PERANG SIBER SEBAGAI ANCAMAN MULTIDIMENSIONAL DALAM PERSPEKTIF GLOBAL, REGIONAL, DAN NASIONAL

Arsenius Wisnu Aji Patria Perkasa
Program Studi Kriminologi, Fakultas Ilmu Sosial dan Studi Global, Universitas Budi Luhur, Indonesia
Email korespondensi: arsenius.wisnu@budiluhur.ac.id

Abstract

Cybercrime and cyberwarfare have evolved into major transnational threats over the past two decades. Unlike conventional crimes, cyberattacks cross national borders without physical barriers, creating new dilemmas for states in safeguarding sovereignty and security. The World Economic Forum (2025) ranks cybercrime among the greatest global risks, with estimated annual economic losses reaching USD 10.5 trillion. This threat is systemic, affecting economic stability, political legitimacy, social cohesion, and democratic processes. This study employs a normative-analytical approach using the risk governance framework and securitization theory. Classical typologies such as cybertrespass, cybertheft, cyberobscenity, and cyberviolence are enriched with contemporary forms, including digital steganography and AI-driven cybercrime. From an International Relations perspective, realism views cyberattacks as instruments of state power, liberalism emphasizes international cooperation, and constructivism highlights the formation of global norms such as the Tallinn Manual. In the Indonesian context, ransomware attacks on hospitals, political hoaxes, and biometric data exploitation reveal structural vulnerabilities arising from low digital literacy and weak adaptive regulation. The main conclusion is that cybercrime must be understood as a multidimensional threat requiring the integration of technical, social, political, and ethical dimensions through legal regulation, digital literacy, international cooperation, and the development of global norms.

Abstrak

Kejahatan siber (cybercrime) dan perang siber (cyberwarfare) telah berkembang menjadi ancaman transnasional utama dalam dua dekade terakhir. Berbeda dengan kejahatan konvensional, serangan siber melintasi batas negara tanpa hambatan fisik, sehingga menimbulkan dilema baru bagi negara dalam menjaga kedaulatan dan keamanan. Laporan World Economic Forum (2025) menempatkan kejahatan siber sebagai salah satu risiko global terbesar, dengan kerugian ekonomi diperkirakan mencapai USD 10,5 triliun per tahun. Ancaman ini bersifat sistemik, berdampak pada stabilitas ekonomi, politik, sosial, dan legitimasi demokrasi. Kajian ini menggunakan pendekatan normatif-analitis dengan kerangka risk governance framework dan securitization theory. Tipologi klasik seperti cybertrespass, cybertheft, cyberobscenity, dan cyberviolence diperkaya dengan tipologi kontemporer, termasuk steganografi digital dan kejahatan berbasis kecerdasan buatan. Perspektif hubungan internasional memperlihatkan bahwa realisme menekankan serangan siber sebagai instrumen kekuasaan negara, liberalisme menyoroti kerja sama internasional, sementara konstruktivisme menekankan pembentukan norma global seperti Tallinn Manual. Dalam konteks Indonesia, kasus ransomware terhadap rumah sakit, hoaks politik, dan eksploitasi data biometrik menunjukkan kerentanan struktural akibat rendahnya literasi digital dan lemahnya regulasi adaptif. Kesimpulan utama kajian ini adalah bahwa kejahatan siber harus dipahami sebagai ancaman multidimensional yang menuntut integrasi aspek teknis, sosial, politik, dan etika melalui regulasi hukum, literasi digital, kerja sama internasional, serta pembangunan norma global.

Kata Kunci

ancaman multidimensional; cybercrime; cyberwarfare; keamanan siber; risk governance; securitization

PENDAHULUAN

Dalam dua dekade terakhir, dunia internasional menghadapi transformasi besar dalam lanskap ancaman global. Jika pada awal 2000-an fokus utama kebijakan keamanan internasional masih tertuju pada terorisme pasca serangan 11 September 2001, maka sejak 2010 perhatian mulai bergeser ke ranah digital. Kejahatan siber (cybercrime) dan perang siber (cyberwarfare) muncul sebagai fenomena baru yang menantang tatanan keamanan tradisional. Berbeda dengan kejahatan konvensional yang terbatas secara geografis, kejahatan siber melintasi batas negara tanpa hambatan fisik, menciptakan dimensi transnasional yang kompleks dan sulit dikendalikan oleh mekanisme hukum tradisional.

Kejahatan siber tidak hanya menyangkut pencurian data atau peretasan sistem komputer, tetapi juga menyangkut ancaman terhadap infrastruktur vital negara, manipulasi opini publik, dan bahkan intervensi dalam proses politik. Fenomena ini menimbulkan pertanyaan mendasar: bagaimana negara dapat mempertahankan kedaulatan dan keamanan dalam ruang siber yang tidak mengenal batas teritorial? Pertanyaan ini semakin relevan ketika kita menyadari bahwa ruang siber telah menjadi arena baru bagi konflik geopolitik, di mana negara-negara menggunakan teknologi digital sebagai instrumen kekuasaan.

Laporan World Economic Forum berjudul Global Risks Report (2025) menempatkan kejahatan siber sebagai salah satu dari lima risiko utama dunia, sejajar dengan perubahan iklim, krisis energi, dan pandemi. Cybersecurity Ventures (2025) memprediksi kerugian ekonomi global akibat kejahatan siber mencapai USD 10,5 triliun per tahun. Angka ini menunjukkan bahwa kejahatan siber bukan sekadar ancaman teknis, melainkan ancaman sistemik yang dapat mengguncang stabilitas ekonomi global. Kerugian tersebut mencakup biaya pemulihan sistem, kehilangan produktivitas, kerusakan reputasi, serta dampak jangka panjang terhadap kepercayaan publik terhadap institusi digital.

Selain aspek ekonomi, kejahatan siber juga memiliki dimensi sosial dan politik yang signifikan. Serangan siber terhadap sistem kesehatan dapat mengganggu pelayanan publik, serangan terhadap sistem keuangan dapat menimbulkan krisis kepercayaan, dan serangan terhadap sistem politik dapat merusak legitimasi demokrasi. Dengan demikian, kejahatan siber tidak hanya berdampak pada individu atau perusahaan, tetapi juga pada stabilitas negara dan tatanan internasional. Hal ini menjadikan kejahatan siber sebagai ancaman transnasional yang setara dengan terorisme, perubahan iklim, dan pandemi.

Indonesia sebagai negara berkembang juga tidak luput dari ancaman ini. Kasus serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) di Surabaya pada 2024 menunjukkan kerentanan infrastruktur digital nasional (Rakhmayanti, 2024). Serangan tersebut tidak hanya menimbulkan kerugian finansial, tetapi juga mengganggu pelayanan publik yang bergantung pada data digital. Hal ini menunjukkan bahwa kejahatan siber bukan hanya isu global, tetapi juga isu lokal yang memerlukan perhatian serius dari pemerintah dan masyarakat.

