JIIC: JURNAL INTELEK INSAN CENDIKIA
https://jicnusantara.com/index.php/jiic
Vol : 2 No: 8, Agustus 2025
E-ISSN : 3047-7824

ANATOMI KRIMINAL SIBER: MOTIF, MODUS, DAN PENANGGULANGANNYA DARI PERSPEKTIF KRIMINOLOGI

ANATOMY OF CYBER CRIME: MOTIVES, MODES, AND COUNTERMEASURES FROM A CRIMINOLOGICAL PERSPECTIVE

Deva Wira Pramudya[1], Hudi Yusuf[2]
Fakultas Hukum Universitas Bung Karno
Email: wiradeva8@gmail.com[1], hoedydjoesoef@gmail.com[2]

Article Info

Article history :
Received : 04-08-2025
Revised : 05-08-2025
Accepted : 07-08-2025
Pulished : 10-08-2025

Abstract

Cybercrime is a modern form of crime that is rapidly evolving along with advances in information and communication technology. This crime has unique characteristics that distinguish it from conventional crime, such as its anonymous nature, its lack of boundaries, and the use of digital devices as its primary means. This research aims to examine the anatomy of cybercrime in depth through a criminological approach, focusing on identifying the perpetrators' motives, their modus operandi, and effective countermeasures strategies. The methodology used in this research is a qualitative approach using a desk study, reviewing various literature, regulations, and actual case reports related to cybercrime. The findings of this study indicate that the motives of cybercrime perpetrators vary widely, ranging from economic motives such as data theft and digital extortion, to ideological motives such as propaganda and disruption of state systems. The modus operandi used is also increasingly complex, utilizing phishing techniques, malware, social engineering, and exploiting weak security systems. Combating cybercrime requires a multidisciplinary and collaborative approach between the government, law enforcement agencies, the private sector, and the general public. Preventive strategies such as improving digital literacy and cybersecurity must go hand in hand with repressive strategies such as firm law enforcement and cross-border cooperation. Therefore, understanding the anatomy of cybercrime from a criminological perspective is crucial for formulating adaptive and responsive policies to the dynamics of digital crime.

Keywords: cybercrime, criminology, criminal motives

Abstrak

Kejahatan siber merupakan bentuk kriminalitas modern yang berkembang pesat seiring dengan kemajuan teknologi informasi dan komunikasi. Kejahatan ini memiliki karakteristik unik yang membedakannya dari kejahatan konvensional, seperti sifatnya yang anonim, tidak berbatas wilayah, serta menggunakan perangkat digital sebagai sarana utama. Penelitian ini bertujuan untuk mengkaji secara mendalam anatomi kriminal siber melalui pendekatan kriminologis, dengan fokus pada identifikasi motif pelaku, modus operandi yang digunakan, serta strategi penanggulangan yang efektif. Metodologi yang digunakan dalam penelitian ini adalah pendekatan kualitatif dengan metode studi pustaka, mengkaji berbagai literatur, regulasi, dan laporan kasus aktual yang berkaitan dengan tindak pidana siber. Temuan dalam penelitian ini menunjukkan bahwa motif pelaku kejahatan siber sangat bervariasi, mulai dari motif ekonomi seperti pencurian data dan pemerasan digital, hingga motif ideologis seperti propaganda dan gangguan terhadap sistem negara. Modus operandi yang digunakan pun semakin kompleks, memanfaatkan teknik phishing, malware, social engineering, dan eksploitasi sistem keamanan yang lemah. Penanggulangan kejahatan siber memerlukan pendekatan multidisipliner dan kolaboratif antara pemerintah, lembaga penegak hukum, sektor swasta, serta masyarakat umum. Strategi preventif seperti peningkatan literasi digital dan keamanan siber harus berjalan seiring dengan strategi represif berupa penegakan hukum yang tegas dan kerja sama lintas negara. Dengan

demikian, pemahaman terhadap anatomi kejahatan siber dari perspektif kriminologi menjadi penting dalam merumuskan kebijakan yang adaptif dan responsif terhadap dinamika kejahatan digital.

