PROSIDING
SEMINAR NASIONAL ILMU SOSIAL & TEKNOLOGI
(SNISTEK) 6 TAHUN 2024
e-ISSN: 3025-9770

Analisis Komparasi *Cybercrime Web Defacement* dan *Darknet Exposure* di Indonesia (Studi Kasus : Lanskap Keamanan Siber di Indonesia Tahun 2022 dan Tahun 2023)

Muthiah As Saidah[a,*], Aggry Saputra[b], Hendi Setiawan[c]

[a] Sekolah Tinggi Teknologi Indonesia Tanjung Pinang, Kota Tanjungpinang

*muthiahassaidah40@gmail.com, aggrysaputra@gmail.com

Abstract
This study aims to analyze the comparison of cyber incidents involving Web Defacement and Darknet Exposure in Indonesia for the years 2022 and 2023, and to evaluate the effectiveness of the mitigation recommendations provided. The method used in this study is the Wilcoxon statistical test to determine significant differences between the incident rates in those two years. The Wilcoxon test results indicate that the Asymp. Sig. (2-tailed) value is 0.008, which, in the case of a one-tailed test, results in a probability of 0.004. This value indicates a significant difference between the Darknet Exposure incident rates in 2022 and 2023. The analysis also suggests that the mitigation recommendations implemented in 2022 were not effective in reducing Darknet Exposure incidents in 2023, as evidenced by an increase in the number of cases. Conversely, for Web Defacement incidents, the Wilcoxon test results show the same Asymp. Sig. (2-tailed) value of 0.008, resulting in a probability of 0.004. This indicates a significant difference between the Web Defacement incident rates in 2022 and 2023. Based on the test results, the mitigation recommendations proved effective in reducing Web Defacement incidents, with a decrease in the number of cases in 2023. From these findings, it can be concluded that cyber incident handling strategies need to be adjusted and strengthened, especially in dealing with Darknet Exposure incidents. Continuous monitoring and evaluation are also crucial for improving the effectiveness of cyber incident management in Indonesia.
Keywords : *Cyber Incidents; Cybercrime; Web Defacement ; Darknet Exposure ; Wilcoxon Statistical Test.*

Abstrak
Penelitian ini bertujuan untuk menganalisis komparasi insiden siber *Web Defacement* dan *Darknet Exposure* di Indonesia pada tahun 2022 dan 2023, serta mengevaluasi efektivitas saran-saran penanganan yang diberikan. Metode yang digunakan dalam penelitian ini adalah uji statistik *Wilcoxon* untuk menentukan perbedaan signifikan antara tingkat insiden pada kedua tahun tersebut. Hasil uji *Wilcoxon* menunjukkan bahwa nilai *Asymp. Sig. (2-tailed)* adalah 0,008, yang dalam kasus uji satu sisi menghasilkan probabilitas sebesar 0,004. Nilai ini menunjukkan bahwa terdapat perbedaan signifikan antara tingkat insiden siber *Darknet Exposure* pada tahun 2022 dan 2023, hasil analisis juga mengindikasikan bahwa saran-saran penanganan yang diterapkan pada tahun 2022 tidak efektif dalam menurunkan insiden *Darknet Exposure* pada tahun 2023, terlihat dari peningkatan jumlah kasus. Sebaliknya, pada kasus *Web Defacement* , hasil uji *Wilcoxon* menunjukkan nilai *Asymp. Sig. (2-tailed)* yang sama, menghasilkan probabilitas 0,004. Ini menunjukkan perbedaan signifikan antara tingkat insiden *Web Defacement* pada tahun 2022 dan 2023, Berdasarkan hasil pengujian diperoleh bahwa saran-saran penanganan terbukti efektif dalam menurunkan insiden *Web Defacement* , dengan penurunan jumlah kasus pada tahun 2023. Dari hasil penelitian ini, dapat disimpulkan bahwa strategi penanganan insiden siber perlu disesuaikan dan diperkuat, terutama dalam menangani insiden siber *Darknet Exposure* . Monitoring dan evaluasi terus-menerus juga sangat penting untuk meningkatkan efektivitas penanganan insiden siber di Indonesia.
Kata Kunci : Insiden siber; Kejahatan Siber; *Web Defacement ; Darknet Exposure ; Uji Statistik Wilcoxon*.

