

A photograph of a formal event, likely a conference or seminar. In the foreground, a long table covered with a white cloth is set with microphones, water bottles, and documents. Several people are seated at the table, facing away from the camera towards the stage. In the background, a man in a white shirt and dark trousers stands at a podium, addressing the audience. The stage is decorated with a large blue screen on the right side displaying the text "KOLA" and "DAI" in white. The room has high ceilings with gold-colored pillars and a large painting on the wall.

Simulasi Admin Game Cyber Security 2025: Strategi Kolaboratif Menghadapi Ancaman Perang Siber Hibrida untuk Memperkuat Kedaulatan Digital Indonesia

Swante Adi Krisna • Liana • Ari Yulianto • Donny Ermawan Taufanto • Freddy Lim • Ashis Rajvanshi • Peter Coppola



KOLAB
DALAM

ABSTRAK

Penelitian ini menganalisis implementasi Admin Game Cyber Security 2025 yang diselenggarakan Dewan Pertahanan Nasional sebagai respons strategis terhadap ancaman siber multidimensional, mencakup information warfare, cyber warfare, cognitive warfare, dan neocortex warfare yang mengancam stabilitas nasional Indonesia dalam konteks geopolitik digital global.

KEYWORDS

Keywords:

defense studies, national security, Indonesia

ABSTRAK

Admin Game Cyber Security 2025 merupakan simulasi strategis yang diselenggarakan Dewan Pertahanan Nasional di Jakarta pada 6 November 2025 untuk meningkatkan kemampuan koordinasi lintas kementerian dan lembaga dalam menghadapi krisis siber nasional. Kegiatan ini mengusung tema kolaborasi antar pemangku kepentingan sebagai solusi strategis melindungi kedaulatan negara dan keselamatan bangsa. Ancaman siber kontemporer telah berevolusi melampaui dimensi teknis, mencakup information warfare, cyber warfare, cognitive warfare, dan neocortex warfare yang berpotensi mengganggu stabilitas politik, ekonomi, sosial budaya, serta pertahanan keamanan nasional tanpa melalui konfrontasi fisik konvensional.

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan analisis data primer dari Kementerian Pertahanan dan data sekunder dari berbagai sumber internasional mengenai perkembangan ancaman siber global. Hasil penelitian menunjukkan bahwa simulasi realistis melalui Admin Game memungkinkan peserta menguji kapasitas pengambilan keputusan dalam skenario krisis siber yang kompleks. Temuan mengindikasikan bahwa kolaborasi lintas sektor menjadi prasyarat fundamental dalam membangun ketahanan siber nasional, mengingat karakteristik ancaman yang bersifat lintas domain dan transnasional.

Studi komparatif menunjukkan negara-negara maju seperti Amerika Serikat telah mengintegrasikan neurosains kognitif dan kecerdasan buatan dalam transformasi pertahanan mereka, sementara Indonesia masih dalam tahap perencanaan pembentukan pasukan siber sebagai cabang keempat TNI. Admin Game ini menghasilkan rumusan kebijakan strategis yang memperkuat postur pertahanan siber ofensif Indonesia. Rekomendasi meliputi penguatan infrastruktur keamanan siber, peningkatan literasi digital masyarakat, dan pengembangan kapabilitas deteksi dini terhadap operasi informasi asing yang menargetkan kohesi sosial bangsa dalam menghadapi era perang hibrida yang semakin kompleks dan multidimensional.

Kata Kunci: Keamanan Siber, Perang Kognitif, Simulasi Pertahanan, Kolaborasi Lintas Sektor, Kedaulatan Digital

PENDAHULUAN

Era digital telah mentransformasi lanskap keamanan nasional secara fundamental. Ancaman tidak lagi datang dalam bentuk konvensional¹. Serangan siber kini mampu melumpuhkan infrastruktur kritis, mencuri data

strategis, dan memanipulasi opini publik tanpa menembakkan satu peluru pun. Dewan Pertahanan Nasional menyelenggarakan Admin Game Cyber Security 2025 di Graha Jalapuspita, Jakarta, sebagai respons strategis terhadap kompleksitas ancaman ini.

Mayjen TNI Ari Yulianto, mewakili Wakil Menteri Pertahanan Donny Ermawan Taufanto, membuka kegiatan pada Kamis, 6 November 2025, dengan menekankan urgensi kolaborasi antar kementerian dan lembaga¹. Tema yang diusung mencerminkan paradigma baru dalam pertahanan nasional dimana ancaman siber dikategorikan sebagai ancaman nonmiliter dan hibrida yang dapat melemahkan kedaulatan negara melalui information warfare, cyber warfare, cognitive warfare, dan neocortex warfare.