Kata kunci: Kejahatan Siber, Kriminologi, Motif Criminal

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah membawa perubahan besar dalam cara manusia hidup, bekerja, dan berinteraksi. Saat ini, hampir semua aktivitas manusia seperti berbelanja, belajar, bekerja, bahkan bertransaksi keuangan dapat dilakukan secara daring (online). Namun, di balik berbagai kemudahan tersebut, muncul pula ancaman baru yang tidak kalah serius, yaitu kejahatan siber (*cybercrime*) (Wall, 2007). Kejahatan siber merupakan tindakan kriminal yang dilakukan melalui internet atau perangkat digital, dengan tujuan merugikan orang lain, mencuri informasi, atau menghancurkan sistem tertentu. Jenis kejahatan ini berbeda dari kejahatan biasa karena pelakunya sering kali tidak terlihat, tidak dikenal, dan bisa berada di mana saja di dunia. Seorang pelaku di luar negeri dapat meretas sistem perbankan atau mencuri data seseorang yang berada di Indonesia hanya dengan koneksi internet (Yar, 2013).

Di Indonesia, kejahatan siber semakin sering terjadi. Kasus peretasan situs pemerintahan, penipuan online, pencurian data pribadi, dan penyebaran konten ilegal terus meningkat dari tahun ke tahun. Meski pemerintah telah menerbitkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagai dasar hukum penanganan kejahatan ini, implementasinya di lapangan masih menghadapi banyak kendala. Salah satu masalah utama adalah keterbatasan aparat penegak hukum dalam memahami teknologi digital, serta rendahnya literasi digital masyarakat. Kejahatan siber bukan hanya persoalan teknis, tetapi juga masalah sosial dan perilaku manusia. Dari sudut pandang kriminologi, penting untuk memahami siapa pelaku kejahatan ini, apa motif mereka, bagaimana cara mereka melakukannya, dan bagaimana kejahatan ini bisa dicegah atau ditangani. Motif kejahatan siber bisa bermacam-macam, mulai dari mencari uang, menunjukkan kemampuan teknis, melakukan aksi protes politik, hingga sekadar iseng.

Modus operandi atau cara yang digunakan pun sangat beragam, mulai dari penipuan email (*phishing*), pencurian identitas, penyebaran virus (*malware*), hingga serangan terhadap sistem jaringan (*hacking*) (Nur, 2023). Oleh karena itu, penelitian ini penting untuk dilakukan guna mengkaji secara lebih dalam *anatomi kriminal siber*, yaitu keseluruhan aspek yang menyusun dan menjelaskan kejahatan siber mulai dari latar belakang pelaku, motif, teknik atau modus yang digunakan, hingga solusi atau strategi penanggulangannya. Pendekatan yang digunakan dalam kajian ini adalah pendekatan kriminologis, yang melihat kejahatan tidak hanya sebagai pelanggaran hukum, tetapi juga sebagai fenomena sosial yang dipengaruhi oleh lingkungan, teknologi, dan motivasi pribadi. Dengan memahami secara menyeluruh bagaimana kejahatan siber bekerja, diharapkan hasil penelitian ini dapat menjadi acuan dalam upaya penanggulangan yang lebih efektif, baik melalui kebijakan hukum, peningkatan kapasitas aparat, maupun edukasi kepada masyarakat luas.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif, yang bertujuan untuk menggambarkan secara rinci dan mendalam mengenai fenomena kejahatan siber berdasarkan tiga aspek utama: motif pelaku**,** modus operandi**,** dan strategi penanggulangan, dengan menjadikan

perspektif kriminologi sebagai kerangka analisis. Pendekatan ini dipilih karena sifat kejahatan siber tidak hanya terbatas pada aspek teknologis semata, tetapi juga erat kaitannya dengan dinamika sosial**,** struktur budaya masyarakat digital**,** perilaku psikologis pelaku, serta interaksi antara pelaku dan korban dalam ruang siber.

Kejahatan siber merupakan bentuk kriminalitas yang sering kali tidak memiliki keterkaitan langsung antara pelaku dan korban secara fisik, sehingga pendekatan kualitatif dianggap relevan untuk mengkaji konteks sosial dan latar belakang individu atau kelompok pelaku. Dalam konteks ini, pendekatan deskriptif tidak hanya mengamati *apa yang terjadi*, tetapi juga mencoba memahami "mengapa" dan "bagaimana" suatu tindakan kriminal berbasis siber dapat terjadi, menyebar, dan berdampak luas (Moleong , 2012).

