KEJAHATAN SIBER DAN TRANSNATIONAL ORGANIZED CRIME

TANTANGAN BAGI INTELIJEN INDONESIA

Tim Penulis:
Yogi Hartanto, Arif Anggodo, Arief Isti Pramusinta, Hilmansyah, Rizqi Ramadhani, Shinta Anggraini, Data, Eldi Bisma Putra Mahendra Bintang, Sri Patmi

KEJAHATAN SIBER DAN TRANSNATIONAL ORGANIZED CRIME

TANTANGAN BAGI INTELIJEN INDONESIA

Tim Penulis:
Yogi Hartanto, Arif Anggodo, Arief Isti Pramusinta, Hilmansyah, Rizqi Ramadhani, Shinta Anggraini, Data, Eldi Bisma Putra Mahendra Bintang, Sri Patmi

Penerbit widina

KEJAHATAN SIBER DAN *TRANSNATIONAL ORGANIZED CRIME* TANTANGAN BAGI INTELIJEN INDONESIA

Tim Penulis:
Yogi Hartanto, Arif Anggodo, Arief Isti Pramusinta, Hilmansyah, Rizqi Ramadhani, Shinta Anggraini, Data, Eldi Bisma Putra Mahendra Bintang, Sri Patmi

Desain Cover:
Andi Juliandi

Sumber Ilustrasi:
www.freepik.com

Tata Letak:
Handarini Rohana

Editor:
Sri Patmi, S.I.Kom., M.Han.

ISBN:
978-634-246-563-9
978-634-246-522-6 (PDF)

Cetakan Pertama:
Januari, 2026

PENERBIT:
WIDINA MEDIA UTAMA
Komplek Puri Melia Asri Blok C3 No. 17 Desa Bojong Emas
Kec. Solokan Jeruk Kabupaten Bandung, Provinsi Jawa Barat

Anggota IKAPI No. 519/JBA/2025
Website: www.penerbitwidina.com
Instagram: @penerbitwidina
Telepon (022) 87355370

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya buku Kejahatan Siber dan *Transnational Organized Crime*: Tantangan bagi Intelijen Indonesia dapat terselesaikan dengan baik. Kehadiran buku ini berangkat dari kegelisahan akademik sekaligus urgensi strategis mengenai semakin kompleksnya ancaman yang dihadapi Indonesia dalam era digital yang melaju tanpa batas. Di tengah transformasi global yang ditandai oleh percepatan teknologi informasi, kejahatan siber dan kejahatan terorganisasi lintas negara telah berkembang menjadi ancaman multidimensi yang tidak hanya menyerang aspek ekonomi dan sosial, tetapi juga langsung menantang kapasitas pertahanan dan intelijen nasional.

Perubahan lanskap ancaman dalam ruang siber telah mengaburkan batas antara aktor negara dan *non*-negara, antara kriminalitas dan geopolitik, serta antara operasi militer dan kejahatan transnasional. Serangan tidak lagi hadir melalui invasi fisik, tetapi melalui kode berbahaya, eksploitasi kerentanan sistem, kebocoran data, manipulasi informasi, hingga gangguan terhadap infrastruktur kritis. Konvergensi antara kejahatan siber dan *transnational organized crime* menghadirkan bentuk ancaman baru yang bersifat terdistribusi, sulit dilacak, dan melampaui yurisdiksi hukum tradisional. Dalam kondisi ini, intelijen Indonesia dituntut untuk tidak sekadar adaptif, tetapi juga transformatif terhadap dinamika ancaman modern.

Buku ini disusun untuk memberikan pemahaman mendalam mengenai akar masalah, karakteristik, pola operasi, dan implikasi strategis dari kejahatan siber yang terhubung dengan jaringan kriminal lintas negara. Dengan menggabungkan perspektif akademis, analisis empirik, serta studi kasus yang relevan, buku ini mencoba memberikan gambaran komprehensif tentang bagaimana modus kejahatan digital berkembang, bagaimana kelompok kriminal memanfaatkan teknologi untuk memperluas jaringan, dan bagaimana negara-negara tertentu

memanfaatkan ruang siber sebagai instrumen proyeksi kekuasaan. Seluruh pembahasan diarahkan pada satu tujuan: memperkuat wawasan, kesadaran, dan kapasitas strategis bagi para pemangku kepentingan nasional, terutama intelijen dan aparat keamanan.

Selain menggambarkan ancaman, buku ini juga menekankan pentingnya membangun sistem pertahanan siber nasional yang tangguh (*resilient*), integratif, dan adaptif. Penguatan intelijen siber, peningkatan kemampuan deteksi dini berbasis kecerdasan buatan, harmonisasi regulasi, keamanan data, dan kerja sama internasional menjadi fondasi penting untuk menghadapi spektrum ancaman yang semakin kompleks. Keamanan siber bukan lagi urusan satu lembaga, tetapi merupakan ekosistem besar yang menuntut kolaborasi pemerintah, sektor swasta, akademisi, dan masyarakat pengguna teknologi.