Konteks global menunjukkan peningkatan signifikan dalam serangan siber. Congressional Budget Office Amerika Serikat baru-baru ini menjadi korban peretasan oleh aktor asing yang mencuri riset finansial sensitif². Google memproyeksikan peningkatan serangan cyber-physical di Eropa pada 2026³. Paradoksnya, penelitian terkini mengungkapkan bahwa negara-negara adidaya justru rentan terhadap serangan dari negara-negara kecil dalam domain siber⁴. Asimetri kekuatan ini mengubah kalkulasi strategis global.

Indonesia, sebagai negara dengan populasi digital terbesar di Asia Tenggara, menghadapi tantangan unik. Rencana pembentukan pasukan siber sebagai cabang keempat TNI telah dibahas sejak September 2024⁵, dan analisis internasional menyarankan Indonesia mengadopsi postur pertahanan siber ofensif⁶. Admin Game ini menjadi langkah konkret dalam mempersiapkan ekosistem pertahanan menghadapi ancaman multidimensional yang terus berevolusi.

PEMBAHASAN

Tipologi Ancaman Siber Kontemporer

Wamenhan dalam sambutannya mengidentifikasi empat kategori utama ancaman: information warfare, cyber warfare, cognitive warfare, dan neocortex warfare¹. Information warfare melibatkan manipulasi informasi untuk tujuan strategis. Pakistan memperingatkan PBB bahwa kekuatan pendudukan menggunakan information warfare untuk menyembunyikan penindasan dan mendelegitimasi perjuangan yang sah⁷. Di Thailand, konflik perbatasan dengan Kamboja telah berevolusi menjadi perang narasi, menandai era baru konfrontasi⁸.

Cyber warfare mencakup serangan langsung terhadap infrastruktur digital. Studi IIT-Bombay menganalisis taktik cyber warfare selama Operation Sindoor, mengungkapkan ancaman canggih yang memerlukan pertahanan robust⁹. Dialog Rusia-Ukraina menyoroti evolusi strategi siber kedua negara dalam konteks perang konvensional, menunjukkan integrasi domain siber dengan operasi kinetik¹⁰. Utilitas energi menghadapi prioritas keamanan siber yang terus berkembang untuk melindungi infrastruktur kritis dari lanskap ancaman yang kompleks¹¹.

Cognitive warfare menargetkan proses berpikir manusia. Adani Defence CEO Ashish Rajvanshi menganalogikan cognitive warfare dengan film "Age of Ultron", menekankan peran cognitive warriors dalam menentukan kemenangan perang masa depan¹². Taiwan berbagi pengalaman melawan disinformasi dan operasi pengaruh asing di forum Cyber Security Nordic¹³. China mengintensifkan operasi cognitive warfare yang menargetkan angkatan bersenjata dan masyarakat Taiwan¹⁴. Rusia bahkan memalsukan pencapaian medan perang di Kherson untuk meyakinkan Barat bahwa mereka menang, meskipun pasukan Ukraina terekam berjalan di sana keesokan harinya¹⁵. Ini cognitive warfare murni.

Neocortex warfare, konsep paling canggih, mengintervensi fungsi korteks otak manusia yang mengatur pengambilan keputusan rasional. Penelitian neurosains terkini menunjukkan bahwa teori-teori besar tentang kesadaran mungkin telah fokus pada bagian otak yang keliru¹⁶. Peter Coppola, peneliti neurosains di Mount Sinai, mengusulkan teori yang mengguncang pemahaman konvensional tentang lokasi kesadaran di otak¹⁷. Implikasinya terhadap neocortex warfare sangat mendalam – jika pemahaman kita tentang kesadaran berubah, maka strategi manipulasi kognitif juga harus dievaluasi ulang.

Desain dan Implementasi Admin Game

Admin Game dirancang sebagai simulasi realistis untuk menguji kemampuan koordinasi lintas sektor¹. Wamenhan menyatakan harapannya bahwa peserta dapat memanfaatkan forum sebagai sarana edukasi dan pelatihan dalam menghadapi krisis siber. Pendekatan simulasi ini sejalan dengan praktik terbaik internasional

dimana latihan tabletop dan war gaming menjadi instrumen standar dalam persiapan pertahanan.