Meski demikian, penting untuk membedakan antara *cybercrime* dan *cyberwarfare*. Cybercrime umumnya bermotif finansial atau kriminal, dilakukan oleh individu maupun kelompok non-negara, sedangkan cyberwarfare melibatkan aktor negara dengan tujuan strategis, geopolitik, dan militer. Perbedaan ini krusial agar analisis tidak mencampuradukkan ancaman kriminal transnasional dengan konflik digital antarnegara. Oleh karena itu, naskah ini bertujuan untuk menilai kejahatan siber sebagai ancaman global, menempatkannya dalam kerangka hubungan internasional, serta membandingkannya dengan isu global lain seperti terorisme, perubahan iklim, dan pandemi. Pendekatan interdisipliner digunakan untuk memberikan gambaran komprehensif tentang bagaimana kejahatan siber berkembang, bagaimana ia dikategorikan, serta bagaimana negara dan masyarakat internasional meresponsnya.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan desain normatif-analitis. Kerangka analisis utama yang digunakan adalah risk governance framework untuk memahami kejahatan siber sebagai risiko sistemik yang melibatkan interdependensi antara teknologi, aktor, dan institusi, serta *Securitization Theory* dari Copenhagen School (Buzan, Wæver, & de Wilde, 1998) untuk menganalisis bagaimana isu siber dikonstruksi sebagai ancaman eksistensial dalam diskursus politik dan kebijakan keamanan.

Pengumpulan data dilakukan melalui studi literatur sistematis (*systematic literature review*) terhadap dokumen kebijakan, laporan lembaga internasional (World Economic Forum, Europol, United Nations, BSSN, CISSReC), publikasi akademik peer-reviewed, serta laporan kasus kejahatan siber global dan nasional. Analisis data bersifat deskriptif-analitis dengan teknik triangulasi sumber untuk meningkatkan validitas argumentasi. Studi kasus dipilih secara purposif, mencakup serangan Stuxnet, WannaCry, NotPetya, serangan terhadap infrastruktur Ukraina, serta kasus-kasus di Indonesia (ransomware PDNS, hoaks politik, dan eksploitasi data biometrik Worldcoin). Pendekatan ini memungkinkan integrasi perspektif kriminologi digital, teori hubungan internasional, dan konsep keamanan siber kontemporer dalam satu kerangka analisis yang koheren.

KERANGKA ANALISIS DAN TIPOLOGI KEJAHATAN SIBER

Kajian mengenai kejahatan siber dan ancaman transnasional menuntut pendekatan interdisipliner yang menggabungkan kriminologi digital, teori hubungan internasional, dan konsep keamanan siber kontemporer. Kriminologi digital berusaha memahami bagaimana teknologi informasi menciptakan bentuk-bentuk kejahatan baru. Dion (2014) menekankan kejahatan siber ke dalam tiga kategori utama yang memandang keterlibatan teknologi dalam aktivitas kriminal, yaitu peran komputer sebagai instrumen, target, atau faktor insidentil dalam kejahatan. Secara lebih lanjut, Wall (2024) mengidentifikasi empat tipe kejahatan siber yang lebih spesifik:

1. *Cybertrespass*: akses ilegal ke sistem komputer, termasuk *hacking* dan intrusi jaringan. Studi kasus: peretasan sistem Yahoo (2013–2014) yang mengakibatkan kebocoran data 3 miliar akun.

2. *Cybertheft/Cyberdeception*: pencurian dan penipuan digital, termasuk pencurian identitas, penipuan kartu kredit, dan manipulasi pasar. Studi kasus: kasus pump and dump di pasar saham digital.

3. *Cyberobscenity/Cyberpornography*: distribusi konten ilegal, termasuk pornografi anak dan konten ekstrem. Studi kasus: jaringan internasional yang menggunakan dark web untuk menyebarkan konten pornografi anak.

4. *Cyberviolence*: kekerasan berbasis siber, termasuk cyberbullying, ancaman teror digital, dan ujaran kebencian. Studi kasus: kasus bunuh diri remaja akibat cyberbullying di media sosial.

> *"Cybercrime is not simply traditional crime committed with new tools; it is a transformation of the nature of crime itself in the information age." (Wall, 2024)*

Perspektif budaya yang ditawarkan Taylor (1999) menunjukkan bahwa hacking awalnya muncul sebagai subkultur teknologi yang didorong oleh rasa ingin tahu, sebelum bergeser menjadi aktivitas kriminal ketika dimanfaatkan untuk keuntungan finansial atau politik. Tipologi Wall dan Dion dapat dipahami sebagai dimensi struktural, sementara perspektif Taylor menambahkan dimensi kultural yang menjelaskan motivasi pelaku.

Konsep keamanan siber kontemporer memperkuat analisis ini dengan menekankan keterbatasan deterrence klasik dalam dunia digital. Nye (2017) berargumen bahwa sulitnya atribusi serangan membuat ancaman balasan tidak efektif, sehingga ia memperkenalkan konsep dissuasion, yaitu mengurangi motivasi aktor melakukan serangan yang dapat dicapai melalui diplomasi, norma, dan kerja sama multilateral.

> *"In cyberspace, the difficulty of attribution and the low cost of attack make classical deterrence problematic; what is needed is a broader strategy of dissuasion." (Nye, 2017, p. 55)*

Singer dan Friedman (2014) menambahkan bahwa keamanan siber harus dipahami sebagai isu multidimensional yang mencakup aspek teknis, sosial, politik, dan ekonomi. Dalam kerangka hubungan internasional, teori realisme melihat cyberwarfare sebagai instrumen kekuasaan negara, di mana serangan siber digunakan untuk melemahkan lawan tanpa harus melibatkan kekuatan militer konvensional. Teori liberalisme menekankan pentingnya kerja sama internasional, seperti Budapest Convention on Cybercrime dan UN Open-Ended Working Group on ICT Security. Sementara itu, teori konstruktivisme menyoroti pembentukan norma global tentang perilaku negara di ruang siber, misalnya melalui Tallinn Manual dan Paris Call for Trust and Security in Cyberspace.

