods. Potential threats of cyber crime in Indonesia include hacking, cracking, cyber sabotage and spyware. The risk management process includes identification, evaluation, handling and controlling risks. To anticipate danger, therefore, technology experts are needed to support the development of defense systems in developed countries and establish a cyber security command center.

Keywords: *Risk Management, Cyber Security, Potential Threats.*

Abstrak

Ancaman terhadap keamanan objek dan file penting berkembang pesat. Dalam pesatnya perkembangan era digital, keamanan barang dan file menjadi hal yang sangat penting yang merupakan masalah besar dalam hal keamanan cyber. Penjahat dunia maya melakukannya lebih cerdik dan terampil dalam memanfaatkan celah keamanan informasi dalam sistem digital. Untuk meningkatkan keamanan cyber memerlukan analisis menyeluruh terhadap ancaman yang dihadapi dalam lingkungan digital dan solusi yang dapat diterapkan. Tujuan dari penelitian ini adalah untuk menganalisis target utama, mengidentifikasi tantangan utama untuk melindungi mereka dari serangan dunia maya, mengevaluasi dan merekomendasikan langkah-langkah dan strategi untuk meningkatkan keamanan file, mengeksplorasi studi kasus terkait ancaman dan solusi di lingkungan digital. Pendekatan kualitatif menggunakan metode pengumpulan data. Potensi ancaman kejahatan cyber di Indonesia termasuk hacking, cracking, sabotase cyber dan spyware. Proses manajemen risiko meliputi identifikasi, evaluasi, penanganan dan pengendalian resiko. Untuk mengantisipasi bahaya Oleh karena itu, dibutuhkan tenaga ahli teknologi untuk mendukung pengembangan sistem pertahanan negara maju dan mendirikan pusat komando keamanan cyber.

Kata Kunci: Manajemen Resiko, Keamanan Cyber, Potensi Ancaman.

1. PENDAHULUAN

Dalam pesatnya perkembangan era digital, keamanan barang dan file menjadi hal yang sangat penting yang merupakan masalah besar dalam hal keamanan cyber. Item penting seperti infrastruktur penting, data sistem sensitif dan sistem kritis lainnya memiliki nilai strategis yang tinggi dan rentan serangan cyber yang dapat menimbulkan kerugian serius. Keamanan file juga penting dalam lingkungan digital karena file-file ini sering kali berisi informasi-informasi penting dan rahasia yang harus dilindungi dari

akses tidak sah. Ancaman terhadap keamanan objek dan file penting berkembang pesat. Penjahat dunia maya menjadi lebih pintar dan mahir dalam mengeksploitasi kerentanan dalam sistem digital, termasuk serangan malware, peretasan, dan serangan jaringan canggih. (Bram Ronald Sanjaya et al., 2022)

Selain itu tantangan pun muncul seiring dengan semakin banyaknya data yang dikirim dan disimpan secara elektronik, melindungi file juga semakin sulit. Oleh karena itu, diperlukan analisis menyeluruh terhadap ancaman yang akan datang, lingkungan digital dan solusi yang dapat diterapkan untuk meningkatkan keamanan cyber. Studi tentang serangan yang telah terjadi dan cara untuk mengalahkannya menjadi sangat penting untuk memahami kompleksitas dan tantangan terkait melindungi objek dan file penting. (Edy Soesanto et al., 2023)

Penelitian ini menganalisis berbagai ancaman di lingkungan digital dan mengeksplorasi solusi yang dapat diterapkan untuk meningkatkan keamanan cyber. Penelitian ini juga menggunakan beberapa studi kasus nyata untuk mendapatkan pemahaman praktis tentang serangan cyber dan metode atau langkah untuk menghadapi serangan tersebut. Melalui penelitian ini, diharapkan dapat menambah pemahaman dan memperdalam pengetahuan akan pentingnya keamanan barang data dan file penting dalam lingkungan digital dan upaya untuk meningkatkannya keamanan cyber umum.