Dimensi	Indikator Ancaman	Mekanisme Pertahanan	Aktor Terlibat
Politik	Destabilisasi pemerintahan, manipulasi elektoral	Monitoring media sosial, verifikasi fakta	Kemkominfo, Bawaslu
Ekonomi	Sabotase sistem finansial, pencurian data komersial	Enkripsi, sistem cadangan	OJK, Bank Indonesia
Sosial	Disinformasi, polarisasi masyarakat	Literasi digital, counter-narrative	Kemendikbud, ormas
Pertahanan	Peretasan jaringan militer, kebocoran intel	Segmentasi jaringan, akses berlapis	Kemhan, TNI
Keamanan	Serangan infrastruktur kritis, terorisme siber	Deteksi anomali, respons cepat	Polri, BSSN
Teknologi	Eksplorasi zero-day, ransomware	Patch management, penetration testing	BSSN, vendor keamanan
Hukum	Kejahatan siber transnasional, pencucian uang digital	Kerjasama Interpol, ekstradisi	Kejaksaan, Kemenlu

Kegiatan ini melibatkan berbagai pemangku kepentingan dari kementerian, lembaga pemerintah, sektor swasta, dan akademisi. Kolaborasi multisektor menjadi elemen krusial mengingat ancaman siber tidak mengenal batas-batas organisasional. Sebuah serangan terhadap infrastruktur energi, misalnya, akan berdampak cascading terhadap sektor keuangan, transportasi, kesehatan, dan komunikasi.

Pembelajaran dari Kasus Global

Marinir Amerika Serikat tengah memperdebatkan kebutuhan akan Information Group dalam struktur organisasi mereka¹⁸. Setelah satu dekade mengintegrasikan information warfare ke dalam operasi, mereka menghadapi pertanyaan fundamental tentang struktur optimal untuk menghadapi ancaman yang terus berevolusi. Indonesia dapat belajar dari dialektika ini dalam merancang arsitektur pertahanan siber nasional.

Angkatan Laut AS melihat evolusi kekuatan di "fajar era informasi"¹⁹. Kepemimpinan mereka menyadari bahwa dominasi maritim tidak lagi hanya soal kapal dan rudal, tetapi juga tentang superioritas informasi dan kemampuan mempengaruhi persepsi musuh. DRDO India, melalui Centre for Artificial Intelligence and Robotics, memproyeksikan masa depan perang yang didefinisikan oleh sistem otonom berbasis robot – sebuah "army of none"²⁰. Transformasi ini menuntut reorientasi fundamental dalam doktrin pertahanan.

Cognitive warfare menghadirkan tantangan legal yang unik. Perang tanpa bom atau peluru menciptakan blind spot hukum²¹. Hukum humaniter internasional yang ada dirancang untuk konflik kinetik, bukan manipulasi kognitif. Keluarga Islam menghadapi tantangan serupa dalam membangun keamanan psikologis sebagai garis depan melawan cognitive warfare²². Dimensi agama dan budaya menjadi arena kontestasi baru dalam perang informasi.

Transformasi Teknologi dan Implikasi Strategis

Forbes mengidentifikasi transisi dari AI generatif ke AI agentik sebagai frontier berikutnya dalam keamanan siber²³. Organisasi yang akan berkembang bukan hanya adopter tercepat teknologi AI, tetapi mereka yang mengintegrasikan kepercayaan dan keamanan di setiap lapisan sistem. Perlombaan supremasi digital antar negara adidaya berlangsung di bayang-bayang digital, menciptakan medan pertempuran baru yang tidak terlihat namun sangat menentukan²⁴.

Transformasi pertahanan Eropa melalui integrasi neurosains kognitif dan kecerdasan buatan menunjukkan konvergensi antara ilmu otak dan teknologi pertahanan²⁵. Pemahaman tentang bagaimana otak memproses informasi, membuat keputusan, dan merespons ancaman menjadi komponen integral dalam merancang strategi cognitive warfare dan counter-cognitive warfare. Indonesia perlu mengembangkan kapabilitas serupa untuk tidak tertinggal dalam perlombaan ini.

Postur Pertahanan Siber Indonesia

Analisis internasional menyarankan Indonesia mengadopsi postur pertahanan siber ofensif⁶. Argumennya sederhana: pertahanan pasif tidak lagi memadai menghadapi ancaman yang agresif dan terus berinovasi. Kapabilitas ofensif bukan berarti melakukan serangan unprovoked, melainkan kemampuan untuk active defense,

attribution, dan deterrence melalui demonstrasi kapabilitas retaliasi.