Kami berharap buku ini dapat menjadi rujukan strategis bagi akademisi, mahasiswa, aparat penegak hukum, praktisi keamanan, serta para pembuat kebijakan yang berkepentingan dengan isu pertahanan dan keamanan digital. Lebih dari itu, kami berharap buku ini mampu menumbuhkan kesadaran kolektif bahwa pertahanan negara di era siber tidak lagi berada hanya di barak-barak militer atau ruang rapat pemerintahan, tetapi juga ada di server data, pusat teknologi, ruang digital publik, dan perangkat yang kita gunakan sehari-hari.

Akhir kata, kami mengucapkan terima kasih kepada seluruh pihak yang telah membantu dalam proses penyusunan buku ini. Semoga karya ini memberikan kontribusi bagi penguatan intelijen Indonesia dan menjaga kedaulatan negara di tengah tantangan dunia digital yang terus berubah.

Jakarta, Januari 2026
Penulis

DAFTAR ISI

BAB I
TRANSFORMASI *LANDSCAPE* KEAMANAN GLOBAL DI ERA SIBER

Dunia sedang mengalami lonjakan perubahan yang sangat cepat ketika teknologi digital menjadi bagian utama dari kehidupan manusia. Ruang siber kini hadir sebagai domain baru yang mempengaruhi dinamika politik, ekonomi, pertahanan, dan keamanan global. Perubahan ini menuntut setiap negara untuk tidak hanya memahami perkembangan digital, tetapi juga menyesuaikan strategi keamanannya agar tetap relevan di tengah arus transformasi global.

Ancaman yang dulu bersifat fisik kini berevolusi menjadi ancaman yang lebih senyap, tersembunyi, dan sulit dideteksi. Serangan siber mampu melumpuhkan sistem penting hanya dalam hitungan detik tanpa kehadiran pelaku di lokasi kejadian. Kompleksitas ancaman ini mengubah cara negara melihat keamanan; tidak lagi terbatas pada perlindungan fisik, tetapi juga pada perlindungan jaringan, aplikasi, dan data yang menjadi tulang punggung kehidupan modern.

Di balik pesatnya digitalisasi, muncul aktor-aktor baru yang memanfaatkan ruang siber untuk tujuan ilegal. Mereka menjadikan anonimitas internet sebagai tameng untuk melakukan serangan, pencurian data, manipulasi informasi, atau bahkan mengganggu stabilitas negara. Para pelaku dapat berasal dari individu, kelompok kriminal, hingga aktor negara yang mengembangkan kemampuan siber untuk kepentingan strategis.

Perkembangan rivalitas geopolitik juga memperkuat posisi ruang siber sebagai arena kompetisi antarnegara. Serangan terhadap infrastruktur kritis, pencurian rahasia pertahanan, dan penyebaran disinformasi menjadi bagian dari strategi kontemporer yang digunakan untuk memperoleh keuntungan politik. Konflik kini terjadi dalam bentuk yang lebih halus dan tidak kasatmata, namun dampaknya dapat menghancurkan stabilitas sebuah negara.

BAB II
PROFIL, TIPE, DAN POLA OPERASI KEJAHATAN SIBER & *TRANSNATIONAL ORGANIZED CRIME*

Bab sebelumnya telah menguraikan secara komprehensif bagaimana transformasi lanskap keamanan global di era siber menciptakan perubahan signifikan terhadap karakter ancaman kontemporer. Kompleksitas teknologi digital, konvergensi sistem komunikasi global, serta meningkatnya interdependensi negara-negara di dunia menjadi fondasi yang memungkinkan munculnya bentuk ancaman baru yang tidak lagi terbatas pada batas-batas geografis. Oleh karena itu, memasuki Bab II ini, pembahasan diarahkan secara lebih spesifik untuk memahami aktor, struktur, dan mekanisme serangan yang beroperasi dalam domain kejahatan siber dan jaringan kriminal transnasional.

Perkembangan teknologi digital bukan hanya menghadirkan efisiensi dan percepatan proses sosial-ekonomi, tetapi juga membuka peluang besar bagi kelompok kriminal untuk memanfaatkan celah dalam infrastruktur digital global. Kejahatan siber kini tidak lagi dilakukan oleh individu tunggal dengan kemampuan teknis terbatas, melainkan oleh kelompok terorganisasi yang menjalankan operasi lintas negara dengan struktur yang semakin profesional. Transformasi ini menjadikan pemetaan profil pelaku dan pola operasional sebagai aspek penting dalam memahami ancaman yang terus berkembang.