Berikut ini adalah tiga masalah penting yang diperlukan untuk penelitian keamanan cyber:

1. Objek penting apa yang harus dilindungi dalam lingkungan digital dan apa tantangan utama untuk melindungi objek penting tersebut dari serangan cyber?
2. Bagaimana keamanan file dapat ditingkatkan dalam lingkungan digital untuk melindungi informasi sensitif dan rahasia dari akses tidak sah?
3. Bagaimana analisis studi kasus ancaman dan solusi di lingkungan digital dapat memberikan wawasan yang dapat ditindaklanjuti untuk meningkatkan keamanan cyber secara efektif dan efisien?

Berdasarkan tiga masalah diatas, tujuan penelitian ini adalah sebagai berikut:

1. Menganalisis objek-objek penting yang perlu dilindungi dalam lingkungan digital, untuk memahami pentingnya melindunginya dan mengidentifikasi tantangan utama untuk melindungi objek-objek penting tersebut dari serangan cyber.
2. Mengevaluasi dan mengusulkan langkah-langkah dan strategi untuk meningkatkan keamanan file di lingkungan digital untuk melindungi informasi sensitif dan rahasia dari akses yang tidak sah.
3. Mengkaji studi kasus ancaman dan solusi di lingkungan digital untuk mendapatkan wawasan praktis mengenai serangan cyber di masa lalu dan langkah-langkah yang diambil untuk memeranginya. Tujuannya adalah untuk mendapatkan pemahaman yang lebih baik tentang cara meningkatkan keamanan cyber secara keseluruhan.

Berikut beberapa manfaat mempelajari keamanan cyber:

1. Meningkatkan kesadaran dan pemahaman tentang ancaman cyber. Studi ini akan membantu meningkatkan pengetahuan tentang jenis serangan cyber, metode yang digunakan penyerang, dan kerentanan sistem. Ini membantu meningkatkan kesadaran dan kesadaran akan ancaman dunia maya di antara manusia, organisasi, dan masyarakat.
2. Meningkatkan keamanan sistem dan data. Penelitian ini dapat menghasilkan penemuan baru di bidang keamanan cyber dan memberikan wawasan mengenai praktik terbaik untuk melindungi sistem dan data dari serangan cyber. Hal ini dapat membantu organisasi mengidentifikasi kesenjangan keamanan dan cara atau tindakan

yang diperlukan untuk meningkatkan keamanan, mengurangi risiko serangan dan pelanggaran data.

3. Mendukung pengembangan kebijakan keamanan cyber. Penelitian ini dapat memberikan pengetahuan yang dibutuhkan untuk mengembangkan kebijakan keamanan cyber yang efektif. Dengan mengidentifikasi ancaman dan tantangan ke depan, kebijakan dapat dikembangkan untuk melindungi infrastruktur TI, mendorong praktik keamanan yang baik, dan meningkatkan koordinasi antar pemangku kepentingan keamanan cyber.
4. Mempromosikan inovasi dan pengembangan solusi baru. Penelitian ini dapat mendorong inovasi dalam pengembangan teknologi dan solusi baru untuk memerangi ancaman dunia maya. Hasil penelitian dapat digunakan untuk mengembangkan alat dan metode baru untuk mendeteksi, mencegah, dan merespons serangan dunia maya. Hal ini dapat memperkuat kemampuan organisasi dalam menghadapi ancaman yang terus berkembang di dunia cyber.
5. Mendukung kepercayaan masyarakat. Dengan meningkatkan keamanan cyber, penelitian ini dapat membantu menjaga kepercayaan masyarakat terhadap sistem dan layanan digital. Perlindungan yang lebih baik terhadap data pribadi dan informasi sensitif dapat membantu orang merasa lebih aman dan percaya diri saat menggunakan teknologi digital dan berpartisipasi di dunia online.