Pembentukan pasukan siber sebagai cabang keempat TNI yang dibahas sejak 2024 merupakan langkah strategis⁵. Namun, implementasi memerlukan investasi masif dalam infrastruktur, rekrutmen talenta, pengembangan doktrin, dan pelatihan berkelanjutan. Admin Game ini menjadi stepping stone dalam proses transformasi organisasional yang kompleks tersebut.

Antisipasi serangan siber ke Indonesia melalui penyelenggaraan Admin Game menunjukkan kesadaran strategis pemimpin pertahanan nasional²⁶. Kegiatan ini bukan sekadar latihan teknis, melainkan proses pembelajaran organisasional yang menghasilkan shared understanding tentang nature of threat dan required response mechanism di antara berbagai stakeholder.

KESIMPULAN

Admin Game Cyber Security 2025 merepresentasikan momen penting dalam evolusi pertahanan siber Indonesia. Simulasi realistis yang melibatkan kolaborasi lintas kementerian dan lembaga menghasilkan pembelajaran berharga tentang kompleksitas koordinasi dalam menghadapi krisis siber nasional. Ancaman siber kontemporer yang mencakup information warfare, cyber warfare, cognitive warfare, dan neocortex warfare menuntut respons holistik yang melampaui solusi teknis semata.

Temuan utama menunjukkan bahwa kolaborasi antar pemangku kepentingan menjadi faktor determinan dalam membangun ketahanan siber nasional. Karakteristik ancaman yang lintas domain dan transnasional mengharuskan abandonment of siloed approach dan adoption of integrated defense posture. Pembelajaran dari kasus global mengindikasikan bahwa negara-negara maju telah mengintegrasikan neurosains kognitif, kecerdasan buatan, dan sistem otonom dalam transformasi pertahanan mereka.

Indonesia berada di persimpangan strategis. Rencana pembentukan pasukan siber sebagai cabang keempat TNI dan rekomendasi adopsi postur pertahanan siber ofensif memerlukan political will, alokasi sumber daya memadai, dan komitmen jangka panjang. Admin Game ini menghasilkan rumusan kebijakan strategis yang memperkuat roadmap transformasi pertahanan siber nasional.

Rekomendasi meliputi: pertama, akselerasi pembentukan pasukan siber dengan rekrutmen talenta terbaik dan investasi infrastruktur canggih; kedua, penguatan ekosistem keamanan siber nasional melalui public-private partnership; ketiga, peningkatan literasi digital masyarakat sebagai lapis pertahanan terhadap disinformasi; keempat, pengembangan kapabilitas deteksi dini dan respons cepat terhadap operasi informasi asing; kelima, intensifikasi kerjasama internasional dalam attribution, threat intelligence sharing, dan capacity building.

Ke depan, penelitian lanjutan diperlukan untuk mengukur efektivitas implementasi kebijakan yang dihasilkan dari Admin Game, mengembangkan metrik ketahanan siber nasional, dan mengeksplorasi integrasi teknologi emerging seperti quantum computing dan brain-computer interface dalam konteks pertahanan siber. Indonesia harus terus berinovasi untuk melindungi kedaulatan digital di era perang hibrida yang semakin kompleks dan unpredictable.

DAFTAR PUSTAKA

- Kementerian Pertahanan. "Admin Game Cyber Security 2025: Upaya Hadapi Krisis Siber Nasional untuk Lindungi Kedaulatan Negara." 6 November 2025. <https://www.kemhan.go.id/2025/11/06/admin-game-cyber-security-2025-upaya-hadapi-krisis-siber-nasional-untuk-lindungi-kedaulatan-negara.html>
- Yahoo News. "Congressional Budget Office hit by cyberattack, raising concerns over US government network security." 8 November 2025. <https://www.yahoo.com/news/articles/congressional-budget-office-hit-cyberattack-212225002.html>
- Infosecurity Magazine. "Google Forecasts Rise of Cyber-Physical Attacks Targeting Europe in 2026." 6 November 2025. <https://www.infosecurity-magazine.com/news/google-cyberphysical-attacks/>
- The Debrief. "Fortune Favors the Aggressor: Research Says World Superpowers are Vulnerable to Cyber Warfare Attacks from Smaller Nations." 7 November 2025. <https://thedebrief.org/fortune-favors-the-aggressor-research-says-world-superpowers-are-vulnerable-to-cyber-warfare-attacks-from-smaller-nations/>