1. Pendahuluan

Keamanan siber telah menjadi bagian utama dari program keamanan nasional. Hal ini disebabkan oleh semakin besarnya ketergantungan terhadap teknologi informasi dan komunikasi di berbagai sektor, seperti pemerintahan, bisnis, dan ranah pribadi. Ancaman siber yang sangat kompleks memerlukan langkah-langkah keamanan siber yang lebih kuat dan efektif untuk melindungi

data serta sistem dari berbagai serangan yang semakin kuat (Abrahams et al., 2024). Indonesia menempati peringkat kedua tertinggi di dunia dalam hal c*ybercrime* (Haryanto & Sutra, 2023). Badan Siber dan Sandi Negara (BSSN) telah merilis lanskap keaman siber semenjak tahun 2018 hingga tahun 2023 (BSSN, 2023). Berdasarkan lanskap kemanan siber tahun 2022 dan tahun 2023 terdapat laporan tentang *cybercrime* termasuk insiden siber *Web Defacement* dan *Darknet Exposure* .

Serangan *Web Defacement* adalah jenis serangan yang dilakukan dengan mengeksploitasi situs web atau server web yang rentan, memanfaatkan kelemahan sistem sehingga penyerang dapat merusak, memodifikasi, atau menghapus konten halaman web yang telah mereka akses secara ilegal (Kurzmeier, 2023). Sedangkan *Darknet Exposure* adalah kondisi ketika informasi kredensial akun dari suatu instansi atau organisasi tertentu terekspos di *darknet*, baik melalui forum jual beli data, forum diskusi peretas, maupun pesan instan, sehingga berpotensi disalahgunakan oleh pihak yang tidak berwenang (BSSN, 2023).

Tabel 1. Data *Web Defacement* dan *Darknet Exposure*

No.	Insiden Siber	Tahun 2022	Tahun 2023
1	*Web Defacement*	2.348	189
2	*Darknet Exposure*	27.956	1.674.185

Berdasarkan data- data yang telah diperoleh diatas diperlukan analisis komparasi. Analisis komparasi adalah teknik analisis statistik yang bertujuan untuk melihat perbedaan dua kelompok data (Wulansari, 2023). Dalam penelitian ini, peneliti melakukan analisis komparatif untuk membandingkan insiden siber *Web Defacement* dan *Darknet Exposure* di Indonesia pada tahun 2022 dan 2023, serta mengevaluasi efektivitas penanganan insiden-insiden selama periode tersebut. Dengan pendekatan ini, diharapkan dapat diperoleh pemahaman yang lebih mendalam mengenai langkah-langkah efektif dalam meningkatkan keamanan siber di masa mendatang. Pada penelitian ini terdapat hipotesis- hipotesis yang akan dibuktikan. Hipotesis- hipotesis tersebut adalah sebagai berikut :

Tabel 1. Hipotesis Penelitian

		Hipotesis
H_{01}	:	Tidak ada perbedaan tingkat insiden siber *Darknet Exposure* pada tahun 2022 dengan insiden siber Darknet Exposure pada tahun 2023 setelah diberikan saran- saran penanganan.
H_1	:	Ada perbedaan tingkat insiden siber *Darknet Exposure* pada tahun 2022 dengan insiden siber Darknet Exposure pada tahun 2023 setelah diberikan saran- saran penanganan.
H_{02}	:	Tidak ada perbedaan tingkat insiden siber *Web Defacement* pada tahun 2022 dengan insiden siber *Web Defacement* pada tahun 2023 setelah diberikan saran- saran penanganan.
H_2	:	Ada perbedaan tingkat insiden siber *Web Defacement* pada tahun 2022 dengan insiden siber dar *Web Defacement* pada tahun 2023 setelah diberikan saran- saran penanganan.