2. TINJAUAN TEORITIS

Teori-teori yang dikaji dalam penelitian ini antara lain:

Data-Data Penting

Dalam keamanan cyber, objek penting mengacu pada sistem atau infrastruktur mereka mempunyai nilai strategis dan sensitif, seperti sistem keuangan, instalasi listrik atau informasi permasalahan penting yang berkaitan dengan keamanan nasional. Berbeda untuk melindungi objek penting ini strategi dan teknologi yang dikembangkan. Misalnya, sistem deteksi intrusi peningkatan pembaruan keamanan rutin dan segmentasi jaringan untuk isolasi barang-barang penting di lingkungan berbahaya. Penelitian terkait konservasi kawasan penting ini penting untuk memahami tantangan dan solusi keamanan file dan keamanan cyber. (Handrini Ardiyanti, 2014)

Keamanan Berkas

Melindungi file di lingkungan digital memerlukan perlindungan data sensitif dan rahasia terhadap akses yang tidak sah. Kegiatan yang harus dilakukan termasuk enkripsi data, penggunaan otentikasi yang kuat, kontrol akses dan kebijakan keamanan yang ketat. Penting untuk mempelajari metode dan teknologi perlindungan file yang efektif dan praktik serta praktik terbaik untuk mengelola dan perlindungan file digital. Analisis potensi ancaman keamanan file insiden seperti serangan ransomware atau pencurian data dapat memberikan informasi informasi tentang langkah-langkah yang harus diambil untuk melindungi file-file ini. (Handrini Ardiyanti, 2014)

Analisis dan Peningkatan Keamanan Cyber

Studi kasus terkait ancaman dan solusi lingkungan digital memberikan gambaran informasi praktis mengenai serangan yang telah terjadi dan tindakan untuk mengatasinya mereka. Berbagai studi kasus serangan cyber dapat dianalisis dalam penelitian ini memberikan gambaran komprehensif tentang taktik dan strategi yang sukses melawan serangan cyber. Solusi perbaikan yang efektif dapat ditemukan di sana, keamanan siber

secara umum, termasuk peningkatan upaya deteksi ancaman, peningkatan kesadaran pengguna tentang praktik keamanan dan pengembangan sistem deteksi dini yang kuat. (Handrini Ardiyanti, 2014)

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan tujuan untuk memperoleh pemahaman mendalam mengenai ancaman keamanan cyber di lingkungan digital dan mencari solusi efektif untuk meningkatkan keamanannya. Dalam proses pengumpulan data, peneliti melakukan analisis dokumen. Informasi dikumpulkan dari berbagai sumber relevan seperti laporan keamanan cyber, studi kasus dan artikel penelitian terkait ancaman keamanan cyber dan solusi yang diterapkan. Data dari sumber-sumber ini dianalisis untuk memberikan wawasan mendalam tentang sifat dan dampak ancaman keamanan cyber serta solusi yang ada atau yang diusulkan untuk meningkatkan keamanan lingkungan digital.

Setelah data terkumpul, peneliti melakukan analisis data secara kualitatif. Data analisis dokumen dianalisis secara tematis untuk mengidentifikasi pola, tema dan hubungan antara ancaman keamanan siber yang ada, karakteristik dan dampaknya, serta solusi yang dapat diterapkan. Penelitian ini berfokus pada studi kasus ancaman keamanan cyber di lingkungan digital. Dengan menggunakan metode kualitatif dan menggunakan sumber data yang berbeda, penelitian ini diharapkan dapat memberikan pengetahuan mendalam tentang masalah siber dan solusi efektif untuk meningkatkan keamanan lingkungan digital.

4. HASIL DAN PEMBAHASAN

Perkembangan globalisasi dan perkembangan teknologi informasi membawa perubahan besar dalam kehidupan masyarakat. Dengan bantuan teknologi informasi, komunikasi antar manusia dan negara menjadi lebih mudah dan cepat, tanpa terpengaruh oleh keterbatasan ruang dan waktu. Teknologi informasi membantu suatu negara memberikan dua hal yang menjadikan teknologi informasi memberikan kontribusi penting terhadap pertumbuhan ekonomi global. Pertama, teknologi informasi meningkatkan permintaan terhadap produk teknologi informasi itu sendiri. Tingginya permintaan terhadap produk-produk tersebut berdampak positif terhadap pertumbuhan industri teknologi informasi dan mendorong inovasi dan pengembangan industri. Kedua, teknologi informasi memudahkan dunia usaha, khususnya di bidang keuangan dan kehidupan bisnis. Perkembangan teknologi informasi telah mengubah cara transaksi pembayaran dilakukan, seiring dengan memasuki pasar sistem pembayaran elektronik, perdagangan elektronik, dan layanan perbankan online. Hal ini memungkinkan perusahaan melakukan bisnis secara efektif dan efisien serta membuka peluang baru untuk perluasan pasar global. (Putri Bilqis Oktaviani & Anggraeni Silvia, 2021)