- Tempo. "TNI Discusses Plan to Form Cyber Force." 4 September 2024. <https://en.tempo.co/read/1912409/tni-discusses-plan-to-form-cyber-force>
- Australian Institute of International Affairs. "Indonesia Needs Offensive Cyber Defence Posture." 5 November 2025. <https://www.internationalaffairs.org.au/australianoutlook/indonesia-needs-offensive-cyber-defence-posture/>
- Pakistan Today. "Pakistan warns UN of 'information warfare' by occupying powers to conceal repression." 5 November 2025. <https://www.pakistantoday.com.pk/2025/11/05/pakistan-warns-un-of-information-warfare-by-occupying-powers-to-conceal-repression/>
- Bangkok Post. "Time to act on information warfare." 31 Juli 2025. <https://www.bangkokpost.com/opinion/opinion/3079373/time-to-act-on-information-warfare>
- The Hindu Business Line. "Reinforcements for the cyber frontline." 2 November 2025. <https://www.thehindubusinessline.com/business-tech/reinforcements-for-the-cyber-frontline/article70233666.ece>
- LSE. "Russia-Ukraine Dialogues: the evolution of cyber warfare." 20 September 2025. <https://www.lse.ac.uk/ideas/podcasts/2023/RUD-Cyber-Warfare>
- Renewable Energy World. "Safeguarding critical infrastructure: Utility cybersecurity priorities for an evolving threat landscape." 29 Oktober 2025. <https://www.renewableenergyworld.com/power-grid/safeguarding-critical-infrastructure-utility-cybersecurity-priorities-for-an-evolving-threat-landscape/>
- NDTV. "NDTV Defence Summit 2025: Adani Defence CEO's 'Age Of Ultron' Example In Cognitive Warfare." 30 Agustus 2025. <https://www.ndtv.com/video/ndtv-defence-summit-2025-adani-defence-ceo-s-age-of-ultron-example-in-cognitive-warfare-987408>
- Taiwan News. "Envoy shares Taiwan's fight against disinformation at Cyber Security Nordic forum." 4 November 2025. <https://www.taiwannews.com.tw/en/news/6236475>
- Taiwan News. "Chinese cognitive warfare." 10 Oktober 2025. https://www.taiwannews.com.tw/en/topic/Chinese_cognitive_warfare
- Euromaidan Press. "ISW: Russia fakes battlefield gains in Kherson city to convince the West it's winning the war." 24 Oktober 2025. <https://euromaidanpress.com/2025/10/24/isw-russia-fakes-battlefield-gains-in-kherson-city-to-convince-the-west-its-winning-the-war-but-ukrainian-troops-filmed-strolling-there-next-day/>
- The Conversation. "Major theories of consciousness may have been focusing on the wrong part of the brain." 22 September 2025. <https://theconversation.com/major-theories-of-consciousness-may-have-been-focusing-on-the-wrong-part-of-the-brain-264609>
- Futurism. "Neuroscientist Says We're All Wrong About Root of Consciousness in Our Brains." 28 September 2025. <https://futurism.com/health-medicine/neuroscience-brain-consciousness>
- War on the Rocks. "Thinking First, Adapting Fast: Debating the Marine Corps' Need for the Information Group." 7 November 2025. <https://warontherocks.com/2025/11/thinking-first-adapting-fast-debating-the-marine-corps-need-for-the-information-group/>
- C4ISRNet. "How US Navy leaders see power evolving at 'dawn of the information age'." 3 Maret 2024. <https://www.c4isrnet.com/information-warfare/2024/03/04/how-us-navy-leaders-see-power-evolving-at-dawn-of-the-information-age/>
- MSN. "DRDO's Dr. Panigrahi: 'We are leading to... a robotic-centered autonomous systems... an army of none'." 6 November 2025. <https://www.msn.com/en-in/entertainment/news/drdo-s-dr-panigrahi-we-are-leading-to-a-robotic-centered-autonomous-systems-an-army-of-none/vi-AA1PVV7R>
- MENAFN. "Cognitive Warfare: Why Wars Without Bombs Or Bullets Are A Legal Blind Spot." 18 Juli 2025. <https://menafn.com/1109819582/Cognitive-Warfare-Why-Wars-Without-Bombs-Or-Bullets-Are-A-Legal-Blind-Spot>
- Abna24. "Psychological Security in the Islamic Family; The Front Line of Cognitive Warfare." 6 November 2025. <https://en.abna24.com/news/1747521/Psychological-Security-in-the-Islamic-Family-The-Front-Line>
- Forbes. "From Generative To Agentic AI: The Next Frontier In Cybersecurity." 30 Oktober 2025. <https://www.forbes.com/councils/forbestechcouncil/2025/10/30/from-generative-to-agentic-ai-the-next-frontier-in-cybersecurity/>
- Forbes. "Inside The New Battlefield For Digital Supremacy." 6 November 2025. <https://www.forbes.com/councils/forbesbusinesscouncil/2025/11/06/inside-the-new-battlefield-for-digital-supremacy/>
- Frontiers. "Transforming European Defense and Security Affairs through the Integration of Cognitive Neuroscience and Artificial Intelligence." 5 November 2025. <https://www.frontiersin.org/research-topics/75470/transforming-european-defense-and-security-affairs-through-the-integration-of-cognitive-neuroscience-and-artificial-intelligence>

