ISSN: 2338 4638

Volume 7 Nomor 7 (2023)

'ADALAH

Buletin Hukum & Keadilan

Perkembangan Cybercrime dan Dampaknya terhadap Keamanan Nasional Indonesia: Analisis Ancaman Asimetris dan Strategi Ketahanan Siber

Gilang Rizki Aji Putra*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v7i7.51842

Abstract:
Cybercrime has transformed from conventional computer-based offenses into a multidimensional threat targeting critical infrastructure, political stability, and national economic resilience. This article analyzes the evolving modus operandi of cybercrime in Indonesia over the past decade and assesses its impact on national security within a multidimensional security framework. Using normative legal research with conceptual, statutory, and case study approaches, the study finds that cybercrime in Indonesia has progressed from online fraud and hacking to structured cyberattacks against national data infrastructure, digital espionage, and large-scale disinformation campaigns threatening political stability. The analysis indicates that existing regulatory frameworks, including the Electronic Information and Transactions Law and the Personal Data Protection Law, as well as institutional bodies such as the National Cyber and Crypto Agency (BSSN), remain largely reactive and insufficient to address the asymmetric and transnational nature of these threats. The article concludes that cybercrime constitutes an existential challenge to Indonesia's digital sovereignty and requires comprehensive legislative, institutional, and regional intelligence cooperation reforms.

Keywords: Cybercrime, National Security, Asymmetric Threats, BSSN, Hybrid Warfare.

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

A. PENDAHULUAN

Perkembangan *cybercrime* global menunjukkan eskalasi yang mengkhawatirkan. *World Economic Forum* dalam *Global Risks Report* 2024 menempatkan serangan siber sebagai salah satu dari lima risiko global teratas, bersama dengan kegagalan mitigasi perubahan iklim dan konflik geopolitik. Biaya ekonomi yang diakibatkan oleh *cybercrime* global diperkirakan mencapai 10,5 triliun dolar AS pada tahun 2025, menjadikannya sebagai ekonomi kriminal terbesar ketiga di dunia setelah perdagangan narkoba dan pemalsuan (Brenner, 2022). Angka ini menunjukkan bahwa cybercrime bukan lagi sekadar kenakalan digital, melainkan telah menjadi industri kejahatan terorganisasi yang sistematis, profesional, dan lintas negara.

Di Indonesia, eskalasi cybercrime memperlihatkan pola yang serupa. Laporan tahunan Badan Siber dan Sandi Negara (BSSN) mencatat peningkatan lebih dari 300% anomali lalu lintas data dan serangan siber dalam empat tahun terakhir, dengan sektor perbankan, pemerintahan, dan kesehatan sebagai target utama (BSSN, 2023). Lebih dari itu, modus operandi yang berkembang tidak lagi terbatas pada penipuan daring (*online fraud*) atau peretasan (*hacking*) sederhana, tetapi telah merambah ke ranah ransomware terhadap fasilitas publik, pencurian data strategis berskala besar, hingga kampanye disinformasi politik yang terstruktur dan sistematis. Fenomena ini menimbulkan pertanyaan

serius: apabila *cybercrime* kini mampu melumpuhkan layanan publik dan memanipulasi persepsi politik, apakah ia masih bisa dikategorikan sebagai masalah kriminal biasa, ataukah sudah bertransformasi menjadi ancaman nyata bagi keamanan nasional?

Sayangnya, perspektif arus utama di Indonesia masih cenderung menempatkan cybercrime dalam kerangka hukum pidana biasa, belum sepenuhnya mengintegrasikannya ke dalam doktrin pertahanan dan keamanan negara. Padahal, konsep keamanan nasional kontemporer telah bergeser dari pendekatan tradisional yang berfokus pada ancaman militer menuju pendekatan multidimensional yang mencakup keamanan ekonomi, politik, sosial, dan informasi (Buzan, Wæver, & de Wilde, 1998). Rumusan masalah dalam artikel ini adalah: Pertama, bagaimana dinamika perkembangan modus dan skala *cybercrime* di Indonesia dalam perspektif ancaman terhadap keamanan nasional? Kedua, mengapa kerangka hukum dan kelembagaan yang ada belum mampu merespons secara efektif, dan strategi apa yang harus ditempuh? Tujuannya adalah untuk menganalisis cybercrime sebagai ancaman asimetris yang memiliki dampak struktural terhadap kedaulatan digital nasional, serta merumuskan pendekatan yang lebih holistik dalam menanganinya.