Meningkatnya konektivitas global dan penggunaan internet secara masif telah mendorong integrasi antara *cybercrime* dan *transnational organized crime*. Di berbagai belahan dunia, kelompok kriminal tradisional seperti kartel narkotika, jaringan perdagangan manusia, hingga organisasi pencucian uang mulai mengadopsi teknik digital untuk memperluas jangkauan serta melindungi operasi mereka dari

BAB III
ANCAMAN KEJAHATAN SIBER DAN TOC TERHADAP KEAMANAN NASIONAL INDONESIA

Bab II sebelumnya telah memetakan profil, tipe, dan pola operasi kejahatan siber serta *Transnational Organized Crime* (TOC), mulai dari struktur jaringan, modus lintas negara, hingga bagaimana teknologi digital *dark* web, *crypto*, AI, dan *deepfake* dimanfaatkan untuk memperkuat jejaring kriminal. Peta itu penting sebagai "gambaran musuh di medan tempur". Namun, memahami siapa dan bagaimana mereka beroperasi baru menjawab separuh persoalan. Bab III akan melangkah lebih jauh: bukan lagi hanya *siapa* dan *bagaimana*, tetapi *sejauh apa ancaman itu mengguncang keamanan nasional Indonesia* termasuk stabilitas politik, ketahanan ekonomi, keamanan siber nasional, dan kepercayaan publik terhadap negara.

Dalam konteks Indonesia, kejahatan siber dan TOC bukan sekadar fenomena kriminal biasa; keduanya telah berkembang menjadi ancaman strategis yang menyentuh dimensi keamanan nasional. Serangan terhadap infrastruktur digital pemerintahan, eksploitasi sektor keuangan berbasis siber, perdagangan orang dan narkotika yang dikoordinasikan melalui *platform* digital, hingga infiltrasi ke ruang informasi publik adalah contoh-contoh nyata bagaimana ranah kriminal "bawah tanah" bersinggungan langsung dengan fungsi-fungsi vital negara. Apa yang tampak di permukaan sebagai sekadar kebocoran data, penipuan *online*, atau serangan *ransomware*, pada level strategis dapat bermetamorfosis menjadi gangguan terhadap layanan publik, menurunnya kepercayaan masyarakat, dan bahkan membuka celah intervensi aktor asing.

Bab III akan mengurai bagaimana ancaman siber dan TOC berkelindan dengan tiga pilar utama keamanan nasional: keamanan siber negara, keamanan ekonomi, dan keamanan sosial-politik. Pada

BAB IV
TANTANGAN INTELIJEN INDONESIA DALAM MENANGANI KEJAHATAN SIBER & TOC

Bab IV menggeser fokus pembahasan dari apa ancaman kejahatan siber dan *transnational organized crime* (TOC) terhadap keamanan nasional Indonesia sebagaimana telah diuraikan dalam Bab III menjadi *siapa* dan *bagaimana* institusi yang berada di garis depan untuk mendeteksi, menganalisis, dan merespons ancaman tersebut: yaitu komunitas intelijen Indonesia. Jika pada Bab III dipetakan kerentanan infrastruktur kritis, kebocoran data, serangan terhadap sektor pemerintah dan pertahanan, hingga dampak ekonomi–politik–sosial, maka Bab IV akan membahas sejauh mana intelijen negara siap menghadapi lanskap ancaman baru yang bersifat digital, terfragmentasi, lintas batas, dan sangat cepat berubah.

Dalam konteks ini, intelijen Indonesia menghadapi transformasi medan tempur yang fundamental. Musuh tidak lagi selalu hadir dalam bentuk aktor fisik bersenjata atau jaringan kriminal konvensional, tetapi juga dalam bentuk *threat actor* anonim di ruang siber: kelompok *ransomware*, sindikat penipuan lintas negara, jaringan perdagangan manusia dan narkotika berbasis digital, hingga aktor negara yang melakukan *cyber espionage* dan operasi pengaruh (*influence operations*). Artinya, metodologi pengumpulan informasi, analisis, dan penyajian *intelligence product* harus beradaptasi dengan realitas baru ini, tanpa kehilangan akar pada mandat utama: melindungi kedaulatan dan stabilitas nasional.

Digitalisasi yang masif di sektor publik dan privat menciptakan paradoks bagi intelijen: di satu sisi, tersedia data dalam volume besar (*big data*) yang dapat menjadi sumber emas bagi analisis ancaman; di sisi lain, banjir informasi ini menimbulkan tantangan dalam memilah, memverifikasi, dan mengolah data menjadi intelijen yang relevan,

BAB V
STRATEGI INTELIJEN INDONESIA MENGHADAPI *CYBERCRIME* & *TRANSNATIONAL ORGANIZED CRIME*

Intelijen Indonesia memasuki babak baru dalam menghadapi ancaman siber dan kejahatan terorganisasi lintas negara yang semakin kompleks. Sebagaimana dipaparkan dalam Bab IV, berlapis-lapis tantangan mulai dari regulasi yang tidak sinkron, kapasitas teknologi yang belum memadai, hingga sifat ancaman yang semakin terselubung menunjukkan bahwa mekanisme penanganan yang ada saat ini belum mampu memberikan respons yang adaptif. Oleh karena itu, strategi yang dibahas dalam Bab V ini dirancang sebagai langkah langsung untuk menutup celah-celah kritis yang telah diidentifikasi sebelumnya.