Selain itu, pendekatan ini memungkinkan peneliti untuk menyelami kompleksitas motif pelaku, yang bisa saja berasal dari dorongan ekonomi (profit-oriented), ideologi (politik atau agama), rasa frustrasi terhadap sistem, atau hanya untuk menunjukkan kemampuan teknis. Dengan memahami motif secara menyeluruh, analisis ini dapat memberikan gambaran yang lebih komprehensif dalam upaya membentuk strategi penanggulangan yang efektif dan tidak hanya bersifat represif, tetapi juga preventif.

Pendekatan ini juga memberikan ruang untuk mengeksplorasi konteks budaya digital, seperti bagaimana norma dan etika berinteraksi di dunia maya membentuk persepsi masyarakat terhadap perilaku menyimpang. Dengan begitu, penelitian ini tidak hanya berfokus pada peristiwa kejahatan, tetapi juga mengaitkannya dengan kondisi sosial yang melatarbelakanginya, termasuk pengaruh globalisasi, perkembangan teknologi, ketimpangan akses digital, dan lemahnya regulasi yang belum sepenuhnya adaptif terhadap dinamika kejahatan modern.

Secara keseluruhan, penggunaan pendekatan kualitatif deskriptif dalam penelitian ini menjadi strategi metodologis yang tepat untuk mengurai berbagai dimensi yang melekat pada kejahatan siber, sekaligus menyajikan pemahaman menyeluruh yang tidak mungkin dicapai melalui pendekatan kuantitatif yang hanya menitikberatkan pada angka dan statistik.

Jenis Penelitian

Jenis penelitian ini adalah studi literatur (library research), yaitu dengan menelaah berbagai sumber ilmiah seperti buku-buku kriminologi, jurnal hukum dan teknologi, peraturan perundang-undangan, laporan penelitian, artikel media, serta laporan resmi dari lembaga pemerintah dan organisasi internasional yang relevan, seperti BSSN (Badan Siber dan Sandi Negara), INTERPOL, Europol, dan lainnya.

Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui:

1. Dokumentasi, yakni mengumpulkan data sekunder dari berbagai sumber tertulis yang kredibel dan ilmiah.
2. Penelusuran Literatur Online, menggunakan database akademik seperti Google Scholar, JSTOR, ProQuest, dan ScienceDirect untuk mendapatkan literatur terkini mengenai cybercrime dan perspektif kriminologisnya.

3. Analisis Perundang-undangan, dengan mencermati regulasi terkait kejahatan siber, seperti UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya, serta konvensi internasional seperti *Budapest Convention on Cybercrime*.

Teknik Analisis Data

Data dianalisis secara deskriptif-analitis, yaitu dengan memaparkan isi dari data yang telah dikumpulkan kemudian dianalisis berdasarkan konsep-konsep dan teori dalam kriminologi, antara lain:

1. Teori Motivasi Kejahatan: Untuk mengidentifikasi motif pelaku (ekonomi, ideologi, psikologis).
2. Teori Kesempatan (Routine Activity Theory): Untuk menjelaskan mengapa kejahatan siber mudah terjadi dalam konteks digital.
3. Teori Strain dan Kontrol Sosial: Untuk memahami faktor sosial yang menyebabkan individu terjerumus dalam tindakan kriminal berbasis teknologi.

Setiap data yang diperoleh dikaji secara komprehensif dan dibandingkan antara satu sumber dengan sumber lainnya guna menghasilkan kesimpulan yang objektif dan mendalam. Validitas data diperkuat dengan triangulasi sumber, yaitu membandingkan berbagai sumber literatur untuk menghindari bias interpretatif.

Lokasi dan Waktu Penelitian

Karena berbasis literatur, penelitian ini tidak terbatas pada lokasi fisik tertentu, namun seluruh sumber yang digunakan mencakup konteks nasional (Indonesia) dan internasional. Waktu pelaksanaan penelitian berlangsung selama Februari–Juli 2025, dengan fokus pada perkembangan terbaru dalam bidang keamanan siber dan pendekatan kriminologis terhadap cybercrime.

ANALISIS DAN HASIL PENELITIAN

Peneltian ini menghasilkan pemahaman yang komprehensif dan mendalam mengenai karakteristik kejahatan siber, yang dianalisis berdasarkan berbagai literatur kriminologi dan sumber data sekunder yang relevan. Kajian ini menunjukkan bahwa kejahatan siber bukanlah sekadar kejahatan teknis yang berkaitan dengan pelanggaran terhadap sistem digital, melainkan merupakan fenomena sosial multidimensi yang memiliki akar permasalahan jauh lebih kompleks. Fenomena ini tidak dapat dipisahkan dari dinamika sosial, tekanan psikologis, konstruksi budaya digital, serta struktur ekonomi dan politik global yang turut membentuk perilaku kriminal dalam ruang maya.