> *"Much of what is called cyberwar is better understood as cyber espionage or sabotage; the term 'war' is often overused and under-defined." (Rid, 2013)*

Kerangka tipologi klasik tidak lagi cukup untuk menjelaskan kompleksitas kejahatan siber saat ini. Inovasi teknologi melahirkan bentuk-bentuk baru yang menuntut klasifikasi kontemporer, seperti steganografi digital (Kipper, 2004; Warren & Streeter, 2005) dan AI-driven cybercrime yang memanfaatkan kecerdasan buatan untuk menghasilkan deepfake, mengotomatisasi serangan phishing, atau memanipulasi opini publik. Kehadiran tipologi kontemporer ini memperlihatkan bahwa kejahatan

siber bersifat dinamis dan terus berkembang, sehingga kerangka teoritis harus adaptif dan terbuka terhadap kategori baru.

SEJARAH DAN EVOLUSI KEJAHATAN SIBER

Sejarah kejahatan siber tidak dimulai secara tiba-tiba dengan fenomena phone phreaking pada 1960–1970, melainkan memiliki akar yang lebih panjang. Para akademisi menelusuri jejak kejahatan siber hingga era pradigital, ketika manipulasi informasi dan kriptografi digunakan sebagai instrumen politik dan militer. Evolusi kejahatan siber dapat dibagi ke dalam beberapa fase historis.

1. Era Pra-Phone Phreaking: Kriptografi, Steganografi, dan Eksperimen Komputer Awal

Praktik manipulasi informasi sudah dikenal sejak ribuan tahun lalu. Julius Caesar menggunakan Caesar Cipher untuk komunikasi militer rahasia pada abad pertama SM, sementara Francis Bacon mengembangkan bilateral cipher pada abad ke-17 sebagai bentuk penyembunyian pesan (Pareek, 2020). Steganografi berbeda dengan kriptografi karena ia bersifat "menyembunyikan" keberadaan isi pesan, bukan "menyamarkan" isi pesan (Kipper, 2004). Dalam konteks kejahatan siber modern, steganografi digunakan untuk menyembunyikan data, malware, atau pesan rahasia dalam file digital agar lolos dari deteksi sistem keamanan (Warren & Streeter, 2005). Memasuki abad ke-20, komputer digunakan dalam kriptografi militer. Mesin Enigma Jerman pada Perang Dunia II dan upaya pemecahannya oleh Alan Turing di Bletchley Park menjadi contoh bagaimana teknologi digital awal digunakan dalam konteks konflik global (Chadd, 2020). Catatan akademik menyebutkan bahwa istilah "*malicious hacking*" pertama kali muncul pada 1963, ketika sistem komputer universitas mulai dieksploitasi oleh mahasiswa untuk mengakses data tanpa izin (Savag, 2009).

2. Era Phone Phreaking (1960–1970)

Fenomena phone phreaking menjadi fase populer pertama dari kejahatan siber modern. Para peretas memanipulasi sistem telekomunikasi untuk melakukan panggilan gratis dengan menggunakan perangkat sederhana seperti blue box. Aktivitas ini awalnya dilakukan sebagai bentuk eksplorasi teknologi dan hiburan, tetapi kemudian berkembang menjadi aktivitas kriminal ketika dimanfaatkan untuk keuntungan finansial (Taylor, 1999). Fenomena ini menunjukkan bahwa motivasi awal peretasan sering kali bersifat non-ekonomi, namun dapat bergeser seiring dengan peluang keuntungan.

3. Era Komputer Pribadi dan Hacking (1980–1990)

Memasuki era komputer pribadi, aktivitas hacking mulai berkembang. Pada 1980-an, kelompok peretas seperti Legion of Doom dan Masters of Deception muncul di Amerika Serikat, memanfaatkan jaringan komputer untuk mengeksplorasi sistem baru. Aktivitas ini kemudian dikriminalisasi karena dianggap mengganggu keamanan sistem komputer. Pada periode ini, hacking masih dipandang sebagai subkultur teknologi, dengan etos kerja yang menekankan kebebasan akses dan eksplorasi (Taylor, 1999). Namun, seiring meningkatnya penggunaan komputer dalam bisnis dan pemerintahan, aktivitas hacking mulai dipandang sebagai ancaman serius.

4. Era Internet dan Globalisasi Kejahatan Siber (1990–2000)

Dengan munculnya internet pada 1990-an, kejahatan siber memasuki fase baru. Internet memungkinkan interaksi lintas negara tanpa batas geografis, sehingga kejahatan siber menjadi fenomena transnasional. Warren & Streeter (2005) mencatat bahwa sindikat kriminal terorganisasi mulai memanfaatkan teknologi digital untuk keuntungan finansial ilegal, termasuk pencurian data kartu kredit dan penipuan online. Pada periode ini, kejahatan siber mulai dikaitkan dengan sindikat kriminal global, bukan hanya individu peretas.

5. Era Malware dan Serangan Massal (2000–2010)

Awal 2000-an ditandai dengan munculnya malware dan serangan massal. Virus komputer seperti ILOVEYOU (2000) dan Mydoom (2004) menyebar dengan cepat melalui email, menyebabkan kerugian miliaran dolar. Serangan Distributed Denial of Service (DDoS) juga mulai digunakan untuk melumpuhkan situs web dan layanan online. Pada periode ini, kejahatan siber mulai berdampak langsung pada ekonomi global, dengan perusahaan dan pemerintah harus mengeluarkan biaya besar untuk pemulihan sistem (Wall, 2024).

6. Era Ransomware dan Serangan terhadap Infrastruktur (2010–2020)

Dekade 2010-an ditandai dengan munculnya ransomware, yaitu malware yang mengenkripsi data korban dan meminta tebusan untuk membukanya. Kasus WannaCry (2017) dan NotPetya (2017) menjadi titik balik yang menunjukkan bahwa serangan siber dapat melumpuhkan sistem kesehatan, transportasi, dan energi di berbagai negara. Serangan ini tidak hanya berdampak pada individu atau perusahaan, tetapi juga pada infrastruktur vital negara. Hal ini menunjukkan bahwa kejahatan siber telah berkembang menjadi ancaman sistemik yang dapat mengguncang stabilitas nasional dan internasional (Singer & Friedman, 2014).

7. Era Cyberwarfare dan Geopolitik Digital (2020–sekarang)

Sejak 2020, kejahatan siber semakin terkait dengan geopolitik. Serangan Rusia terhadap Ukraina pada 2022 menunjukkan bagaimana serangan siber digunakan sebagai bagian dari strategi militer. Dugaan intervensi digital dalam pemilu AS (2016) dan rivalitas siber antara AS dan Tiongkok menunjukkan bahwa ruang siber telah menjadi arena baru bagi konflik geopolitik (Nye, 2017). Pada periode ini, istilah cyberwarfare semakin populer, meskipun Rid (2013) berargumen bahwa banyak serangan siber lebih mirip dengan spionase atau sabotase daripada perang konvensional. Selain itu, perkembangan teknologi kecerdasan buatan (AI) dan deepfake menambah dimensi baru dalam kejahatan siber. Teknologi ini digunakan untuk membuat konten palsu yang dapat memengaruhi opini publik dan merusak legitimasi politik.