2. Kajian Literatur

2.1 Keamanan Siber

Keamanan siber adalah upaya yang dilakukan oleh organisasi untuk melindungi sistem teknologi informasi dari berbagai ancaman dan serangan ilegal, termasuk akses tidak sah. Keamanan siber mencakup alat, kebijakan, dan konsep keamanan yang digunakan untuk melindungi seluruh aset organisasi dan penggunanya. Dengan menerapkan keamanan siber yang tepat, organisasi dapat meminimalkan risiko ancaman terhadap sistem teknologi informasi yang dapat merugikan organisasi dan pihak terkait, termasuk subjek data pribadi (Vania et al., 2023). Keamanan siber juga mencakup perlindungan terhadap pengawasan yang tidak diinginkan dan bertujuan meminimalisir gangguan pada ketersediaan, integritas, dan kerahasiaan informasi (M. P. Aji, 2023).

2.2 Cybercrime

Cybercrime adalah bentuk kejahatan modern yang menarik perhatian luas di tingkat nasional, regional, dan internasional. Kejahatan ini muncul karena adanya komunitas dunia maya di internet dan memiliki karakteristik yang unik (Januri et al., 2022). Persoalan tentang *Cybercrime* telah diatur dalam Undang-Undang Nomor 19 Tahun 2016, yang merupakan perubahan dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-undang ini menegaskan bahwa *cybercrime* adalah tindak pidana yang dilarang dan pelakunya akan ditindak sesuai hukum.

2.3 Web Defacement

Web Defacement merupakan salah satu kejahatan yang umum dalam dunia *cybercrime*. *Web Defacement* adalah tindakan peretas yang merusak atau mengubah tampilan halaman depan sebuah situs web. Tindakan ini sering dilakukan untuk merusak reputasi organisasi atau individu, mengeksploitasi kerentanan keamanan, atau menyampaikan pesan politik atau ideologis. Kejahatan ini memiliki konsekuensi serius bagi pemilik situs web dan pengguna yang mengandalkan informasi atau layanan dari situs tersebut (B. B. Aji, 2023).

2.4 Darknet Exposure

Darknet adalah jenis ruang siber yang menyediakan privasi dan kebebasan bagi pengguna. Hali ini menyebabkan beberapa orang terlibat dalam aktivitas sosial dan politik yang konstruktif, sementara yang lain menggunakannya untuk memenuhi keinginan kriminal. Secara umum, masyarakat dan media memandang *darknet* sebagai tempat bagi para penjahat. Persepsi negatif ini juga didukung

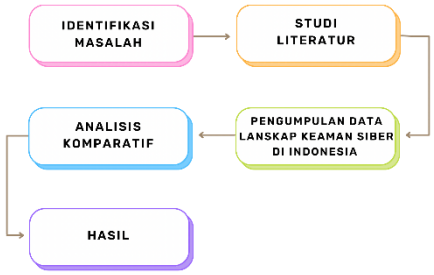
oleh penelitian akademis yang menemukan bahwa *darknet* adalah sarang berbagai transaksi ilegal. Transaksi narkoba melalui mata uang kripto adalah yang paling dominan, mencakup sebagian besar transaksi di pasar. Selain narkoba, pengguna juga dapat membeli produk atau layanan ilegal seperti senjata, pornografi, barang palsu, hewan eksotis, informasi kartu kredit dan pribadi, serta perangkat lunak peretasan, yang biasanya tidak dapat dijual dan dibeli secara offline atau di internet biasa (Lee, 2019).