Laju perkembangan ancaman siber yang jauh lebih cepat dari perkembangan kemampuan negara menjadi alasan mendasar perlunya strategi yang bersifat proaktif dan berbasis prediksi. Kelompok kriminal kini memanfaatkan kecerdasan buatan, serangan otomatis, enkripsi berlapis, hingga infrastruktur digital global untuk mengaburkan jejak. Bab IV telah menekankan bahwa pendekatan reaktif tidak lagi memadai, sehingga Bab V harus mengarahkan intelijen Indonesia untuk membangun sistem deteksi dini yang mampu mengantisipasi ancaman sebelum terjadi.

Kendala koordinasi dan fragmentasi antar-lembaga yang terurai pada Bab IV juga mengharuskan adanya strategi integrasi komando dan interoperabilitas. Ketidaksinkronan arus informasi selama ini menjadi hambatan utama dalam merespons serangan siber dan aktivitas TOC yang bersifat lintas batas dan lintas sektor. Oleh sebab itu, Bab V merumuskan strategi yang memfokuskan pada penguatan kolaborasi, standardisasi protokol intelijen, dan pembangunan pusat komando terpadu.

DAFTAR PUSTAKA

Aini, N., & Lubis, F. (2023). Tantangan pembuktian dalam kasus kejahatan siber. *Judge: Jurnal Hukum.*

Alinea. (2019). Potensi tumpang tindih RUU Kamtansiber BSSN. *Alinea.*

Ananta, A. R. R., Wicaksono, D. B., Indrawati, I., Istikhomah, & Amalina, Z. (2025). Potensi konflik kewenangan pada perlindungan dari ancaman siber di Indonesia. *Jurnal Rechtsvinding.* (Badan Pembinaan Hukum Nasional)

Associated Press. (2024). Interpol clamps down on *cybercrime* and arrests over 1,000 suspects in Africa. *AP News.*

Badan Narkotika Nasional (BNN). (2024). *Brainstorming Kejahatan Cyber Narcotics pada Dark Web – Seri Pertama.*

Badan Pembinaan Hukum Nasional (BPHN). (n.d.). *Kajian Konvensi Budapest dan regulasi tindak pidana teknologi informasi.*

Badan Perencanaan Pembangunan Nasional. (2024). *Ringkasan Eksekutif Visi Indonesia 2045.* Bappenas.

Badan Siber dan Sandi Negara (BSSN). (2023). *Lanskap keamanan siber Indonesia 2023.* EduCSIRT Kemendikbud.

Badan Siber dan Sandi Negara (BSSN). (2024). *Lanskap Keamanan Siber Indonesia 2024 (Laporan).* https://bssn.go.id

Badan Siber dan Sandi Negara (BSSN). (2025). *Lanskap Keamanan Siber Indonesia (Laporan).* https://csirt.kemenpora.go.id/wp-content/uploads/2025/02/keamanan.pdf

Badan Siber dan Sandi Negara. (2023). *Lanskap Keamanan Siber 2023.* EduCSIRT Kemendikbud.

Badan Siber dan Sandi Negara. (2024). *Lanskap Keamanan Siber Indonesia 2024.* BSSN.

BCG. (2024). *2024 Cybersecurity Workforce Report.* Boston Consulting Group.

BDO/ISC2. (2024). *Bridging the Cybersecurity Talent Gap/Global shortfall report.* BDO / ISC2.

Binus University. (2024). *10 Kasus Cyber Crime yang Bikin Heboh di Indonesia.* Binus Bandung.

BPK. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE.* JDIH BPK.

BPK. (2024). *UU No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (perubahan terbaru).* JDIH BPK.

BSSN/Antara. (2022). *1.6 billion cyberattacks in Indonesia in 2021: BSSN* (news report). ANTARA.

Bunga, D. (2019). Legal response to *cybercrime* in global and *national* scope. *Padjadjaran Journal of Law, 6*(3), 69–88.

CCDCOE (NATO Cooperative *Cyber* Defence Centre of Excellence). (2018). *Insider threat study.* CCDCOE. https://ccdcoe.org/uploads/2018/10/*Insider_Threat*_Study_CCDCOE.pdf

CNN Indonesia. (2020, May 3). Kronologi lengkap 91 juta akun Tokopedia bocor dan dijual. *CNN Indonesia.* https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention).* Council of Europe. https://www.coe.int/en/web/*cybercrime*/the-budapest-convention

CSIRT Kemenpora. (2025). *Laporan Penanganan Insiden Siber Nasional.*

CSIRT Kominfo. (2024). *Laporan Tahunan Kamsiber 2024.* Kementerian Komunikasi dan Informatika. (CSIRT Komdigi)

CSIRT Kominfo. (2024). *Laporan Tahunan Keamanan Siber 2024.* Kominfo-CSIRT.

*Cyber*lands. (2024). *Top 10 cybersecurity breaches in Indonesia. Cyber*lands.