Ditemukan bahwa kriminalitas siber berkembang seiring transformasi teknologi**,** di mana akses terhadap perangkat digital yang semakin murah dan luas telah membuka peluang bagi lebih banyak individu untuk terlibat dalam aktivitas ilegal di internet. Namun, kecanggihan teknologi itu sendiri tidak cukup untuk menjelaskan mengapa seseorang terlibat dalam tindakan kejahatan. Oleh karena itu, pendekatan kriminologi menjadi penting untuk menjelaskan faktor-faktor non-teknis, seperti motivasi pribadi, tekanan sosial, eksklusi ekonomi, disorientasi identitas, bahkan kebutuhan akan pengakuan dalam komunitas digital.

Kejahatan siber juga berakar pada budaya digital yang permisif**,** di mana pelanggaran data atau privasi sering kali dianggap remeh, terutama dalam komunitas daring yang anonim. Kondisi

ini menciptakan ruang interaksi sosial yang minim regulasi etis dan hukum, sehingga mendorong individu untuk melakukan kejahatan dengan perasaan aman dan tanpa rasa bersalah. Selain itu, perubahan pola interaksi manusia yang kini lebih banyak terjadi di ranah virtual telah menggeser cara kejahatan dilakukan: dari tindakan fisik yang kasatmata menjadi kejahatan tidak berwujud yang sulit dideteksi dan dibuktikan secara hukum.

Berdasarkan temuan ini, dapat disimpulkan bahwa pendekatan tradisional dalam memaknai dan menangani kejahatan tidak lagi memadai untuk menjawab tantangan kejahatan siber. Diperlukan pendekatan interdisipliner yang menggabungkan pemahaman teknologi informasi, kriminologi, psikologi sosial, serta studi kebijakan publik agar respons terhadap kejahatan siber menjadi lebih tepat sasaran, berkelanjutan, dan humanistik.

Motif Pelaku Kejahatan Siber: Multifaktor dan Adaptif

Hasil studi menunjukkan bahwa motif pelaku kejahatan siber bersifat multifaktor, dinamis, dan adaptif terhadap perubahan sosial maupun perkembangan teknologi informasi. Tidak ada satu motif tunggal yang dapat menjelaskan seluruh tindakan kriminal di dunia maya. Sebaliknya, motif-motif tersebut seringkali saling beririsan, dipengaruhi oleh kondisi pribadi, struktural, maupun peluang yang tersedia secara teknologis.

1. **Motif Ekonomi (Profit-Oriented Cybercrime)**

   Motif ekonomi menjadi dorongan paling dominan, terutama dalam kejahatan yang melibatkan penipuan daring (online fraud), pencurian identitas, pencurian data kartu kredit, serta ransomware. Pelaku mencari keuntungan finansial dengan risiko rendah melalui celah keamanan sistem informasi. Kejahatan ini seringkali dilakukan oleh individu atau kelompok yang memiliki keterampilan teknis tinggi, bahkan dalam beberapa kasus, berafiliasi dengan sindikat kejahatan transnasional.

   Namun demikian, motif ekonomi juga dapat muncul dari kondisi ekonomi yang tertekan, seperti pengangguran, ketimpangan digital, atau kebutuhan mendesak yang membuat individu mencari jalan pintas dengan mengeksploitasi ruang siber. Dalam konteks ini, kejahatan muncul sebagai bentuk adaptasi atas keterbatasan struktural dalam masyarakat nyata (Yar, 2013).

2. **Motif Ideologis dan Politik (Hacktivism dan Cyberterrorism)**

   Di sisi lain, muncul pula kejahatan siber yang dilatarbelakangi oleh motif ideologis, politik, dan religius. Pelaku atau kelompok tertentu melakukan serangan terhadap infrastruktur digital milik negara, organisasi internasional, atau korporasi multinasional sebagai bentuk perlawanan simbolik terhadap kekuasaan, ketimpangan, atau kebijakan tertentu. Misalnya, serangan yang dilakukan oleh kelompok *hacktivist* seperti Anonymous biasanya dilandasi oleh semangat keadilan sosial dan perlawanan terhadap otoritarianisme.