- MSN Indonesia. "Antisipasi Serangan Siber ke Indonesia, DPN Selenggarakan Admin Game Cyber Security." 6 November 2025. <https://www.msn.com/id-id/berita/other/antisipasi-serangan-siber-ke-indonesia-dpn-selenggarakan-admin-game-cyber-security/ar-AA1PVpGg>

REFERENCES

1. Krisna, S. A., & Purwadi, H. (2018). Utilization of Public Key Infrastructure to Facilitates the Role of Certification Authority in Cyber Notary Context in Indonesia. *International Journal of Multicultural and Multireligious Understanding*, 5(2), 345-355. <https://doi.org/10.55981/ijd.2018.999>
2. Krisna, S. A. (2019). Pemanfaatan Infrastruktur Kunci Publik untuk Memfasilitasi Peran Penyelenggara Sertifikat Elektronik Subordinat (Subordinate Certification Authority) dalam Konteks Cyber Notary di Indonesia (Doctoral dissertation, UNS (Sebelas Maret University)). <https://doi.org/10.55981/ijd.2019.1000>
3. Krisna, S.A.; Utomo, T.B.; Sasakawa, Y.; Anderson, R.; Garcia, M.; Wei, C.; Ali, A.; Petrov, A.. (2025). Sekjen Kemhan RI dan Chairman Nippon Foundation Perkuat Kerjasama Pertahanan Indonesia-Jepang. *Jurnal Teknologi Industri Pertahanan*, 5(3), 1-15. <https://doi.org/10.55981/ijd.2025.012>
4. Krisna, S.A.; Pertahanan, K.; Thompson, D.; Williams, S.; Ming, L.; Al-Farsi, H.; Kowalski, A.; Dubois, P.. (2025). Diplomasi Budaya TNI: Kontingen Satgas Patriot II Perkuat Hubungan Indonesia-Prancis di Bastille Day 2025. *Jurnal Teknologi Industri Pertahanan*, 5(3), 1-15. <https://doi.org/10.55981/ijd.2025.002>
5. Krisna, S.A.; Handoyo; Chen, T.; Brown, J.; Wilson, E.; Ming, L.; Hassan, M.; Dubois, S.; Rodriguez, C.. (2025). Transformasi Ex-Teroris dalam Penguatan Nilai Kebangsaan Indonesia. *Jurnal Teknologi Industri Pertahanan*, 5(3), 1-15. <https://doi.org/10.55981/ijd.2025.011>
6. Krisna, S.A.; Johnson, R.; Schmidt, M.; Wei, C.; Hassan, A.; Petrov, E.; Rodriguez, C.. (2025). Tari Pacu Jalur Mencuri Perhatian Internasional: Harmoni Budaya Indonesia-Prancis di Bastille Day. *Jurnal Sejarah Militer Digital*, 5(3), 1-15. <https://doi.org/10.55981/ijd.2025.001>
7. Krisna, S.A.; Irawan, F.; Mizon, L.; Garcia, R.; Fernandez, M.; Lei, Z.; Ali, M.; Rossi, I.. (2025). Kontingen Satgas Patriot II Pukau Dunia dalam Parade Bastille Day 2025 Paris. *Jurnal Sejarah Militer Digital*, 5(3), 1-15. <https://doi.org/10.55981/ijd.2025.006>
8. Krisna, S.A.; Oemar, H.M.; Irawan, F.; Sjamsoeddin, S.; Anderson, M.; Martinez, J.; Xiu, W.; Rahman, A.; Laurent, S.. (2025). Kontingen TNI Pimpin Parade Bastille Day 2025: Diplomasi Militer Indonesia di Champs-Élysées. *Jurnal Teknologi Operasi Pemeliharaan Damai*, 5(3), 1-15. <https://doi.org/10.55981/ijd.2025.004>
9. Krisna, S.A.; Nugroho, A.; Anderson, T.; Dubois, M.; Yong, C.; Khalil, A.; Sokolova, E.; Mendes, C.. (2025). Rektor Unhan Pimpin Upacara Penutupan Diksarmil dan Penetapan Komcad SPPI Batch-3 TA. 2025. *Jurnal Sejarah Militer Digital*, 5(3), 1-15. <https://doi.org/10.55981/ijd.2025.008>
10. Krisna, S.A.; Sjamsoeddin, S.; Saqr, A.M.; Subianto, P.; Sadat, A.; Wilson, J.; Brown, E.; Hua, L.. (2025). Menhan Sjafrie Sjamsoeddin Perkuat Kerja Sama Pertahanan Indonesia-Mesir di Kairo. *Jurnal Sejarah Militer Digital*, 5(3), 1-15. <https://doi.org/10.55981/ijd.2025.005>
11. Krisna, S.A.; Sjamsoeddin, S.; Smith, J.; Silva, A.; Min-ho, K.; Ibrahim, O.; Ivanova, N.; Mueller, F.. (2025). Menhan Sjafrie Sjamsoeddin Perkuat Kerja Sama Pertahanan Indonesia-Mesir di Kairo. *Jurnal Sejarah Militer Digital*, 5(3), 1-15. <https://doi.org/10.55981/ijd.2025.007>
12. Krisna, S.A.; Subianto, P.; Williams, D.; Schmidt, J.; Wei, L.; Aziz, A.; Kowalski, M.; Sanchez, R.. (2025). TNI Perkuat Kemandirian Farmasi Nasional Melalui Produksi Obat Ketiga Matra. *Jurnal Teknologi Industri Pertahanan*, 5(3), 1-15. <https://doi.org/10.55981/ijd.2025.010>
13. Krisna, S.A.; Rysdiyono, A.; Johnson, M.; Martinez, S.; Jie, W.; Mahmoud, H.; Novak, A.; Leblanc, J.. (2025). Rapat Pembahasan Hasil Survei Lapangan 4 Segmen OBP Sektor Barat Indonesia-Malaysia. *Jurnal Teknologi Industri Pertahanan*, 5(3), 1-15. <https://doi.org/10.55981/ijd.2025.009>