Cybersecurity Ventures. (2024). *Cybercrime to cost the world $9.5 trillion USD annually in 2024.*

Cybersecurity Ventures. (2025). *Cyberwarfare and cybercrime report: 2015–2025 projections.*

DigitalSociety. (2024, August 15). Tumpang tindih tanggung jawab kementerian dan badan siber dalam merespons serangan *ransomware*. *DigitalSociety.id.*

Europol. (2023). *288 dark web vendors arrested in major marketplace seizure* (press release). Europol.

Europol. (2024). *Common challenges in cybercrime 2024.* Europol.

FBI. (2020). *Operation DisrupTor* (press release). Federal Bureau of Investigation. https://www.fbi.gov/news/stories/operation-disruptor-jcode-shuts-down-*dark*net-drug-*vendor*-092220

Firdaus, R. A. (2023). Perlindungan hukum dan pencegahan kejahatan siber di era digital dalam sistem hukum di Indonesia. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam.*

Global Initiative Against *Transnational Organized Crime*. (2023). *Global Organized Crime Index 2023.* Global Initiative.

Global *Organized Crime* Index. (2025). *Indonesia country profile 2025.* Global Initiative Against *Transnational Organized Crime*.

Gov*Insider*. (2025). BSSN: Kolaborasi adalah kunci ketahanan siber nasional. *GovInsider Asia.*

IBM Security. (2024). *Cost of a Data Breach Report 2024.* IBM. https://www.ibm.com/security/data-breach

IBM. (2024). *83% of organizations reported insider attacks in 2024* (blog summary). IBM. https://www.ibm.com/think/insights/83-percent-organizations-reported-*insider-threat*s-2024

Indonesia *Cybersecurity analysis*. (2024). *Indonesia cybersecurity readiness survey summary.* IndoSec Summit / CSIS Indonesia.

Inter*national* Criminal Police Organization / IC3–FBI. (2024). *2024 IC3 annual report.* Internet *Crime* Complaint Center.

Inter*national* Telecommunication Union. (2024). *Global Cybersecurity Index 2024.* ITU.

Isfan Fajar, R., Hardyansah, R., & Darmawan, D. (2024). Development of *cybercrime* law in Indonesia: Challenges and prospects. *SICO Journal of Science, Technology and Society.*

ITU. (2024). *Global Cybersecurity Index & national capacity building overview.* Inter*national* Telecommunication Union.

Katadata. (2024). *Pemerintahan, Sektor Paling Rentan Insiden Siber 2024.* Databoks Katadata.

Ken Research. (2024). *Indonesia Cybersecurity Market 2019–2030: Skills gap and market growth.* Ken Research.

Khan, B., Riaz, A., & Parveen, K. (2025). Mining the shadows: A *hybrid* NLP framework for *dark* web *cybercrime* investigation. *International Journal for Electronic Crime Investigation.*

Komunitas Digital Indonesia/Komdigi. (2025). Tumpang tindih tugas badan siber dengan lembaga lain. *Komdigi.* (Kementerian Komunikasi dan Digital)

Loso, J., & Nugroho, B. (2025). Regulasi keamanan siber dan penegakan hukum terhadap *cybercrime* di Indonesia. *Sanskara Hukum dan HAM.*

Maurer, T. (2021). Colonial *Pipeline* case study (*ransomware*) — in: *Studies on cyber incidents and impacts* (MIT monograph chapter). (MIT Press Direct)

Maurer, T. (2021). Lessons from the Colonial *Pipeline ransomware* case. In *Studies on cyber incidents and impacts* (pp. xx–xx). MIT Press.

Menpan RI. (2021, May 22). Data BPJS Kesehatan diduga bocor. *Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi.* https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas

Microsoft. (2024). *Digital Defense Report 2024.* Microsoft.

National Cyber Security Centre. (n.d.). *Guidance and National Cyber Approach.* UK Government.

National Institute of Justice (NIJ). (2020). *Taking on the Dark Web: Investigative needs.*

NCC Group. (2024). *The Lazarus group: North Korean scourge for +10 years.* NCC Group.

Nurul Aini, & Lubis, F. (2023). Tantangan Pembuktian dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum.*

Odebade, A. T., & Benkhelifa, E. (2023). A comparative study of *national cyber* security strategies of ten *nation*s. *International Journal of Cybersecurity Strategy.*

OECD. (2022). *OECD Digital Security Governance Report.*

Office of the Director of *National Intelligence* — CTIIC. (2015). *Cyber Threat Intelligence Integration Center (CTIIC).* DNI.

Organisation for Economic Co-operation and Development (OECD). (2024). *Digital Public Infrastructure for Digital Governments (Report).*

Osula, A. M. (2015). *Mutual legal assistance & other mechanisms* (CCDCOE Research). CCDCOE.