3. Metode Penelitian

Penelitian ini merupakan penelitian kausal komparatif dengan pendekatan studi kasus. Penelitian kausal komparatif adalah jenis penelitian yang bersifat *expost- facto*, artinya data penelitian dikumpulkna setelah semua fenomena atau kejadian yang diteliti berlangsung, atau tentang hal- hal yang telah terjadi sehingga tidak ada yang dikontrol. Dengan demikian pada penelitian kausal komparatif tidak terjadi intervensi langsung pada data yang diteliti. Pengaruh atau efek variabel bebas dapat diketahui dengan membandingkan kedua kelompok data (Yusuf, 2014).

Penelitian ini bertujuan untuk membandingkan dua fenomena berbeda, yaitu kejahatan siber berupa *Web Defacement* dan *Darknet Exposure* , dalam konteks keamanan siber di Indonesia. Penelitian ini dilakukan dengan membandingkan data dan temuan dari periode waktu berbeda yaitu data tahun 2022 dan 2023 untuk mengidentifikasi perbedaan dan persamaan dalam lanskap keamana siber terkait kedua jenis kejahatan siber tersebut. Pada penelitian ini akan dilakukan pengujian data yang telah diperoleh dari lanskap keaman siber di Indonesia yang dikeluarkan oleh Badan Siber dan Sandi Negara, dengan pengujian statistik nonparametrik yaitu uji *Wilcoxon. Uji Wilcoxon* adalah pengujian dua kelompok data yang saling berhubungan dan bertujuan menguji, apakah kedua kelompok data mempunyai hubungan (Santoso, 2022).

Alur penelitian adalah serangkaian langkah yang disusun secara sistematis untuk mencapai tujuan penelitian yang telah ditentukan (As Saidah et al., 2024). Berikut ini adalah alur penelitian yang akan dilaksanakan pada penelitian ini:



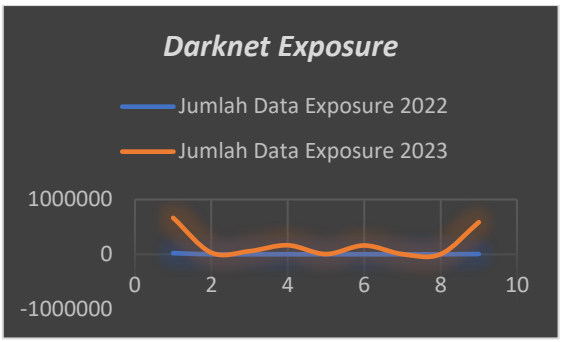
Gambar 1. Alur Penelitian

4. Hasil dan Pembahasan

Berdasarkan langkah-langkah analsis komparasi, langkah pertama yang harus dilakukan adalah menentukan dua kelompok data yang akan dianalisis. Data insiden siber *Darknet Exposure* yang diperoleh dari lanskap keamanan siber BSSN adalah sebagai berikut :

Tabel 2. Jumlah Insiden Siber *Darknet Exposure*

No.	Sektor	Tahun 2022	Tahun 2023
1	Administrasi Pemerintahan	21.302	665.916
2	ESDM	143	29.350
3	Transportasi	406	56.925
4	Keuangan	503	165.085
5	Kesehatan	17	3.785
6	TIK	375	161.282
7	Pangan	28	3.287
8	Pertahanan	14	1.958
9	Lainnya	5.168	586.597



Gambar 1. *Darknet Exposure* Tahun 2022 dan 2023

Pada lanskap kemanan siber Indonesia tahun 2022 terdapat saran-saran penanganan yang harus dilakukan untuk mengurangi insiden siber *Darknet Exposure* yaitu manajemen akun pengguna, *Restrict File and Directory Permissions*, kebijakan password terkait kombinasi karakter, tidak menggunakan akun/kredensial dinas untuk kepentingan selain kedinasan, dan segmentasi jaringan, serta melakukan himbauan pergantian password kepada setiap pegawai di masing- masing instansi (BSSN, 2022). Selanjutnya dilakukan uji *Wilcoxon* menggunakan bantuan SPPS dengan data diatas, untuk melihat apakah dengan saran penanganan yang telah diberikan oleh BSSN pada tahun 2022 mempengaruhi tingkat insiden siber *Darknet Exposure* pada tahun 2023, dari pengujian tersebut diperoleh :