CYBERWARFARE SEBAGAI ANCAMAN GLOBAL

Cyberwarfare muncul sebagai dimensi baru dalam lanskap ancaman global, berbeda dari kejahatan siber konvensional yang biasanya bermotif finansial. Dalam *cyberwarfare*, aktor negara atau kelompok yang didukung negara menggunakan serangan digital untuk tujuan geopolitik, militer, dan strategis. Karakteristik utamanya adalah keterlibatan negara, tujuan strategis yang jelas, kesulitan atribusi pelaku, serta dampak sistemik yang dapat melumpuhkan infrastruktur vital. Nye (2017) menekankan bahwa

strategi deterrence klasik sulit diterapkan karena identitas pelaku sering kali disamarkan, sehingga ia mengusulkan pendekatan *dissuasion* dan pembangunan norma internasional sebagai alternatif.

Serangkaian kasus empiris menunjukkan bahwa *cyberwarfare* telah menjadi instrumen geopolitik yang semakin penting. Berbeda dengan perang konvensional, operasi siber memungkinkan negara mencapai tujuan strategis dengan risiko eskalasi fisik yang lebih rendah, atribusi yang sulit, dan biaya relatif lebih murah. Tabel berikut merangkum tiga kasus utama yang sering dijadikan rujukan dalam literatur keamanan siber:

Tabel Keamanan Siber, diolah dari berbagai sumber.

No	Kasus	Tahun	Aktor yang Diduga	Target Utama	Tujuan Strategis	Dampak Utama	Sumber
1	**Stuxnet**	2010	AS & Israel (dugaan)	Fasilitas nuklir Natanz, Iran	Menghambat program pengayaan uranium Iran tanpa serangan militer terbuka	Kerusakan fisik pada sentrifugal; menunda program nuklir Iran; menjadi preseden *malware* sebagai senjata strategis	Singer & Friedman (2014); Rid (2013)
2	**Serangan terhadap jaringan listrik Ukraina + integrasi dalam invasi**	2015–2016 & 2022	Rusia	Jaringan listrik dan infrastruktur digital Ukraina	Melemahkan kapasitas negara, menciptakan chaos, mendukung operasi militer konvensional	Pemadaman listrik massal; gangguan layanan publik; integrasi operasi siber dengan perang kinetic	Nye (2017); Wall (2024)

3	**Intervensi pemilu AS & rivalitas siber AS–Tiongkok**	2016 (pemilu) & berkelanjutan	Rusia (pemilu); Tiongkok & AS (spionase)	Sistem pemilu, opini publik, kekayaan intelektual	Memengaruhi legitimasi politik; pencurian IP; keunggulan ekonomi-teknologi	Polarisasi politik; erosi kepercayaan publik; ketegangan perdagangan dan teknologi	Singer & Friedman (2014); Wall (2024)

Kasus **Stuxnet** (2010) menjadi titik balik penting karena pertama kali menunjukkan bahwa *malware* dapat menimbulkan kerusakan fisik pada infrastruktur industri kritis (*cyber-physical systems*). Operasi ini membuktikan bahwa ruang siber dapat digunakan untuk mencapai tujuan militer strategis tanpa harus melakukan serangan kinetik yang berisiko memicu perang terbuka. Stuxnet juga memperlihatkan dilema atribusi: meskipun banyak bukti menunjuk ke AS dan Israel, kedua negara tidak pernah secara resmi mengakuinya, sehingga mempersulit penerapan mekanisme *deterrence* klasik.

Kasus **Rusia terhadap Ukraina** menunjukkan evolusi lebih lanjut. Serangan terhadap jaringan listrik pada 2015–2016 masih bersifat terbatas, tetapi pada invasi 2022 operasi siber diintegrasikan secara sistematis dengan manuver militer darat, laut, dan udara. Ini menandai pergeseran dari *cyber operations* yang berdiri sendiri menjadi bagian dari *multi-domain warfare*. Selain itu, dugaan intervensi Rusia dalam pemilu AS 2016 memperlihatkan bahwa *cyberwarfare* tidak hanya menargetkan infrastruktur fisik, tetapi juga *cognitive domain*, yaitu persepsi, opini publik, dan legitimasi demokratis.

Sementara itu, rivalitas **AS–Tiongkok** menambahkan dimensi ekonomi dan teknologi. Spionase digital dan pencurian kekayaan intelektual menjadi isu sentral, di mana ruang siber digunakan untuk mempercepat keunggulan kompetitif dalam industri strategis (semikonduktor, AI, 5G, dan seterusnya). Dimensi ini memperlihatkan bahwa *cyberwarfare* tidak selalu berujung pada kerusakan fisik, melainkan dapat berbentuk *economic statecraft* melalui ruang digital.

Perspektif Hubungan Internasional

Dalam kerangka hubungan internasional, fenomena di atas dapat dianalisis melalui tiga lensa teoritis utama:

1. **Realisme** memandang *cyberwarfare* sebagai kelanjutan logis dari kompetisi kekuasaan antarnegara (*struggle for power*). Serangan siber dilihat sebagai instrumen *power* yang relatif murah dan dapat digunakan untuk mengubah *balance of power* tanpa harus menanggung biaya perang konvensional yang tinggi. Kasus Stuxnet dan serangan Rusia terhadap Ukraina sejalan dengan logika realis: negara akan memanfaatkan segala sarana yang tersedia, termasuk ruang

siber, untuk mempertahankan atau memperbesar kepentingan nasionalnya. Kesulitan atribusi justru memperkuat daya tarik instrumen ini karena mengurangi risiko pembalasan langsung.

2. **Liberalisme** menekankan pentingnya institusi, rezim internasional, dan kerja sama untuk mengelola ancaman bersama. Dalam konteks siber, liberalisme menyoroti upaya pembentukan norma dan kerangka hukum seperti *Budapest Convention on Cybercrime* (2001), *UN Open-Ended Working Group on ICT Security*, serta berbagai inisiatif *confidence-building measures*. Namun, efektivitas pendekatan liberal masih terbatas karena partisipasi negara tidak universal (beberapa negara besar belum meratifikasi Budapest Convention) dan perbedaan kepentingan geopolitik menghambat konsensus tentang norma perilaku di ruang siber.
3. **Konstruktivisme** berfokus pada pembentukan identitas, norma, dan makna sosial. *Tallinn Manual* dan *Paris Call for Trust and Security in Cyberspace* merupakan contoh upaya untuk mengonstruksi norma global tentang apa yang dianggap "perilaku bertanggung jawab" negara di ruang siber. Dari perspektif ini, ancaman siber tidak hanya bersifat material, tetapi juga bersifat ideasional: bagaimana suatu tindakan didefinisikan sebagai "serangan", "spionase", atau "sabotase" sangat bergantung pada intersubjektivitas dan wacana yang berkembang di antara aktor internasional. Rid (2013), misalnya, mengkritik penggunaan istilah "cyberwar" yang berlebihan karena banyak operasi siber lebih tepat dikategorikan sebagai spionase atau sabotase.