B. *CYBERCRIME* DALAM PARADIGMA KEAMANAN MULTIDIMENSIONAL

Untuk memahami dampak *cybercrime* terhadap keamanan nasional, diperlukan perluasan kerangka analisis dari kriminologi konvensional menuju studi keamanan kritis. *Copenhagen School* melalui teori sekuritisasi (*securitization*) yang dikembangkan oleh Buzan et al. (1998) menawarkan kerangka yang relevan. Menurut teori ini, sebuah isu dapat dikategorikan sebagai ancaman keamanan jika ia dieksistensialkan oleh aktor negara sebagai ancaman terhadap objek referensi, seperti kedaulatan negara, integritas teritorial, atau stabilitas masyarakat dan memerlukan tindakan luar biasa di luar prosedur politik normal. Dalam konteks ini, *cybercrime* yang semula dipandang sebagai isu kriminal telah mengalami proses sekuritisasi di banyak negara, termasuk melalui pembentukan komando siber militer dan anggaran keamanan siber yang masif.

Ancaman siber, termasuk *cybercrime*, memiliki karakteristik asimetris. Pelaku bisa individu, kelompok kriminal, atau aktor negara yang menggunakan *proxy*, dengan biaya serangan yang relatif murah tetapi dampak yang luar biasa besar. Konsep *asymmetric threat* dalam keamanan siber menggambarkan situasi di mana aktor yang lemah secara konvensional dapat menimbulkan kerusakan yang tidak proporsional terhadap negara yang kuat (Libicki, 2009). Serangan terhadap infrastruktur

informasi vital seperti jaringan listrik, sistem perbankan, atau pusat data pemerintahan dapat melumpuhkan fungsi-fungsi dasar negara tanpa perlu mengerahkan satu pun pasukan militer. Selain itu, munculnya fenomena *cyber-enabled crime*, yaitu kejahatan yang menggunakan infrastruktur digital sebagai pengganda kekuatan, mengaburkan batas antara kejahatan ekonomi dan ancaman terhadap keamanan nasional.

Dalam spektrum yang lebih luas, *cybercrime* telah menjadi komponen integral dari *hybrid warfare* strategi konflik yang menggabungkan operasi militer konvensional dengan perang informasi, perang siber, dan perang ekonomi. Kampanye disinformasi yang didanai oleh aktor kriminal atau negara asing untuk mempolarisasi masyarakat, melemahkan legitimasi pemerintah, atau memengaruhi hasil pemilihan umum adalah contoh nyata *hybrid threat* (Schmitt, 2017). Di sinilah letak urgensi pembahasan: Indonesia harus membaca *cybercrime* bukan hanya dalam KUHP atau UU ITE, tetapi juga dalam strategi pertahanan dan doktrin keamanan nasional.

C. PERKEMBANGAN MODUS *CYBERCRIME* DAN DAMPAKNYA TERHADAP PILAR KEAMANAN NASIONAL

1. Dari Penipuan Daring ke Serangan Sistematis terhadap Infrastruktur Publik

Modus *cybercrime* di Indonesia telah mengalami eskalasi kualitatif. Lima tahun lalu,

dominasi pemberitaan masih terfokus pada phishing, penipuan *e-commerce*, dan carding. Kini, ancaman yang paling mengkhawatirkan adalah serangan *ransomware* terhadap institusi pemerintahan. Insiden serangan terhadap Pusat Data Nasional Sementara (PDNS) pada Juni 2024 oleh varian Brain Cipher merupakan *game changer*. Server-server yang menyimpan data berbagai kementerian dan layanan publik disandera, menyebabkan lumpuhnya layanan imigrasi, perizinan, dan administrasi publik lainnya selama berhari-hari. Serangan ini jelas menunjukkan bahwa kedaulatan digital Indonesia sangat rentan. Apabila pusat data yang mengelola data kependudukan, keamanan, atau pertahanan berhasil dibobol, implikasinya tidak hanya kerugian finansial, tetapi juga ancaman terhadap kerahasiaan negara dan keselamatan warga (Nugroho, 2024).