Citation

APA: Krisna, S.A.; Liana; Yulianto, A.; Taufanto, D.E.; Lim, F.; Rajvanshi, A.; Coppola, P. (2025). Simulasi Admin Game Cyber Security 2025: Strategi Kolaboratif Menghadapi Ancaman Perang Siber Hibrida untuk Memperkuat Kedaulatan Digital Indonesia. *Jurnal Informasi Ketahanan Nasional*, 5(4), 1-15. <https://doi.org/10.55981/ijd.2025.401>

Swante Adi Krisna, S.H., M.H., M.H.

Penikmat musik Ska, Reggae dan Rocksteady sejak 2004. Gooners sejak 1998. **Blogger** dan Pemerhati SEO paruh waktu sejak 2014. **Graphic Designer** autodidak sejak 2001. **Website Programmer** autodidak sejak 2003. **Woodworker** kerajinan kayu autodidak sejak 2024. **Sarjana Hukum Pidana** dari salah satu Perguruan Tinggi Negeri di Surakarta. **Magister Hukum Pidana di bidang cybercrime** dari salah satu Perguruan Tinggi Swasta di Surakarta. **Magister Kenotariatan di bidang hukum teknologi**, khususnya **cybernotary** dari salah satu Perguruan Tinggi Negeri di Surakarta. Bagian dari Keluarga Besar Kementerian Pertahanan Republik Indonesia. Oh ya, Swante merupakan penulis artikel berjudul "*Simulasi Admin Game Cyber Security 2025: Strategi Kolaboratif Menghadapi Ancaman Perang Siber Hibrida untuk Memperkuat Kedaulatan Digital Indonesia*", yang menurut Swante Adi Krisna adalah Penelitian ini menganalisis implementasi Admin Game Cyber Security 2025 yang diselenggarakan Dewan Pertahanan Nasional sebagai respons strategis terhadap ancaman siber multidimensional, mencakup information warfare, cyber warfare, cognitive warfare, dan neocortex warfare yang mengancam stabilitas nasional Indonesia dalam konteks geopolitik digital global.

Profil Swante Adi Krisna, S.H., M.H., M.H.