Dampak Multidimensional

Dampak *cyberwarfare* meluas ke empat ranah utama:

- **Ekonomi**: kerugian finansial langsung (pemulihan sistem, tebusan *ransomware*), hilangnya produktivitas, dan kerusakan reputasi perusahaan maupun negara.
- **Politik**: erosi legitimasi demokrasi melalui disinformasi, *deepfake*, dan manipulasi opini publik; polarisasi sosial-politik.
- **Sosial**: penurunan kepercayaan publik terhadap institusi digital dan layanan publik berbasis teknologi.
- **Militer**: integrasi operasi siber ke dalam doktrin perang modern (*multi-domain operations*), sehingga ruang siber menjadi domain perang keempat setelah darat, laut, dan udara.

Dengan karakteristik tersebut, *cyberwarfare* dapat diposisikan sejajar dengan ancaman global lain seperti pandemi dan perubahan iklim: bersifat transnasional, sistemik, sulit diatribusikan secara cepat, dan menuntut respons kolektif yang melampaui kapasitas satu negara. Perbedaannya terletak pada kecepatan eskalasi dan ketergantungan yang semakin tinggi terhadap infrastruktur digital, sehingga kerentanan yang ditimbulkan bersifat instan dan meluas.

PERANG SIBER DALAM KONTEKS GLOBAL DAN NASIONAL

Dalam konteks global, kejahatan siber telah berkembang menjadi salah satu ancaman transnasional paling signifikan pada dekade terakhir.

Lanskap Global: Dari Risiko Teknis Menjadi Ancaman Eksistensial

Pembahasan mengenai lanskap global kejahatan siber tidak dapat lagi dimulai dari pertanyaan "berapa banyak serangan yang terjadi", melainkan dari pertanyaan yang lebih mendasar: bagaimana suatu fenomena teknis berhasil dikonstruksi menjadi ancaman eksistensial yang menempati posisi setara dengan perubahan iklim dan krisis geopolitik? Pertanyaan ini menuntut analisis yang menggabungkan data empiris, kerangka teoritis, dan lensa kriminologi digital.

Secara metodologis, bagian ini bertumpu pada pendekatan *risk governance framework* yang memandang kejahatan siber sebagai risiko sistemik, serta *securitization theory* (Buzan, Wæver, & de Wilde, 1998) yang menjelaskan proses politik di mana suatu isu diangkat dari ranah teknis biasa menjadi ancaman yang memerlukan tindakan luar biasa. Data yang digunakan bersumber dari laporan lembaga internasional (World Economic Forum, Europol, Cybersecurity Ventures) yang kemudian dianalisis secara kritis melalui perspektif kriminologi.

A. Pergeseran Posisi Ancaman dalam Tata Risiko Global

Laporan *Global Cybersecurity Outlook 2025* menempatkan serangan siber di posisi tiga besar risiko global, sejajar dengan perubahan iklim dan ketegangan geopolitik (World Economic Forum, 2025). Posisi ini bukan semata hasil perhitungan teknis, melainkan hasil dari proses *securitization* yang berlangsung selama lebih dari satu dekade. Jika pada awal 2000-an kejahatan siber masih dipandang sebagai masalah penegakan hukum pidana atau keamanan informasi perusahaan, maka sejak pertengahan 2010-an isu ini semakin sering dibingkai sebagai ancaman terhadap kelangsungan hidup negara dan masyarakat. Estimasi kerugian ekonomi global akibat kejahatan siber yang mencapai USD 10,5 triliun per tahun (Cybersecurity Ventures, 2025), dan kerugian khusus *ransomware* yang diperkirakan lebih dari USD 265 miliar per tahun, memberikan legitimasi kuantitatif bagi pembingkaian tersebut. Namun, dari sudut pandang kriminologi, angka-angka ini hanya merupakan permukaan. Yang lebih penting adalah **transformasi sifat kejahatan** itu sendiri. Wall (2024) menegaskan dengan tajam:

> *"Cybercrime is not simply traditional crime committed with new tools; it is a transformation of the nature of crime itself in the information age."*

Kutipan ini menjadi sendi analitis penting. Ia menolak pandangan yang melihat kejahatan siber sekadar sebagai "kejahatan lama dengan alat baru". Sebaliknya, ruang siber menciptakan *opportunity structure* baru, bentuk victimisasi baru, dan bahkan kategori pelaku baru yang tidak sepenuhnya dapat ditangkap oleh kategori kriminologi konvensional (seperti *white-collar crime* atau *organized crime* klasik).

B. Eskalasi Kasus sebagai Bukti Pergeseran Karakter Ancaman

Untuk memperlihatkan eskalasi tersebut secara lebih sistematis, tabel berikut menyajikan sejumlah kasus monumental yang menjadi titik balik dalam pemahaman global terhadap kejahatan siber:

Tabel Kejahatan Siber, diolah dari berbagai sumber.

Tahun	**Kasus**	**Karakter Serangan**	**Target Utama**	**Dampak Sistemik**	**Implikasi Kriminologis**	**Sumber**
2017	WannaCry	Ransomware yang menyebar massal via EternalBlue	Sistem kesehatan (NHS Inggris), perusahaan global	Penundaan operasi medis, kerugian miliar dolar	Cyberviolence terhadap layanan publik kritis; memperlihatkan kerentanan infrastruktur sipil	Singer & Friedman (2014); Rid (2013)
2021	Colonial Pipeline	Ransomware terhadap operator infrastruktur energi	Jaringan pipa bahan bakar AS	Kelangkaan BBM di Pantai Timur AS, kepanikan publik	Cybertheft + economic disruption; menunjukkan *ransomware* sebagai ancaman keamanan nasional	Wall (2024)
2015–2022	Serangan siber terhadap Ukraina	Operasi siber yang terintegrasi dengan perang kinetic	Jaringan listrik, sistem pemerintahan, komunikasi	Pemadaman listrik massal, chaos sosial, dukungan invasi militer	State-sponsored cyberviolence; mengaburkan batas antara *cybercrime* dan *cyberwarfare*	Nye (2017)
2024–2025	Deepfake & AI-driven attacks	Manipulasi konten + otomatisasi phishing	Opini publik, proses politik, individu berprofil tinggi	Erosi kepercayaan, polarisasi, potensi intervensi pemilu	Cyberdeception berbasis AI; memperluas *harm* ke ranah kognitif dan politik	Europol (2024)

Tabel di atas tidak hanya berfungsi sebagai ringkasan data, melainkan juga sebagai alat analisis. Dari kasus WannaCry hingga serangan berbasis AI, terlihat pola yang jelas: target bergeser dari sistem individu atau perusahaan tunggal menuju infrastruktur kritis dan *cognitive domain* masyarakat. Pergeseran ini memiliki dua implikasi kriminologis penting.