Indonesia termasuk dalam lima negara teratas dalam penggunaan media sosial dengan potensi positif (kekuatan) dan potensi negatif (kerentanan/kelemahan) terkait perang cyber. Penggunaan media sosial oleh publik dapat mengancam kedaulatan suatu negara. Namun media sosial dapat menjadi sumber informasi, komunikasi, dan teknologi digital yang memungkinkan masyarakat belajar di dunia digital. Pemanfaatan teknologi digital di Indonesia memungkinkan terjadinya perang cyber. Pemanfaatan teknologi informasi dapat dengan mudah disusupi oleh para hacker atau cracker dari berbagai negara, sehingga menyebabkan rentannya suatu informasi, khususnya dalam penyampaian informasi intelijen melalui dunia maya. Indonesia mempunyai posisi

penting dalam pemanfaatan media sosial yang mempunyai peran penting dalam pemanfaatan teknologi informasi. berdampak positif terhadap pemahaman masyarakat terhadap dunia digital. Namun hal tersebut juga menimbulkan kerentanan terhadap serangan cyber yang dapat mengancam kedaulatan negara dan keamanan informasi yang dikirimkan melalui platform digital. (Putri Bilqis Oktaviani & Anggraeni Silvia, 2021)

Potensi ancaman kejahatan cyber dapat berdampak pada perang siber. Berikut beberapa potensi ancaman kejahatan siber di Indonesia:

- Peretasan

Salah satu penyebab serangan cyber, mulai dari niat tidak sengaja untuk menguji keamanan hingga penolakan pemerintah. Contoh kejadian pada Pilpres 2014 adalah tersebarnya berita bahwa website KPU diretas oleh hacker. Referensi tersebut menunjukkan bahwa website KPU mengalami kendala akses sehingga tidak dapat diakses untuk sementara waktu.

- Cracking

Di Indonesia, peristiwa peretasan dilakukan oleh oknum yang dikenal dengan sebutan "carde". Cara ini mereka gunakan untuk mencuri informasi kartu kredit, yakni melihat informasi kartu kredit pelanggan. Setelah mendapatkan akses ke informasi ini, para peretas mencoba mendapatkan akses ke informasi sensitif dan simpanan nasabah di bank untuk kepentingan penjahat.

- Sabotase dunia maya

Sabotase dunia maya adalah tindakan yang disengaja untuk mengganggu, merusak, atau menghancurkan informasi atau sistem jaringan komputer yang terhubung ke Internet. Kegiatan ini merupakan praktik yang paling ditakuti oleh banyak perusahaan besar di seluruh dunia.

- Perangkat mata-mata

Sebuah program mengacu pada perangkat lunak yang secara diam-diam mencatat penggunaan jaringan, mis. cookie atau data pendaftaran. Data yang berhasil disimpan kemudian dapat dikirim atau dijual kepada perusahaan atau individu tertentu yang kemudian dapat menggunakan data tersebut untuk mengirimkan iklan yang tidak diinginkan atau menyebarkan virus berbahaya. Sayangnya, 24 infeksi malware terkait penggunaan perbankan online oleh masyarakat terdeteksi di Indonesia. (Dian Islami, 2021)