Tabel 3. *Wilcoxon Signed Ranks Test*

	N	*Mean Rank*	*Sum of Ranks*
Negative Ranks	0[a]	.00	.00
Positive Ranks	9[b]	5.00	45.00
Ties	0[c]		
Total	9		

Tabel 4. Tes *Statistics*[a]

	Jumlah_Exposure_Data2023 - Jumlah_Exposure_Data2022
Z	-2.666[b]
Asymp. Sig. (2-tailed)	.008

a. Wilcoxon Signed Ranks Test
b. Based on negative ranks.

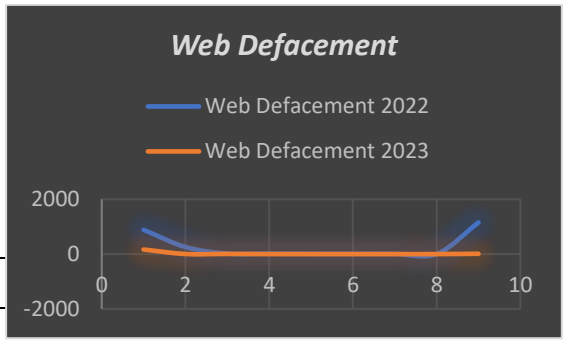
Dasar pengambilan keputusan berdasarkan probabilitas (Santoso, 2022) : (1) Jika probabilitas > 0,05 maka H_0 diterima; (2) Jika probabilitas < 0,05 maka H_0 ditolak.

Berdasarkan hasil uji wilcoxon diatas terlihat bahwa diperoleh hasil tes statistik *Asymp. Sig. (2-tailed)* dari data adalah 0,008. Karena kasus pada penelitian ini adalah uji satu sisi, maka probabilitas menjadi 0,004. Sehingga dari nilai probabilitas tersebut dapat disimpulkan bahwa (0,004 < 0,05). Maka H_{01} ditolak atau H_1 dterima, artinya ada perbedaan tingkat insiden siber *Darknet Exposure* pada tahun 2022 dengan insiden siber *Darknet Exposure* pada tahun 2023 setelah diberikan saran- saran penanganan. Berdasarkan hasil pengujian diatas dapat disimpulkan bahwa saran- saran penanganan insiden siber *Darknet Exposure* pada tahun 2022 tidak memiliki efek yang berarti pada penurunan insiden siber *Darknet Exposure* pada tahun 2023. Hal ini didukung oleh hasil *Wilcoxon Signed Ranks Test* pada tabel 3, bahwa terjadi peningkatan kasus insiden siber *Darknet Exposure* pada tahun 2023.

Selanjutnya, data insiden siber *Web Defacement* yang diperoleh dari lanskap keamanan siber BSSN adalah sebagai berikut :

Tabel 5. Jumlah Insiden Siber *Web Defacement*

No.	Sektor	Tahun 2022	Tahun 2023
1	Adm. Pemerintahan	885	167
2	Pertahanan	258	3
3	Kesehatan	16	7
4	TIK	14	0
5	Pangan	7	0
6	Keuangan	6	0
7	ESDM	6	0
8	Transportasi	3	0
9	Lainnya	1153	12



Gambar 2. *Web Defacement* Tahun 2022 dan 2023

Pada lanskap keamanan siber Indonesia tahun 2023 terdapat saran- saran penanganan yang harus dilakukan untuk mengurangi insiden siber *Web Defacement* adalah sebagai berikut (BSSN, 2022) : (1) Password kepada setiap pengguna serta tidak menggunakan default username dan password; (2) Melakukan pembaruan sistem secara berkala; (3) Melakukan pemeriksaan terhadap konfigurasi yang telah diterapkan. Selain itu, melakukan audit atau penetration testing juga dapat

e-ISSN: 3025-9770

membantu pemilik sistem elektronik untuk mengidentifikasi kerentanan termasuk kesalahan konfigurasi; (4) Aplikasi seharusnya dibangun dengan memperhatikan keamanannya, misalnya melakukan sanitasi input pengguna. Selain itu, sebagai pengamanan tambahan seharusnya server menerapkan *Web Application Firewall* (WAF).