Pertama, victimisasi menjadi semakin kolektif dan tidak personal. Korban tidak lagi hanya individu yang kehilangan data atau uang, tetapi seluruh populasi yang bergantung pada layanan kesehatan, energi, atau informasi yang andal. Kedua, batas antara kejahatan kriminal dan operasi negara semakin kabur. Ketika serangan siber digunakan sebagai bagian dari strategi geopolitik, kategori *cybercrime* klasik menjadi tidak memadai. Di sinilah pentingnya membedakan *cybercrime* (bermotif kriminal/finansial) dengan *cyberwarfare* (bermotif strategis/negara), sebagaimana telah digariskan pada bagian kerangka analisis.

C. Dari Deterrence Klasik menuju Dissuasion

Salah satu dilema teoritis yang muncul dari lanskap global ini adalah kegagalan pendekatan *deterrence* klasik di ruang siber. Nye (2017) merumuskan masalahnya secara ringkas:

> *"In cyberspace, the difficulty of attribution and the low cost of attack make classical deterrence problematic; what is needed is a broader strategy of dissuasion."*

Kesulitan atribusi, siapa pelaku sebenarnya, membuat ancaman pembalasan menjadi kurang kredibel. Biaya melakukan serangan yang relatif rendah semakin memperlemah logika *deterrence*. Oleh karena itu, Nye menawarkan konsep *dissuasion*: mengurangi motivasi aktor untuk menyerang melalui kombinasi norma, diplomasi, biaya reputasi, dan arsitektur keamanan yang lebih tangguh. Dari perspektif kriminologi, argumen Nye sejalan dengan pergeseran dari model *punishment-centered* menuju model yang lebih menekankan pencegahan situasional, pengurangan kesempatan, dan pembangunan kapasitas sosial. Kejahatan siber, seperti kejahatan lainnya, berkembang dalam konteks kesempatan yang memungkinkan (*opportunity*) dan kontrol yang lemah (*weak guardianship*). Memperkuat *capable guardianship* di ruang digital, baik melalui regulasi, teknologi, maupun literasi, menjadi salah satu kunci *dissuasion*.

D. Catatan Metodologis dan Implikasi Analitis

Secara metodologis, analisis lanskap global ini mengandalkan data sekunder yang bersifat agregat. Keterbatasan yang perlu diakui adalah kemungkinan *under-reporting* dan perbedaan standar pengukuran antarnegara. Namun, konsistensi temuan dari berbagai lembaga (WEF, Europol, Cybersecurity Ventures) memberikan keyakinan yang memadai bahwa pergeseran dari "risiko teknis" menjadi "ancaman eksistensial" merupakan fenomena nyata, bukan sekadar konstruksi wacana. Implikasi analitisnya jelas: kejahatan siber global tidak dapat lagi dipahami hanya sebagai masalah penegakan hukum atau keamanan jaringan. Ia telah menjadi bagian dari tata risiko global yang menuntut respons multi-level, dari penguatan kapasitas teknis hingga pembentukan norma

internasional. Bagian-bagian selanjutnya akan memperlihatkan bagaimana dimensi sosial-politik dan konteks nasional (Indonesia) memperumit serta memperkaya pemahaman ini.

Dimensi Sosial-Politik: Kejahatan Siber sebagai Ancaman terhadap Kohesi dan Legitimasi

Jika lanskap global memperlihatkan bagaimana kejahatan siber bergeser dari risiko teknis menjadi ancaman eksistensial di tingkat sistem global, maka Bagian 2 berfokus pada lapisan yang lebih subtil namun tidak kalah merusak: dimensi sosial dan politik. Di sini, ancaman tidak selalu berwujud kerusakan infrastruktur fisik atau kerugian finansial yang dapat dihitung, melainkan berupa erosi kepercayaan, polarisasi sosial, dan pelemahan legitimasi institusi demokratis. Secara metodologis, analisis pada bagian ini menggabungkan perspektif kriminologi digital (khususnya konsep *social harm* dan *political harm*) dengan teori *securitization* serta kajian tentang disinformasi sebagai bentuk kekerasan simbolik.

a) Dari Kerusakan Material menuju Social dan Political Harm

Kriminologi konvensional cenderung mengukur kejahatan melalui kerugian material atau pelanggaran hukum pidana yang jelas. Namun, di ruang siber, bentuk kerugian yang paling dalam sering kali bersifat non-material. Wall (2024) mengingatkan bahwa transformasi kejahatan di era informasi tidak hanya mengubah modus operandi, tetapi juga mengubah karakter *harm* yang ditimbulkan. Dalam konteks ini, *cyberviolence* dan *cyberdeception* tidak selalu berujung pada kerugian uang atau kerusakan sistem, melainkan pada kerusakan hubungan sosial dan legitimasi politik.

Rid (2013) memberikan peringatan penting yang sering diabaikan dalam wacana "perang siber":

> *"Much of what is called cyberwar is better understood as cyber espionage or sabotage; the term 'war' is often overused and under-defined."*

Kutipan ini relevan karena banyak operasi yang dikategorikan sebagai "serangan siber" justru lebih tepat dipahami sebagai upaya memengaruhi persepsi, menanamkan keraguan, dan merusak kohesi sosial. Ketika deepfake digunakan untuk membuat seolah-olah seorang pemimpin politik menyatakan sesuatu yang tidak pernah ia ucapkan, atau ketika jaringan bot menyebarkan narasi palsu secara masif menjelang pemilu, yang diserang bukanlah server, melainkan kepercayaan publik itu sendiri.

b) Disinformasi dan Manipulasi Opini sebagai Bentuk Cyberviolence

Penyebaran misinformasi dan disinformasi melalui media sosial telah terbukti memengaruhi proses demokrasi di berbagai negara. Kasus intervensi dalam pemilu Amerika Serikat (2016), polarisasi di Brasil, serta kampanye disinformasi di India menunjukkan pola yang berulang: ruang digital dimanfaatkan untuk memperdalam retakan sosial yang sudah ada, bukan semata-mata untuk "mengubah hasil suara" secara langsung. Dari sudut pandang kriminologi, fenomena ini dapat dibaca sebagai bentuk *cyberviolence* yang menargetkan kohesi sosial. Berbeda dengan kekerasan fisik, kekerasan di sini bersifat simbolik dan kognitif. Ia bekerja dengan cara merusak kemampuan

masyarakat untuk membedakan fakta dari fiksi, serta melemahkan institusi yang seharusnya menjadi rujukan kebenaran bersama (media, lembaga penyelenggara pemilu, lembaga ilmiah).