Yang terbaik adalah mengidentifikasi risiko kejahatan dunia maya secara rutin untuk mengidentifikasi pemicu kejahatan dunia maya. Prosesnya melibatkan evaluasi berbagai aspek yang dapat memicu kejahatan dunia maya. Pesatnya perkembangan teknologi penyadapan hingga peretasan media sosial telah menjadi ancaman besar di era perang siber. Menurut Abdul Wahid dan Mohammad Labib, ada dua jenis utama kejahatan dunia maya, yaitu kejahatan yang menggunakan teknologi informasi (TI) sebagai alatnya: ini mengacu pada kejahatan di mana pelakunya menggunakan teknologi informasi sebagai alat atau instrumen untuk melakukan kejahatan bekerja. Contohnya termasuk serangan dunia maya, penipuan online, pencurian identitas, distribusi malware, atau aktivitas ilegal lainnya yang menggunakan teknologi informasi sebagai sarana implementasinya. Dua kejahatan terhadap sistem dan fasilitas teknologi informasi (TI): Ini mengacu pada kejahatan yang secara langsung menargetkan sistem dan fasilitas TI itu sendiri. Contohnya termasuk serangan dunia maya terhadap infrastruktur TI, pencurian

data, sabotase jaringan komputer, atau eksploitasi kelemahan sistem keamanan informasi. (Eko Budi et al., 2021)

Indonesia memiliki sejumlah kejahatan cyber sehingga keamanan dan stabilitas ketertiban negara sangat terancam. Eskalasi kejahatan dunia maya telah mencapai tingkat yang cukup tinggi. Menangani aktivitas ilegal di dunia maya tidaklah mudah dengan hukum positif tradisional. Hal ini disebabkan adanya hubungan yang kompleks antara lima faktor yang saling terkait yaitu pelaku, korban, penanggulangan kejahatan dan hukum. Meskipun undang-undang berperan penting dalam pencegahan dan pemberantasan kejahatan, namun undang-undang menciptakan ketentuan hukum yang memenuhi persyaratan yang berbeda-beda. Bidang hukum berubah dengan cepat, begitu pula teknologi. Pengetahuan bukanlah tugas yang mudah Menanggapi tantangan kejahatan dunia maya memerlukan kerja sama antar berbagai sektor, termasuk pemerintah, penegak hukum, sektor swasta, dan masyarakat. Selain itu, pengembangan kerangka hukum yang adaptif dan penggunaan teknologi keamanan siber yang canggih sangat penting untuk memerangi kejahatan siber yang terus meningkat. (Eko Budi et al., 2021)

Menurut Rahmawati, dalam menghadapi ancaman kejahatan cyber dalam proses manajemen risiko dapat dilakukan beberapa langkah yang dijelaskan sebagai berikut:

- Identifikasi

Identifikasi risiko kejahatan dunia maya secara rutin untuk mengidentifikasi akar penyebab kejahatan dunia maya. Selama proses ini, semua aspek yang dapat menyebabkan kerusakan harus diidentifikasi secara cermat. Setelah teridentifikasi, semua risiko yang teridentifikasi diukur. Ada dua metrik utama yang digunakan untuk mengukur ancaman kejahatan dunia maya, yaitu probabilitas dan dampak.

- Penilaian

Tujuan dari analisis risiko, atau Assess, pada dasarnya adalah untuk menilai tingkat risiko kejahatan dunia maya dan dampaknya terhadap berbagai bidang kehidupan, termasuk pertahanan negara. Penilaian risiko kejahatan dunia maya tidak dapat dilakukan secara langsung, namun tabel matriks dapat digunakan untuk mengukur risiko. Dalam penilaian risiko kejahatan dunia maya, tabel matriks menggambarkan probabilitas dan dampak dari ancaman kejahatan dunia maya yang teridentifikasi.

- Treat

Memutuskan tindakan dan tindakan penanggulangan terkait risiko kejahatan dunia maya melibatkan keputusan apakah akan menerima, mentransfer, meminimalkan atau menghindarinya. Dalam kasus di mana pencurian informasi dan data terjadi antara individu dan institusi, meminimalkan risiko adalah hal yang penting.