Serangan terhadap infrastruktur kritis adalah direct assault terhadap keamanan nasional. Ia berbeda dari penipuan daring yang merugikan individu. Kerugiannya bersifat massal dan sistemik, menurunkan kepercayaan publik terhadap kemampuan negara, dan membuka celah bagi sabotase lebih lanjut. Dalam konteks hukum internasional, serangan siber terhadap infrastruktur kritis suatu negara dapat dikategorikan sebagai pelanggaran kedaulatan atau bahkan *use of force* jika memiliki dampak setara dengan serangan bersenjata (Schmitt, 2017). Namun, karena sulitnya atribusi

yakni memastikan secara teknis dan politis siapa pelaku di balik serangan negara seringkali kesulitan untuk memberikan respons yang proporsional.

2. Spionase Digital dan Pencurian Data Strategis

Kasus "Bjorka" yang mencuat pada tahun 2022 dan 2023 menjadi fenomena spionase digital yang paling mengganggu. Seorang atau sekelompok aktor anonim berhasil meretas dan membocorkan data-data sensitif milik pejabat tinggi negara, dokumen kementerian, serta data pribadi warga negara. Kebocoran ini tidak hanya mempermalukan pemerintah di forum internasional, tetapi juga mengekspos kerentanan sistem komunikasi dan penyimpanan data rahasia negara. Dalam doktrin intelijen, hilangnya data rahasia akibat spionase baik yang dilakukan oleh aktor negara maupun non-negara adalah pukulan langsung terhadap keamanan nasional karena informasi tersebut dapat dimanfaatkan oleh pihak asing untuk kepentingan politik, ekonomi, atau militer (ID-SIRTII, 2023).

Lebih jauh, maraknya perdagangan data pribadi di dark web menimbulkan ancaman serius terhadap keamanan warga negara. Data Nomor Induk Kependudukan (NIK), data perbankan, dan riwayat kesehatan yang bocor dapat digunakan untuk penipuan identitas, spionase korporasi, hingga profiling politik. Akumulasi data ini, jika jatuh ke tangan aktor yang berniat destabilisasi, dapat menjadi senjata untuk pemerasan massal atau

manipulasi elektoral. Dalam konteks ini, *cybercrime* pencurian data bukan lagi sekadar pelanggaran privasi, melainkan fondasi bagi ancaman *hybrid* yang lebih luas.

3. Disinformasi Terstruktur dan Ancaman terhadap Stabilitas Politik

Perkembangan mutakhir *cybercrime* yang paling berdampak terhadap keamanan nasional adalah penyalahgunaan platform digital untuk kampanye disinformasi. Pada Pemilihan Umum 2024, berbagai riset menunjukkan adanya jejaring akun bot dan *coordinated inauthentic behavior* yang menyebarkan narasi polarisasi, ujaran kebencian, serta klaim kecurangan terstruktur (Mulyadi, 2024). Banyak dari kampanye ini bukan sekadar ulah buzzer politik, melainkan bagian dari bisnis jasa *disinformation-as-a-service* yang digerakkan oleh motif ekonomi. Artinya, pelaku menyewakan infrastruktur disinformasi kepada pihak-pihak yang membayar, tanpa peduli terhadap dampak sosialnya.

Efek disinformasi terhadap keamanan nasional sangat nyata: polarisasi sosial akut dapat melemahkan kohesi nasional, memicu konflik horizontal, dan merusak kepercayaan publik terhadap lembaga demokrasi. Dalam jangka panjang, masyarakat yang terfragmentasi menjadi lahan subur bagi radikalisasi dan ekstremisme. Ketika polarisasi mencapai titik tertentu, legitimasi pemerintah untuk memerintah pun dipertanyakan,

menciptakan krisis konstitusional. Maka, memerangi disinformasi bukan hanya soal melindungi individu dari hoaks, melainkan soal mempertahankan kedaulatan politik negara. Sayangnya, pendekatan hukum Indonesia saat ini masih melalui kacamata pasal-pasal penyebaran berita bohong (Pasal 28 ayat (1) UU ITE) yang bersifat reaktif dan individual, belum mampu membongkar infrastruktur dan model bisnis di balik industri disinformasi (Harahap & Nugroho, 2023).