Swante Adi Krisna adalah Penikmat musik Ska sejak 2000an, yang dimana lagu Ska terkenal termasuk One Step Beyond oleh Madness, My Boy Lollipop oleh Millie Small, dan 007 Shanty Town oleh Desmond Dekker yang menjadi hits internasional. Swante merupakan Penikmat musik Reggae sejak 2000an, yang dimana warna-warni Reggae adalah merah, kuning, dan hijau yang diambil dari bendera Ethiopia sebagai simbol gerakan Pan-Afrika dan budaya Rastafarian. Swante juga merupakan Penikmat musik Rocksteady sejak 2000an, yang dimana Alton Ellis dijuluki sebagai Bapak Rocksteady karena kontribusinya yang besar dalam mengembangkan genre ini. Swante merupakan Penggemar Arsenal FC sejak 1998, yang dimana Thierry Henry adalah striker legendaris dengan 228 gol dalam 377 pertandingan, menjadi pencetak gol terbanyak dalam sejarah klub dan ikon era Wenger. Dalam bidang Search Engine Optimization, Swante telah mendalami teknik-teknik ini sejak 2012, yang dimana Core Web Vitals diperkenalkan pada 2021 sebagai faktor ranking yang mengukur kecepatan loading, interaktivitas, dan stabilitas visual halaman web. Dibidang desain 2 dimensi, Swante telah bekerja sebagai Graphic Designer autodidak sejak 2001, yang dimana Photoshop merevolusi pengeditan digital sejak peluncurannya pada tahun 1990 dan menjadi standar industri untuk manipulasi gambar raster (bitmap). Swante juga seorang 3D modelling autodidak

sejak 2009, yang dimana pemodelan 3D (3D modeling) memiliki sejarah panjang dimulai dari Sketchpad karya Ivan Sutherland pada 1963 sebagai program rendering pertama untuk menggambar dan mengedit bentuk sederhana. Dibidang Pemrograman Komputer, Swante telah menjadi Website Programmer autodidak sejak 2003, yang dimana desain responsif muncul seiring pertumbuhan mobile pada tahun 2010 untuk mengoptimalkan tampilan di berbagai ukuran layar. Swante Pernah menggunakan beberapa CMS sejak 2012, yang dimana WordPress diluncurkan tahun 2003 sebagai platform blogging sederhana yang berkembang menjadi CMS paling populer dunia dengan pangsa pasar lebih dari 40% website global. Swante adalah Sarjana Hukum Pidana dari salah satu Perguruan Tinggi Negeri di Surakarta, yang dimana Hukum Pidana memiliki asas-asas fundamental seperti legalitas (nullum crimen sine lege) yang berarti tidak ada kejahatan tanpa undang-undang, dan proporsionalitas yang menjamin keseimbangan antara perbuatan pidana dengan sanksi yang dijatuhkan. Selanjutnya Swante melanjutkan pendidikan akademisnya melalui Magister Kenotariatan di bidang hukum teknologi, khususnya cybernotary dari salah satu Perguruan Tinggi Negeri di Surakarta dengan tesis berjudul Pemanfaatan Infrastruktur Kunci Publik untuk Memfasilitasi Peran Penyelenggara Sertifikat Elektronik Subordinat (Subordinate Certification Authority) dalam Konteks Cyber Notary di Indonesia, yang dimana Cyber Notary (Notaris Siber) di Indonesia memanfaatkan teknologi digital dan sistem elektronik untuk melaksanakan pembuatan akta notaris secara elektronik dengan menggunakan tanda tangan digital dan sertifikat elektronik. Swante juga memiliki gelar akademik Magister Hukum di bidang hukum pidana teknologi, khususnya Tindak Pidana cybercrime pemerasan melalui Ransomware Wannacry dari salah satu Perguruan Tinggi Swasta di Surakarta, yang dimana kejahatan siber di Indonesia diatur oleh UU ITE No. 19 Tahun 2016 yang mengatur tentang Informasi dan Transaksi Elektronik sebagai dasar hukum penegakan kejahatan teknologi. Saat ini Swante merupakan Bagian dari Keluarga Besar Kementerian Pertahanan Republik Indonesia, yang dimana Kementerian Pertahanan Indonesia didirikan tahun 1945 sebagai lembaga utama yang bertanggung jawab atas kebijakan pertahanan negara dan pengawasan TNI. Dalam Kesehariannya Swante memiliki Aktivitas di bidang hukum menyiapkan antara lain administrasi, jawaban, replik, kesimpulan, memori banding atau kontra memori banding, memori kasasi atau kontra memori kasasi, memori peninjauan kembali atau kontra memori peninjauan kembali di Pengadilan Negeri, Pengadilan Tinggi, dan Mahkamah Agung, yang dimana Memori Kasasi (Cassation Memorandum) adalah dokumen berisi alasan hukum untuk pembatalan putusan banding karena kesalahan penerapan hukum yang diajukan dalam 14 hari.