- Kontrol

Untuk menilai keberhasilan manajemen risiko, penting untuk terus memantau dan beradaptasi. Proses pengendalian merekomendasikan penerapan mekanisme peringatan dini bagi pihak yang bertanggung jawab di bidang keamanan, seperti Kementerian Pertahanan Republik Indonesia, sehingga mereka dapat mengambil langkah-langkah yang diperlukan untuk mencegah ancaman kejahatan dunia maya. (Yusep Ginanjar, 2022)

Untuk mencegah kejahatan cyber, penting untuk melibatkan pakar teknologi yang memiliki kemampuan mendukung pengembangan sistem pertahanan negara yang maju dan modern. Kerja sama dengan industri pertahanan Indonesia diperlukan untuk

menciptakan sistem informasi dan program komunikasi yang mampu bersaing dengan negara lain. Ada dua faktor yang mempengaruhi berkembangnya sistem pertahanan siber di Indonesia, yaitu regulasi dan keberadaan pusat komando cyber. Untuk mengatur perkembangan keamanan cyber nasional, pemerintah harus membuat peraturan yang tepat dan sesuai. (Handrini Ardiyanti, 2014)

Topik penting lainnya adalah pembangunan pusat komando keamanan pertahanan cyber. Pemerintah Indonesia berencana menerapkan Komando Operasi cyber yang bertujuan untuk menjadi pusat komando pertahanan cyber Indonesia. Dengan beroperasinya pusat komando ini diharapkan negara Indonesia lebih siap dalam mencegah ancaman non-tradisional yaitu cybercrime yang semakin meningkat terhadap kedaulatan NKRI. Ini merupakan langkah besar yang perlu diperkuat agar kinerjanya optimal. Regulasi dan kemampuan yang memadai diperlukan untuk sistem, jaringan, aplikasi, dan kebijakan pertahanan nasional terkait keamanan cyber. (Yusep Ginanjar, 2022)

5. KESIMPULAN

Mencuri informasi dan data rahasia sebagai ancaman kejahatan dunia maya menargetkan individu, lembaga pemerintah, dan militer yang dapat mengancam pertahanan negara. Oleh karena itu, manajemen risiko informasi dan komunikasi menjadi penting untuk mengurangi kerentanan terhadap penyalahgunaan informasi di dunia maya, yang dapat berdampak pada banyak warga negara dan informasi rahasia. Selain pertahanan negara yang kuat, menghadapi ancaman kejahatan siber juga memerlukan bantuan hukum yang saling berhubungan dan saling mempengaruhi.

6. REFERENCES

Bram Ronald Sanjaya, Dian Efrianti, Mohammad Ali, Taufiq Prasetyo, M Mukhtadi, Yuniar Kurnia Widasari, & Zahrotul Khumairoh. (2022). PENGEMBANGAN CYBER SECURITY DALAM MENGHADAPI CYBER WARFARE DI INDONESIA. Journal of Advanced Research in Defense and Security Studies, Vol. 1, No. 1, 19–34.

Dian Islami. (2021). ANALISIS KONTEKSTUAL PADA STRATEGI KEAMANAN SIBER MESIR 2017-2021 DALAM UPAYA PENGAMANAN SIBER NASIONAL. MUKADIMAH: Jurnal Pendidikan, Sejarah, Dan Ilmu-Ilmu Sosial., Volume 5(Issue 1), 159–170.

Edy Soesanto, Septiana Cahyaningrum Tarmono Putri, Annisa Azahra Aulia, FarrelYafi Wicaksana, & Rahma Fithriami Thalitha. (2023). SISTEM PENGAMANAN FILE DAN CYBER SECURITY PADA PENGAMANANOBJEK VITAL PT PDAM (Perusahaan Daerah Air Minum). Vol. 6 No. 2, 766–774.

Eko Budi, Dwi Wira, & Ardian Infantono. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0 (Strategies For Strengthening Cyber Security To Achieve National Security in Society 5.0). Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia - Akademi Angkatan Udara, Volume 3, 223–234.

Handrini Ardiyanti. (2014). CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA. Politica, Vol. 5 No. 1, 95–110.

Putri Bilqis Oktaviani, & Anggraeni Silvia. (2021). Strategi Keamanan Siber Malaysia. Jurnal Kajian Ilmiah, Vol. 21 No. 1, 69–84.

Yusep Ginanjar. (2022). STRATEGI INDONESIA MEMBENTUK CYBER SECURITY DALAM MENGHADAPI ANCAMAN CYBER CRIME MELALUI BADAN SIBER DAN SANDI NEGARA. Jurnal Dinamika Global, Vol.7 No. 2, 295–316.