Ottis, R. (2008). *Analysis* of the 2007 *Cyber Attack*s Against Estonia. *CCDCOE/Analytical paper.*

Pase, A. T., & Fernando, Z. J. (2025). *Dark* Web *Crime*: Criminal Law Challenges in the Era of *Cybercrime*. *The Indonesian Journal of International Clinical Legal Education.* (UNNES Journal)

Ponemon Institute. (2025). *Cost of insider threats global report (2025).* Ponemon Institute. https://ponemon.dtexsystems.com/

Reeder, J. R., & Hall, K. (2021). Lessons Learned from the Colonial *Pipeline Ransomware Attack*. *Cyber Defense Review.*

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).* https://peraturan.bpk.go.id/Download/26683/UU%20Nomor%2011%20Tahun%202008.pdf

Research on AI-*Driven Cybersecurity*. (2024). *AI-Driven Cybersecurity: Leveraging Big data for Advanced Threat Detection and Risk Mitigation* (Paper). (ResearchGate)

Research on Indonesian Digital Work*force* (Gayatri *et al*., 2022). (2022). *The Indonesian Digital Workforce Gaps in 2021–2025. Sustainability.* (MDPI)

Reuters. (2024, March 27). Southeast Asia *human trafficking* now a global crisis, Interpol says. *Reuters.*

Reuters. (2025). Billion-dollar *cyberscam* industry spreading globally, UN says. *Reuters News.*

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux.

Runturambi, A. J. S. (2025). *Hybrid crime*s among Indonesian migrant workers in Southeast Asia. *Journal of Policing, Intelligence and Counter Terrorism.* (ScienceDirect)

Rusman, & Kamaludin, A. (2024). Investigation of *Cyber Crime* in the Indonesian Legal Framework. *Journal La Sociale.* (New In Era)

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press.

Security Journal. (2023). *Foundations and trends in darknet-related criminals.*

Shaikh, F., & Shaikh, F. (2024). The *Dark* Web: Challenges and *Counter*measures in Combating *Cybercrime*. *IJRASET.*

Sriyai, S. (2025). Global inequality and digital vulnerability: Unpacking *online scam*s and *human trafficking*. *ISEAS Perspective,* (45). (ISEAS-Yusof Ishak Institute)

Suari, K. R. A., & Sarjana, I. M. (2024). Analisis Forensik Digital terhadap Perdagangan Data Pribadi di *Dark* Web Menggunakan OSINT & *Threat Intelligence*. *JUKTISI.* (LKP Karya Prima Journal)

Suseno, S. (2025). *Cybercrime* in the new criminal code in Indonesia. *Cogent Social Sciences, 11*(1). (Taylor & Francis *Online*)

Tempo.co. (2023, August 25). Risiko tumpang tindih wewenang telik sandi. *Tempo.*

The Guardian. (2024). Russia's FSB protected Evil Corp gang that carried out NATO *cyber-attack*s. *The Guardian.*

United *Nation*s Office on Drugs and *Crime* (UNODC). (2024). *Transnational organized crime and the convergence of cyber and other modalities.*

United *Nation*s Office on Drugs and *Crime*. (2021). *Darknet cybercrime threats to Southeast Asia.* United *Nation*s Office on Drugs and *Crime*. https://www.unodc.org/roseap/en/*dark*net.html

United *Nation*s Office on Drugs and *Crime*. (2023). *Darknet cybercrime threats to Southeast Asia.* UNODC.

United *Nation*s Office on Drugs and *Crime*. (2023). *Transnational Organized Crime: Global Analysis 2023.* UNODC.

United *Nation*s Office on Drugs and *Crime*. (2024). *Global Report on Trafficking in Persons 2024/Forced criminality and online scamming centres.* UNODC.

United *Nation*s Office on Drugs and *Crime*. (2024). *Responding to emerging crimes in Indonesia.* UNODC Regional Office for Southeast Asia and the Pacific.

United *Nation*s Office on Drugs and *Crime*. (2024). *Transnational organized crime and the convergence of cyber modalities.* UNODC.

United *Nation*s Office on Drugs and *Crime*. (n.d.). *Trafficking and organized crime – Indonesia.* UNODC.

United *Nation*s Office on Drugs and *Crime*. (n.d.). *UN cybercrime convention – Full text.* UNODC.

United *Nation*s Office on Drugs and *Crime*. (n.d.). *United Nations Convention against Transnational Organized Crime (UNTOC).* UNODC.

UNODC. (2021). *Darknet cybercrime threats to Southeast Asia.* United *Nation*s Office on Drugs and *Crime*.

UNODC. (2023). *Darknet cybercrime threats to Southeast Asia.* United *Nation*s Office on Drugs and *Crime*.

UNODC. (2023). *Transnational Organized Crime: Global Analysis 2023.* United *Nation*s Office on Drugs and *Crime*.

UNODC. (2024). *Transnational Organized Crime and the Convergence of Cyber Modalities.* United *Nation*s Office on Drugs and *Crime*.

Utami, T. K. (2025). Personal data breach cases in Indonesia after the enactment of the personal data protection law. *Journal of Contemporary Law.* (Pubmedia Journal Series)

Verizon. (2024). *Data Breach Investigations Report 2024.* Verizon.

Wall Street Journal. (2024). *Cyber* leaders struggle to fill AI security jobs. *The Wall Street Journal.*

World Economic Forum. (2023). *Global Cybersecurity Outlook 2023.* World Economic Forum.

World Economic Forum. (2025). *Global cybersecurity outlook 2025.* World Economic Forum.