Selanjutnya, dilakukan pengujian dengan menggunakan uji *Wilcoxon* untuk apakah dengan saran penanganan yang telah diberikan oleh BSSN pada tahun 2022 mempengaruhi tingkat insiden siber *Web Defacement* pada tahun 2023, dari pengujian tersebut diperoleh :

Tabel 6. *Wilcoxon Signed Ranks Test*

	N	*Mean Rank*	*Sum of Ranks*
Negative Ranks	9[a]	5.00	45.00
Positive Ranks	0[b]	.00	.00
Ties	0[c]		
Total	9		

Tabel 7. Tes *Statistics*[a]

	Web_Defacement_2023 - Web_Defacement_2022
Z	-2.668[b]
Asymp. Sig. (2-tailed)	.008

a. Wilcoxon Signed Ranks Test
b. Based on negative ranks.

Berdasarkan hasil uji wilcoxon diatas terlihat bahwa diperoleh hasil tes statistik *Asymp. Sig. (2-tailed)* dari data adalah 0,008. Karena kasus pada penelitian ini adalah uji satu sisi, maka probabilitas menjadi 0,004. Sehingga dari nilai probabilitas tersebut dapat disimpulkan bahwa (0,004 < 0,05). Maka H_{02} ditolak atau H_2 dterima, artinya ada perbedaan tingkat insiden siber *Web Defacement* pada tahun 2022 dengan insiden siber *Web Defacement* pada tahun 2023 setelah diberikan saran- saran penanganan. Berdasarkan hasil pengujian diatas juga dapat disimpulkan bahwa saran-saran penanganan insiden siber *Web Defacement* pada tahun 2022 memiliki efek yang berarti pada penurunan insiden siber *Web Defacement* pada tahun 2023. Hal ini didukung oleh hasil *Wilcoxon Signed Ranks Test* pada tabel 6, bahwa terjadi penurunan kasus insiden siber *Web Defacement* pada tahun 2023.

5. Kesimpulan dan Saran

Penelitian ini bertujuan untuk mengevaluasi efek dari saran-saran penanganan terhadap insiden siber *Darknet Exposure* dan *Web Defacement* antara tahun 2022 dan 2023.

Berdasarkan hasil uji *Wilcoxon*, terdapat perbedaan signifikan antara tingkat insiden siber *Darknet Exposure* pada tahun 2022 dan 2023 setelah diberikan saran-saran penanganan dan terlihat bahwa saran-saran penanganan tidak memiliki efek yang berarti dalam menurunkan insiden siber *Darknet Exposure* pada tahun 2023. Bahkan terjadi peningkatan kasus pada tahun tersebut.

Selanjutnya, hasil uji *Wilcoxon* untuk insiden siber *Web Defacement* terdapat perbedaan signifikan antara tingkat insiden siber *Web Defacement* pada tahun 2022 dan 2023 setelah diberikan saran-saran penanganan. Berdasarkan hasil pengujian, saran-saran penanganan memiliki efek yang signifikan dalam menurunkan insiden siber *Web Defacement* pada tahun 2023. Terlihat adanya penurunan kasus pada tahun tersebut.

Saran penguatan penanganan untuk insiden iber *Darknet Exposure* perlu dilakukan evaluasi dan peningkatan strategi penanganan. Metode yang telah diterapkan pada tahun 2022 terbukti tidak efektif sehingga diperlukan pendekatan baru yang lebih komprehensif. Serta perlu meningkatkan pelatihan dan kesadaran akan bahaya *Darknet Exposure* , serta implementasi teknologi yang lebih canggih untuk mendeteksi dan mencegah insiden tersebut.