4. Dampak Ekonomi dan Kedaulatan Finansial Digital

Cybercrime juga memukul pilar ekonomi keamanan nasional. Sektor jasa keuangan digital adalah target favorit bagi sindikat penipuan dan peretasan. Kasus penipuan *binary option* yang melibatkan influencer nasional mencatat kerugian hingga puluhan triliun rupiah. Selain itu, serangan terhadap *payment gateway* dan dompet elektronik berpotensi melumpuhkan sistem pembayaran nasional. Ketika masyarakat kehilangan kepercayaan terhadap keamanan transaksi digital, dampak ekonominya sangat besar, terutama bagi negara yang sedang gencar mendorong digitalisasi keuangan seperti Indonesia. Ancaman terhadap stabilitas sistem keuangan adalah salah satu dimensi keamanan ekonomi yang diakui dalam doktrin pertahanan siber (BSSN, 2023). Tanpa keamanan siber yang andal, cita-cita Indonesia menjadi digital economy powerhouse hanya akan menjadi ilusi.

D. KELEMAHAN STRUKTURAL DALAM PENANGANAN *CYBERCRIME* DI INDONESIA

Mengapa *cybercrime* yang dampaknya begitu nyata terhadap keamanan nasional masih sulit ditanggulangi? Setidaknya ada tiga kelemahan struktural. Pertama, legal gap dan fragmentasi kelembagaan. Indonesia belum memiliki Undang-Undang Keamanan dan Ketahanan Siber yang komprehensif yang mengintegrasikan aspek pertahanan, penegakan hukum, intelijen, dan diplomasi siber. BSSN sebagai otoritas keamanan siber masih memiliki kewenangan yang terbatas, lebih fokus pada audit dan respons insiden, bukan pada koordinasi penindakan dan ofensif siber. Sementara itu, Polri, TNI, Kominfo, dan BIN memiliki mandat parsial yang seringkali tumpang tindih.

Kedua, kapasitas sumber daya manusia dan teknologi yang asimetris. Jumlah pakar forensik digital dan analis ancaman siber di Indonesia sangat terbatas, baik di sektor publik maupun swasta. Laboratorium forensik digital belum merata di seluruh daerah, sementara pelaku *cybercrime* terus meningkatkan kecanggihan alat dan metodenya. Ketiga, ketiadaan kerangka kerjasama internasional yang kuat. *Cybercrime* bersifat transnasional, namun Indonesia belum meratifikasi Konvensi Budapest dan belum memiliki perjanjian ekstradisi dan bantuan hukum timbal balik yang memadai dengan negara-negara yang menjadi basis operasi sindikat

siber (Santoso, 2023). Akibatnya, aktor utama di balik banyak serangan besar tetap bebas berkeliaran di luar negeri tanpa dapat disentuh.

E. MENEMPATKAN *CYBERCRIME* SEBAGAI ANCAMAN KEAMANAN NASIONAL

Untuk merespons secara efektif, Indonesia harus merekonstruksi paradigma penanganan cybercrime. Perubahan pertama adalah mengadopsi doktrin *active defense* dan *deterrence by denial*. Negara tidak cukup hanya memasang tembok, tetapi harus memiliki kemampuan untuk mendeteksi, melacak, dan membalas serangan siber secara proporsional. Ini memerlukan pembentukan komando siber yang terintegrasi di bawah TNI atau lembaga khusus, yang juga diperkuat dengan regulasi yang jelas tentang *rules of engagement* di ranah siber.