Yuliana, R., & colleagues. (2025). *Cyber* law policy development: Indonesia's response to global *cybercrime* challenges. *Jurnal Politik dan Hukum, 12*(1). (Riset Press)

PROFIL PENULIS

Yogi Hartanto, S.H., S.Fil., M.S.I.

Sehari-hari penulis bekerja sebagai Perancang Peraturan Perundang-undangan pada Direktorat Hukum, Deputi bidang Hukum dan Kerja Sama, Badan Narkotika Nasional. Mempunyai ketertarikan untuk menekuni pada bidang keilmuan filsafat, hukum, sosial, keamanan, dan pertahanan. Penulis menyadari penguasaan pada bidang keilmuan berkontribusi besar pada hasil kualitas kebijakan yang dihasilkan, peraturan perundang-undangan yang dibentuk, dan hasil evaluasi kebijakan yang komprehensif dari berbagai aspek.

Arif Anggodo, S.E., M.Sc.In.

Penulis lahir di Batang, Jawa Tengah dari pasangan buruh pabrik tekstil dan guru TK di daerah Alas Roban, Pantura Jawa. Ayah dan Ibunya selalu mendukung agar anaknya mengenyam pendidikan lebih baik. Pendidikan dasar dan menengah dilalui di Kota Berkembang, sedangkan pendidikan tingkat atas ia lanjutkan di Kota Satria, mengikuti jejak kakaknya. Penulis menjalani pendidikan di bidang ekonomi/keuangan di Sekolah Tinggi Akuntansi Negara serta Sekolah Tinggi Ilmu Ekonomi Indonesia, Jakarta. Gelar master ia dapatkan dari Perguruan Tinggi Kedinasan di Bogor, Jawa Barat. Dengan tetap menjunjung tinggi Tri Dharma Perguruan Tinggi, saat ini penulis fokus ke permasalahan keamanan ekonomi/keuangan serta strategi pertahanan di tengah gempuran disrupsi yang menjadi suatu keniscayaan global. Email: arif.anggodo@outlook.com.

Arief Isti Pramusinta, S.Tr.Ak., M.Sc.In.

Pegiat ekonomi dan keuangan serta strategi pertahanan.

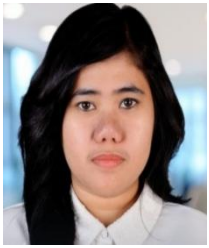
Hilmansyah, S.E., M.S.I.

Penulis merupakan lulusan Program Studi Ekonomi dari Universitas Jenderal Soedirman (Unsoed). Memiliki minat yang kuat terhadap isu-isu strategis, terutama di bidang pertahanan dan keamanan negara serta geopolitik internasional. Latar belakang ekonomi yang dimiliki menjadi dasar bagi penulis dalam menganalisis keterkaitan antara dinamika ekonomi, kebijakan publik, dan perkembangan keamanan global.

Rizqi Ramadhani, S.Sos., M.S.I.

Penulis merupakan penggiat kajian pertahanan dan Intelijen. Penulis meyakini bahwa intelijen yang baik dan profesional dapat menjadi indikator keamanan negara. karena tugas intelijen adalah memberikan peringatan dini mengenai ancaman potensial dan nyata. Dengan kemampuan ini, pemerintah dapat mengambil langkah-langkah pencegahan, penangkalan, dan penanggulangan sebelum ancaman tersebut berkembang menjadi krisis.

Shinta Anggraini, S.H., M.S.I.



Penulis saat ini aktif bekerja dalam tugas dan fungsi di bidang obat dan makanan. Penulis memiliki latar Pendidikan S1 Hukum Universitas Riau dan melanjutkan pendidikan magister pada perguruan tinggi kedinasan di Bogor. Penulis memiliki ketertarikan pada analisis kasus dan *trend* terutama yang berkaitan dengan tugas dan fungsi penulis sebagai salah satu pegawai pada instansi pemerintah.

Letkol Data, S.Tr.(Han)., S.M., M.Sc.In., CRMP.

Penulis lahir di Grobogan Jawa tengah. Penulis saat ini berdinas di Ditjakstra Ditjen Strategi Pertahanan Kementerian Pertahanan Republik Indonesia. Penulis merupakan militer aktif dari Korps Marinir TNI AL yang telah memiliki pengalaman penugasan yang beragam. Kepala Seksi Penyusun Evaluasi Kebijakan Umum Pertahanan Negara dan Kebijakan Penyelenggaraan Pertahanan Negara, Subdit Sunevajakstra Ditjakstrahan Ditjen Strahan Kemhan. Penulis berlatar belakang Militer dari Korps Marinir TNI AL.

Eldi Bisma Putra Mahendra Bintang, S.Sos., M.Sc.In.

Penulis memperoleh gelar sarjana di bidang kriminologi dan magister di bidang Kajian Intelijen. Saat ini penulis bekerja sebagai Kepala Seksi Pengendalian Krisis pada Direktorat Penindakan, Badan Nasional Penanggulangan Terorisme Republik Indonesia.