Saran perbaikan berkelanjutan untuk insiden siber *Web Defacement* , karena strategi penanganan yang diterapkan telah berhasil menurunkan insiden siber *Web Defacement* . Oleh karena itu, metode tersebut harus terus diperbaiki dan diadaptasi sesuai dengan perkembangan teknologi dan metode serangan yang baru. Serta melakukan monitoring dan evaluasi secara berkala terhadap insiden siber dan efektivitas penanganannya. Ini akan membantu dalam mengidentifikasi kelemahan dan peluang perbaikan.

Dengan langkah-langkah ini, diharapkan mampu memberikan penanganan yang lebih efektif terhadap insiden siber di masa depan, khususnya dalam mengatasi *Darknet Exposure* dan *Web Defacement* .

Ucapan Terima Kasih

Terima kasih yang sebesar-besarnya saya sampaikan kepada semua pihak yang telah memberikan dukungan dan kontribusinya dalam penelitian ini : (1) Sekolah Tinggi

Teknologi Indonesia Tanjung Pinang, atas fasilitas dan dukungan akademik yang diberikan selama proses penelitian ini; (2) Rekan Peneliti atas kerja sama dan partisipasi dalam pengumpulan data serta diskusi yang konstruktif; (3) Pihak-pihak Lain yang tidak dapat saya sebutkan satu per satu, yang telah membantu secara langsung maupun tidak langsung dalam menyelesaikan penelitian ini.

Saya sangat menghargai segala bentuk bantuan, dukungan, dan doa yang diberikan. Semoga penelitian ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya dalam bidang keamanan siber di Indonesia. Terima kasih.

Daftar Pustaka

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Azeez Olanipekun Hassan. (2024). a Review of Cybersecurity Strategies in Modern Organizations: Examining the Evolution and Effectiveness of Cybersecurity Measures for Data Protection. *Computer Science & IT Research Journal*, *5*(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699

Aji, B. B. (2023). Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website. *Cyber Security Dan Forensik Digital*, *6*(1), 25–29. https://doi.org/10.14421/csecurity.2023.6.1.4049

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

As Saidah, M., Shobri, M. Q., & Nasra, N. D. (2024). Implementasi Analytic Hierarchy Process (AHP) Dalam Pengambilan Keputusan Desain Kualitas Software. *Jurnal Bangkit Indonesia*, *13*(1), 7–12. https://doi.org/10.52771/bangkitindonesia.v13i1.268

BSSN. (2022). Lanskap Keamanan Siber Indonesia 2022. *Badan Siber Dan Sandi Negara*, 1–97.

BSSN. (2023). *Lanskap Kemanan Siber Indonesia | www.bssn.go.id*. https://www.bssn.go.id/monitoring-keamanan-siber/

Haryanto, A., & Sutra, S. M. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Global Political Studies Journal*, *7*(1), 56–69. https://doi.org/10.34010/gpsjournal.v7i1.8141

Januri, Melati, D. P., & Muhadi. (2022). *Upaya Kepolisian Dalam Penanggulangan Kejahatan Cyber Terorganisircyber Terorganisir*. *01*(1), 94–100.

Kurzmeier, M. (2023). *Using a national web archive for the study of Web Defacement s ? A case-study approach*.

Lee, J. (2019). Child pornography websites on the darknet. *International Journal of Recent Technology and Engineering*, *8*(2 Special Issue 6), 48–54. https://doi.org/10.35940/ijrte.B1010.0782S619

Santoso, S. (2022). *Panduan Lengkap SPSS*. PT Elex Media Komputindo.

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber. *Jurnal Multidisiplin Indonesia*, *2*(3), 654–666. https://doi.org/10.58344/jmi.v2i3.157

Wulansari, A. D. (2023). *Aplikasi Statistika NonParametrik Dalam Penelitian*. 268 halaman.

Yusuf, M. (2014). *Metode Penelitian Kuantitatif, Kualitatif & Gabungan* (Pertama). Prenadamedia Group.