   Dalam spektrum yang lebih ekstrem, kejahatan siber juga digunakan sebagai alat terorisme modern (cyberterrorism), di mana propaganda, rekrutmen, dan bahkan perencanaan serangan fisik dilakukan melalui platform digital. Kejahatan ini bersifat sangat terorganisir, sistematis, dan berpotensi mengancam stabilitas nasional serta keamanan internasional.

3. Motif Psikologis dan Personal (Revenge, Recognition, Curiosity)

Selain motif yang bersifat rasional, pelaku juga seringkali terdorong oleh faktor psikologis dan personal, seperti kebutuhan akan pengakuan (recognition), rasa ingin tahu (curiosity), atau keinginan membalas dendam (revenge) terhadap individu, institusi, atau sistem tertentu. Hal ini banyak ditemukan dalam kasus peretasan akun media sosial, pencemaran nama baik, atau *revenge porn*, yang kerap dilakukan oleh orang dekat korban.

Motif semacam ini menunjukkan bahwa pelaku kejahatan siber tidak selalu berasal dari latar belakang kriminal, melainkan bisa saja individu biasa, termasuk remaja atau mahasiswa, yang memiliki akses teknologi dan tidak mendapatkan pendampingan moral atau etika digital. Dalam beberapa kasus, tindakan ini berawal dari rasa frustrasi, isolasi sosial, atau sekadar iseng, namun dapat berkembang menjadi kebiasaan menyimpang yang lebih serius (Maras, 2016).

4. Relevansi dengan Teori Kriminologi: Routine Activity Theory

Temuan mengenai kompleksitas motif ini selaras dengan Routine Activity Theory yang dikembangkan oleh Cohen dan Felson. Teori ini menyatakan bahwa suatu kejahatan akan terjadi apabila terdapat tiga unsur secara bersamaan: (1) pelaku yang termotivasi, (2) target yang layak, dan (3) ketiadaan penjagaan yang memadai. Dunia maya menyediakan ketiganya secara simultan: pelaku termotivasi dapat berasal dari berbagai latar belakang; target yang layak bisa berupa data pribadi, sistem keuangan, atau infrastruktur digital; dan pengawasan di ruang digital masih sangat lemah, baik secara teknis maupun hukum.

Dengan demikian, motif kejahatan siber menjadi refleksi dari hubungan antara individu, teknologi, dan struktur sosial. Analisis terhadap motif ini penting tidak hanya untuk memahami karakter pelaku, tetapi juga sebagai dasar dalam merumuskan strategi pencegahan yang berbasis pada pemetaan risiko dan faktor pemicu kejahatan secara kontekstual.

Pola Modus Operandi: Canggih, Terorganisir, dan Terus Berkembang

Penelitian ini mengidentifikasi bahwa modus operandi dalam kejahatan siber tidak statis, melainkan mengalami perkembangan pesat seiring kemajuan teknologi, perubahan sistem keamanan digital, serta peningkatan kemampuan teknis para pelaku. Transformasi ini menandai pergeseran dari kejahatan digital yang bersifat sederhana dan individual, menjadi tindakan kriminal yang sangat terstruktur, terorganisir, dan melibatkan aktor lintas negara.

1. Evolusi Modus Operandi: Dari Defacing ke Malware Canggih

Pada tahap awal, kejahatan siber banyak dilakukan oleh individu (lone hackers) dengan motif eksistensial atau hanya sekadar "iseng", seperti melakukan defacing situs web atau membobol akun media sosial. Aksi ini lebih bersifat simbolik dan terbatas dalam dampak. Namun dalam satu dekade terakhir, terjadi transformasi signifikan ke arah kejahatan yang bersifat sistematis dan masif, dengan pelaku memanfaatkan teknologi otomatis, skrip canggih, serta kecerdasan buatan untuk meningkatkan efektivitas dan skala serangan.

Bentuk kejahatan seperti ransomware telah menjadi salah satu ancaman utama. Dalam skema ini, pelaku tidak hanya menyebabkan gangguan sistem, tetapi menyandera data penting korban, lalu meminta tebusan dalam bentuk mata uang kripto seperti Bitcoin. Strategi ini tidak

hanya menimbulkan kerugian ekonomi, tetapi juga menyulitkan proses pelacakan hukum karena transaksi dilakukan secara anonim dan lintas yurisdiksi.