Kedua, legislasi harus segera diselesaikan. Rancangan Undang-Undang Keamanan dan Ketahanan Siber yang sudah digodok bertahun-tahun harus segera disahkan. Undang-undang ini harus memberikan kewenangan yang memadai kepada otoritas siber nasional, menetapkan standar keamanan yang ketat bagi infrastruktur informasi vital, serta memberikan perlindungan hukum bagi aparat yang melakukan operasi siber defensif. Ketiga, kerjasama internasional harus diintensifkan. Indonesia harus segera meratifikasi Konvensi Budapest dan aktif dalam ASEAN *Cybersecurity Cooperation Strategy.* Hanya dengan kolaborasi lintas

batas, upaya penegakan hukum tidak akan berhenti pada aktor lapangan, tetapi mampu mencapai otak sindikat di kancah global (Kusumawardhani, 2024).

Keempat, literasi keamanan siber dan ketahanan masyarakat terhadap disinformasi harus menjadi program nasional yang masif. Keamanan siber tidak bisa hanya bertumpu pada pemerintah; ia harus menjadi tanggung jawab bersama antara negara, sektor swasta, akademisi, dan masyarakat sipil (*multistakeholder approach*). Masyarakat yang cerdas secara digital adalah benteng paling kokoh melawan cybercrime.

F. KESIMPULAN

Cybercrime di Indonesia telah melampaui definisi kriminal biasa. Modusnya yang terus berevolusi dari *ransomware* terhadap pusat data nasional, spionase dan kebocoran data strategis, hingga kampanye disinformasi yang mempolarisasi bangsa telah membuktikan bahwa ia adalah ancaman nyata bagi keamanan nasional dalam dimensi politik, ekonomi, dan sosial. Menjawab rumusan masalah pertama, *cybercrime* adalah ancaman asimetris yang memiliki kapasitas melumpuhkan fungsi vital negara dan menggerogoti kedaulatan digital. Menjawab rumusan kedua, kelemahan regulasi yang fragmentaris, kapasitas SDM yang timpang, dan minimnya kerjasama internasional adalah hambatan utama yang membuat respons negara masih jauh dari memadai.

Rekomendasi yang diajukan mencakup: pertama, percepatan pengesahan Undang-Undang Keamanan dan Ketahanan Siber yang memberikan kewenangan penuh kepada otoritas siber nasional; kedua, pembangunan kapasitas ofensif dan defensif siber melalui pendidikan dan rekrutmen talenta; ketiga, ratifikasi Konvensi Budapest dan penguatan aliansi siber regional; serta keempat, integrasi perspektif *cybercrime* ke dalam doktrin pertahanan negara. Tanpa langkah-langkah strategis ini, Indonesia akan terus menjadi raksasa digital yang rentan, mudah dilumpuhkan oleh entitas yang tidak terlihat dan tidak terprediksi.

REFERENSI:

Brenner, S. W. (2022). Cybercrime: Criminal Threats from Cyberspace (2nd ed.). Praeger.

BSSN. (2023). Lanskap Keamanan Siber Indonesia 2023. Jakarta: Badan Siber dan Sandi Negara.

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A New Framework for Analysis. Lynne Rienner Publishers.

Harahap, A., & Nugroho, B. (2023). Menuju Tata Kelola Multi-Pemangku Kepentingan dalam Penegakan Hukum Siber Indonesia. Jurnal Legislasi Indonesia, 20(4), 512–530.

ID-SIRTII. (2023). Laporan Aktivitas Serangan Siber terhadap Domain Indonesia tahun 2022.

Indonesia Security Incident Response Team on Internet Infrastructure.

Kusumawardhani, A. (2024). Kecerdasan Buatan dan Kekosongan Hukum Pidana di Indonesia. Jurnal Hukum Siber, 6(1), 15–32.

Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation.

Mulyadi, L. (2024). Disinformasi dan Kedaulatan Politik: Studi Pemilu 2024. Jurnal Komunikasi dan Politik, 12(1), 45–63.

Nugroho, A. (2024). Serangan Ransomware terhadap Infrastruktur Publik: Pembelajaran dari Kasus PDNS. Jurnal Ketahanan Informasi, 5(2), 88–105.

Santoso, L. (2023). Kapasitas Forensik Digital dalam Sistem Peradilan Pidana Indonesia. Jurnal Yudisial, 16(3), 301–322. https://doi.org/10.29123/jy.v16i3.542

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