Sri Patmi, S.I.Kom., M.Han.

Penulis adalah akademisi, penulis, sekaligus peneliti muda yang konsisten menekuni bidang pertahanan dan keamanan di era kontemporer. Saat ini, beliau berkiprah sebagai Asisten Dosen di Universitas Pertahanan Republik Indonesia (Unhan RI), khususnya pada kajian strategi pertahanan laut. Dengan capaian akademik gemilang sebagai lulusan terbaik Program Studi Strategi Pertahanan laut (GPA 3,98), ia meneguhkan diri sebagai sosok yang memadukan kecermelangan akademis dengan pengabdian nyata bagi bangsa.

Sebelum terjun di dunia akademik pertahanan, Sri Patmi telah meniti karier profesional di berbagai sektor, mulai dari industri *digital marketing*, pengembangan SDM, hingga manajemen proyek strategis. Pengalaman lintas sektor ini memperkuat wawasannya tentang pentingnya integrasi antara inovasi teknologi, sumber daya manusia, dan strategi pertahanan negara.

Sebagai penulis produktif, ia telah menghasilkan beragam karya ilmiah maupun populer, mencakup buku, artikel jurnal, hingga tulisan media massa. Karya-karya *non*fiksi terbarunya membahas isu-isu penting seperti *Defense Innovation and Maritime Defense Technology Management* (2024), *Revolution in Military Affairs 21st Century* (2024), serta *Indonesian Maritime Defense Underwater Surveillance* (2025). Selain itu, ia juga aktif menulis puisi, esai, dan antologi yang mencerminkan sisi *human*is dari seorang peneliti pertahanan.

Keaktifannya dalam forum ilmiah, pelatihan, dan bimbingan teknis di kalangan akademisi maupun militer menjadikan Sri Patmi sebagai penghubung antara dunia akademik dengan praktik strategis di lapangan. Ia juga pernah menjadi pembicara dalam peluncuran buku *Jejak Dr. Nurdin: Working with Conscience, Building with Vision* serta narasumber teknis di Sekolah Staf dan Komando TNI Bandung.

Melalui karya ini, “Smart Defense: Adaptasi Strategi Pertahanan Menyongsong Indonesia Emas 2045 di Tengah Revolusi Digital dan Globalisasi”, Sri Patmi menghadirkan refleksi dan strategi komprehensif tentang bagaimana Indonesia dapat membangun ketahanan

pertahanan yang adaptif, inovatif, dan berdaulat dalam menghadapi tantangan global.

Di era ketika kehidupan manusia terhubung oleh jutaan jaringan tak kasatmata, ancaman terhadap keamanan negara tidak lagi datang dari moncong senjata atau armada militer, tetapi dari serangan senyap yang menyusup melalui kode, server, dan perangkat yang kita gunakan setiap hari. Kejahatan Siber dan *Transnational Organized Crime*: Tantangan bagi Intelijen Indonesia menghadirkan gambaran paling komprehensif tentang bagaimana dunia digital membentuk ulang medan tempur modern dan mendorong Indonesia memasuki babak baru pertarungan melawan kejahatan lintas negara.

Buku ini membuka mata pembaca terhadap kenyataan bahwa serangan siber bukan sekadar isu teknologi, melainkan ancaman strategis terhadap kedaulatan nasional. Dengan memanfaatkan data global, studi kasus aktual, dan analisis akademik yang mendalam, buku ini mengungkap bagaimana kelompok kriminal terorganisasi, *hacktivist*, hingga aktor negara memanfaatkan ruang siber untuk mencuri, memeras, memanipulasi, dan melumpuhkan sistem vital sebuah negara.

Melalui penjelajahan yang tajam, pembaca diajak memahami bagaimana kejahatan siber dan *transnational organized crime* kini berkonvergensi menjadi ancaman hibrida yang tidak hanya menggerogoti ekonomi, tetapi juga merusak kepercayaan publik dan melemahkan stabilitas politik. Buku ini juga menyoroti tantangan besar yang dihadapi intelijen Indonesia dalam membaca pola serangan, melakukan atribusi, hingga memperkuat pertahanan digital di tengah percepatan transformasi digital nasional. Dengan gaya narasi yang lugas dan berbasis bukti, karya ini menawarkan peta jalan strategis yang dapat menjadi rujukan penting bagi akademisi, aparat keamanan, pembuat kebijakan, serta siapa pun yang ingin memahami masa depan pertahanan negara di era siber. Buku ini tidak hanya menyajikan pengetahuan, tetapi juga membangkitkan kesadaran: bahwa di balik layar perangkat kita, sebuah perang baru tengah berlangsung dan bangsa ini harus bersiap menghadapinya.

www.penerbitwidina.com
@penerbitwidina
penerbit widina
penerbitwidina@gmail.com
widina store
widina bookstore

Layanan Pembaca & Penerbitan Buku
0815-7000-699

SCANME

Politik, Keamanan & Pertahanan

ISBN 978-634-246-563-9

9 786342 465639