Tabel berikut merangkum beberapa dimensi *harm* sosial-politik yang dihasilkan oleh kejahatan siber:

Tabel Social Political Harm, diolah Wall (2024).

Dimensi Harm	**Bentuk Konkret**	**Mekanisme**	**Dampak Jangka Menengah–Panjang**	**Contoh Empiris**
Kognitif	Deepfake, narasi palsu, manipulasi algoritma	Merusak kemampuan memverifikasi informasi	Erosi kepercayaan terhadap fakta bersama	Kampanye deepfake menjelang pemilu
Sosial	Ujaran kebencian terorganisir, polarisasi algoritmik	Memperdalam fragmentasi identitas	Melemahnya kohesi sosial, meningkatnya intoleransi	Echo chamber dan filter bubble
Politik	Intervensi pemilu, propaganda negara, hoaks sistematis	Menyerang legitimasi proses dan hasil demokrasi	Krisis kepercayaan terhadap institusi	Dugaan intervensi Rusia 2016; hoaks politik di berbagai negara
Institusional	Serangan terhadap sistem penyelenggara pemilu atau lembaga publik	Mengganggu kapasitas negara menjalankan fungsi dasar	Pelemahan kapasitas tata kelola	Serangan terhadap sistem data pemilu atau layanan publik

Tabel di atas menunjukkan bahwa *harm* yang dihasilkan bersifat berlapis. Serangan terhadap satu dimensi (misalnya kognitif) dapat merembet ke dimensi lain (sosial dan politik). Inilah yang membuat kejahatan siber dalam ranah sosial-politik sulit ditangani hanya dengan pendekatan hukum pidana atau teknis semata.

c) Krisis Kepercayaan sebagai Produk Struktural

Penurunan kepercayaan publik terhadap sistem digital dan institusi demokrasi bukanlah akibat sampingan yang tidak disengaja, melainkan sering kali merupakan **tujuan** dari operasi itu sendiri. Ketika masyarakat tidak lagi percaya pada hasil pemilu, pada pemberitaan media, atau pada pernyataan pejabat publik, maka kapasitas kolektif untuk mengambil keputusan bersama ikut

melemah. Dalam bahasa kriminologi, ini merupakan bentuk *undermining of social order* yang lebih dalam daripada sekadar pelanggaran hukum.

Nye (2017) kembali relevan di titik ini. Ketika ia berbicara tentang *dissuasion*, yang dimaksud bukan hanya mencegah serangan teknis, tetapi juga membangun ketahanan sosial sehingga operasi pengaruh (*influence operations*) menjadi kurang efektif. Ketahanan sosial ini mencakup literasi digital, kapasitas verifikasi informasi, dan kepercayaan yang sehat terhadap institusi—bukan kepercayaan buta, melainkan kepercayaan yang grounded pada transparansi dan akuntabilitas.

d) Keterbatasan Norma Internasional dan Dilema Kolektif

Organisasi internasional seperti PBB dan Uni Eropa telah berupaya membangun norma global untuk mengatur perilaku negara di ruang siber (United Nations, 2024). Namun, konsensus tetap sulit dicapai. Perbedaan kepentingan geopolitik, terutama di antara negara-negara besar, membuat kesepakatan tentang apa yang termasuk "perilaku bertanggung jawab" di ruang siber menjadi arena tawar-menawar politik.

Dari perspektif kriminologi kritis, keterbatasan ini dapat dibaca sebagai cerminan dari ketimpangan kekuasaan dalam tata kelola global. Negara-negara yang memiliki kapasitas ofensif siber yang kuat cenderung enggan terikat oleh norma yang membatasi ruang manuver mereka, sementara negara-negara dengan kapasitas lebih lemah lebih membutuhkan perlindungan norma tersebut. Akibatnya, ruang siber tetap menjadi arena di mana logika kekuasaan seringkali lebih dominan daripada logika hukum atau etika.

Secara metodologis, analisis dimensi sosial-politik ini menghadapi tantangan pengukuran. Berbeda dengan kerugian finansial yang relatif lebih mudah dihitung, *social harm* dan *political harm* bersifat kualitatif dan seringkali baru terlihat dalam jangka menengah hingga panjang. Oleh karena itu, pendekatan yang digunakan bersifat interpretatif dan bertumpu pada studi kasus serta laporan lembaga yang kredibel.

Bagian ini memperlihatkan bahwa kejahatan siber tidak hanya "menyerang sistem", tetapi juga "menyerang masyarakat dan politik". Ancaman terhadap kohesi dan legitimasi inilah yang membuatnya setara, meski berbeda bentuk, dengan ancaman global lain. Bagian berikutnya akan membawa analisis ini ke konteks yang lebih spesifik: Indonesia sebagai negara dengan populasi digital besar yang menampilkan kerentanan struktural khas. Selain aspek teknis, dimensi sosial dan politik juga semakin penting. Penyebaran misinformasi dan disinformasi melalui media sosial telah memengaruhi proses demokrasi di berbagai negara, termasuk pemilu di Amerika Serikat, Brasil, dan India. Organisasi internasional seperti PBB dan Uni Eropa berusaha membangun norma global untuk mengatur perilaku negara di ruang siber, namun konsensus masih sulit dicapai karena perbedaan kepentingan geopolitik (United Nations, 2024).

Indonesia, sebagai negara dengan populasi digital yang sangat besar juga menghadapi tantangan serius dalam bidang keamanan siber. Laporan Badan Siber dan Sandi Negara (BSSN) mencatat bahwa

sepanjang tahun 2023–2024 terjadi lebih dari 200 juta anomali trafik siber, dengan tren serangan yang semakin kompleks dan melibatkan aktor transnasional. Pada 2025, Indonesia bahkan tercatat sebagai salah satu sumber serangan DDoS tertinggi di dunia menurut CISSReC, menunjukkan bahwa ruang siber Indonesia tidak hanya menjadi target, tetapi juga sumber aktivitas berbahaya.

Rangkuman tren kasus kejahatan siber di Indonesia tahun 2023–2025 mencakup: (1) Tahun 2023 – lebih dari 200 juta anomali trafik siber (BSSN) dengan tipologi cybertrespass dan cyberviolence; (2) Tahun 2024 – serangan ransomware pada rumah sakit dan lembaga pendidikan yang melumpuhkan layanan vital; (3) Januari 2025 – video hoaks bantuan dana Presiden Prabowo Subianto sebagai contoh *cyberdeception* untuk tujuan politik; (4) Mei 2025 – fenomena Worldcoin/WorldID (pemindaian iris mata) yang menimbulkan risiko privasi dan eksploitasi data biometrik; (5) Tahun 2025 – Indonesia tercatat sebagai salah satu sumber serangan DDoS tertinggi (CISSReC, 2025).

Tabel dan data tersebut menunjukkan bahwa kejahatan siber di Indonesia bersifat multidimensi karena melibatkan aspek teknis (DDoS, ransomware), sosial (hoaks, ujaran kebencian), politik (manipulasi pemilu, propaganda digital), dan ekonomi (eksploitasi data biometrik). Kerentanan ini diperparah oleh rendahnya literasi digital masyarakat dan lemahnya regulasi yang adaptif terhadap perkembangan teknologi. Indonesia menghadapi dilema yang sering dijumpai pada negara berkembang, yaitu kebutuhan digitalisasi untuk pembangunan ekonomi berhadapan dengan kerentanan keamanan yang tinggi. Posisi Indonesia dalam diplomasi siber global masih terbatas, meskipun partisipasi dalam forum ASEAN dan PBB mulai menunjukkan komitmen. Strategi kebijakan yang lebih konkret diperlukan, seperti integrasi literasi digital ke dalam kurikulum pendidikan, penguatan regulasi adaptif, serta kerja sama regional untuk menghadapi ancaman transnasional.

KESIMPULAN

Kajian ini menegaskan bahwa kejahatan siber merupakan fenomena multidimensional yang tidak dapat dipahami hanya dari sudut pandang teknis. Integrasi antara teori kriminologi digital, tipologi kejahatan siber, konsep keamanan siber kontemporer, serta perspektif hubungan internasional memperlihatkan bahwa ancaman ini memiliki implikasi yang luas: dari individu hingga negara, dari ranah sosial hingga geopolitik global. Tipologi klasik seperti *cybertrespass*, *cybertheft*, *cyberobscenity*, dan *cyberviolence* tetap relevan, namun harus diperkaya dengan tipologi kontemporer seperti steganografi digital dan kejahatan berbasis kecerdasan buatan. Hal ini menunjukkan bahwa kejahatan siber bersifat dinamis, terus berevolusi seiring perkembangan teknologi, dan menuntut kerangka teoritis yang adaptif.

Dalam konteks Indonesia, kejahatan siber memperlihatkan kerentanan yang khas: rendahnya literasi digital, lemahnya regulasi adaptif, serta tingginya eksposur masyarakat terhadap hoaks politik dan eksploitasi data biometrik. Kasus-kasus seperti serangan ransomware terhadap rumah sakit, video hoaks politik, dan fenomena Worldcoin memperlihatkan bahwa ancaman siber di Indonesia bukan sekadar isu teknis, melainkan tantangan struktural bagi demokrasi, ekonomi, dan keamanan nasional. Sementara itu, dalam konteks global, kejahatan siber telah diakui sebagai salah satu risiko terbesar dunia, sejajar dengan krisis iklim dan konflik geopolitik. Serangan terhadap infrastruktur vital di berbagai negara

menunjukkan bahwa ruang siber telah menjadi arena baru bagi persaingan kekuasaan, sekaligus medan perdebatan normatif tentang etika dan tanggung jawab negara. Kejahatan siber juga berinteraksi dengan ancaman global lain. Pandemi COVID-19 mempercepat digitalisasi, yang pada gilirannya meningkatkan kerentanan terhadap serangan siber. Krisis energi dapat diperburuk oleh serangan terhadap infrastruktur energi, sementara transformasi menuju teknologi hijau menciptakan ketergantungan baru pada sistem digital yang rentan. Dengan demikian, kejahatan siber tidak berdiri sendiri, melainkan saling terkait dengan lanskap risiko global.

Kejahatan siber akhirnya harus dipahami sebagai ancaman multidimensional yang menuntut pendekatan interdisipliner. Regulasi hukum, literasi digital, kerja sama internasional, dan pembangunan norma global merupakan pilar yang harus diperkuat secara simultan. Tanpa integrasi antara aspek teknis, sosial, politik, dan etika, penanggulangan kejahatan siber akan selalu tertinggal dari dinamika teknologi yang terus berkembang. Oleh karena itu, penelitian dan kebijakan di bidang ini harus diarahkan pada pembentukan ekosistem keamanan digital yang berkelanjutan, inklusif, dan adaptif, agar masyarakat global dapat menghadapi ancaman siber dengan ketahanan yang lebih kuat.

REFERENSI

Badan Siber dan Sandi Negara (BSSN). (2024). *Laporan tahunan keamanan siber Indonesia*. Jakarta: BSSN.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner.

Chadd, K. (2020). *The history of cybercrime and cybersecurity, 1940–2020*. Cybercrime Magazine.

CISSReC. (2025). *Laporan keamanan siber Indonesia 2025*. Lembaga Riset Keamanan Siber.

Clough, J. (2015). *Principles of cybercrime* (2nd ed.). Cambridge University Press.

Cybersecurity Ventures. (2025). *Cybercrime report.*

Dion, M. (2014). *Financial crimes and existential philosophy*. Springer.

Europol. (2024). *Internet organised crime threat assessment (IOCTA)*. The Hague: Europol.

Kipper, G. (2004). *Investigator's guide to steganography*. CRC Press.

Kshetri, N. (2013). Cybercrime and cybersecurity in the Global South. *Palgrave Macmillan*.

Nye, J. S. (2004). *Soft power: The means to success in world politics*. Public Affairs.

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71.

Pareek, A. (2020). Chronology of cyber crime: First phase of history of cyber crime before 1960s. Government Law College, Churu.

Rakhmayanti, I. (2024, Juni 27). Kronologi lengkap Pusat Data Nasional diserang hacker. *CNBC Indonesia*.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

Savag, S. (2009). Cybercrime: From pre-internet to the modern era. *ACM Digital Library*.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Taylor, P. A. (1999). *Hackers: Crime in the digital sublime*. Routledge.

United Nations. (2024). *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace*. New York: United Nations.

Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age* (2nd ed.). Polity Press.

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe.

Warren, P., & Streeter, M. (2005). *Cyber alert: How the world is under attack from a new form of crime*. Vision Paperbacks.

World Economic Forum. (2025a). *Global cybersecurity outlook 2025*. Geneva: World Economic Forum.

World Economic Forum. (2025b). *Global risks report 2025*. Geneva: World Economic Forum.