2. Serangan Siber yang Menyasar Infrastruktur Kritis

Penelitian juga mencatat pergeseran target serangan, dari entitas individual ke institusi vital, seperti sektor pemerintahan, layanan kesehatan, sistem keuangan, dan infrastruktur publik. Modus seperti spear phishing yaitu teknik manipulasi psikologis yang disesuaikan secara spesifik dengan profil korban—telah digunakan untuk mengakses jaringan internal organisasi dengan tujuan sabotase, pencurian data, atau penanaman malware jangka panjang.

Contoh empiris dapat ditemukan dalam serangan terhadap sistem rumah sakit di Jerman (2020), di mana ransomware menyebabkan terganggunya layanan gawat darurat dan mengakibatkan kematian pasien akibat keterlambatan penanganan. Peristiwa ini mengindikasikan bahwa kejahatan siber kini telah memiliki konsekuensi nyata terhadap keselamatan publik, bukan sekadar kerugian digital.

3. Keterlibatan Jaringan Kriminal dan Aktor Negara

Dalam banyak kasus, kejahatan siber tidak lagi dilakukan oleh pelaku tunggal, melainkan oleh jaringan terorganisir yang beroperasi seperti kartel kriminal. Mereka memiliki struktur hierarkis, sistem distribusi tugas, serta penggunaan alat serangan yang diperjualbelikan di pasar gelap (*dark web*), seperti exploit kits, botnet rental, hingga zero-day vulnerabilities. Bahkan dalam beberapa kasus, terdapat dugaan keterlibatan aktor negara (*state-sponsored attackers*) yang menjadikan dunia siber sebagai arena konflik geopolitik.

4. Adaptasi terhadap Sistem Keamanan

Menariknya, para pelaku kejahatan siber juga terus berinovasi untuk menghindari deteksi dan penindakan hukum. Mereka menggunakan teknik obfuscation (penyamaran kode), multi-layer encryption, serta menjalankan operasi melalui virtual private networks (VPN) atau server bouncing untuk menyamarkan lokasi. Dengan demikian, penegakan hukum menghadapi tantangan besar dalam membongkar jaringan pelaku dan mengamankan bukti digital secara sah.

5. Implikasi Kriminologis

Dari perspektif kriminologi, perkembangan modus operandi ini mencerminkan rasionalitas instrumental para pelaku yang selalu menyesuaikan strategi dengan lingkungan sosial dan teknologi. Dalam pendekatan Crime-as-a-Service (CaaS), kejahatan siber bahkan telah dikomersialisasi layaknya layanan legal, di mana pelaku dapat menyewa alat atau jasa serangan tanpa harus memiliki kemampuan teknis sendiri. Hal ini menuntut pendekatan penanggulangan yang tidak hanya berbasis hukum dan teknologi, tetapi juga melibatkan analisis struktural dan motivasional pelaku, pemetaan jaringan, serta kerja sama lintas negara yang efektif dan berkelanjutan (Bareskrim Polri, 2022).

Strategi Penanggulangan Kejahatan Siber: Pendekatan Integratif dan Multidisipliner

Penanggulangan kejahatan siber tidak dapat disederhanakan hanya dalam kerangka hukum formal atau pendekatan represif konvensional. Kejahatan siber merupakan bentuk kriminalitas modern yang bersifat transnasional (lintas batas negara), tidak berwujud secara fisik (nonphysical),

dan kerap kali dilakukan secara anonim, sehingga sangat sulit untuk dilacak maupun ditindak melalui prosedur hukum yang lazim. Pelaku kejahatan siber seringkali tidak berada dalam yurisdiksi yang sama dengan korban maupun dengan otoritas penegak hukum yang menangani kasus, sehingga memunculkan tantangan serius dalam aspek penegakan hukum dan kecepatan respon.

Karakteristik tersebut menuntut lahirnya strategi penanggulangan yang holistik, adaptif, dan berkelanjutan, yang tidak hanya mengandalkan penegakan hukum (law enforcement), tetapi juga menyentuh aspek pencegahan, perlindungan sistem, pemberdayaan masyarakat, dan kerjasama lintas sektoral. Pendekatan ini juga harus responsif terhadap dinamika teknologi informasi dan komunikasi (TIK) yang berubah sangat cepat. Oleh karena itu, penanggulangan kejahatan siber memerlukan kerangka kerja integratif yang melibatkan empat pilar utama, yaitu:

1. **Pendekatan Legal dan Regulatif: Penguatan Hukum Siber**

   Kerangka hukum merupakan fondasi utama dalam merespons kejahatan siber. Di Indonesia, regulasi utama seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan perubahannya perlu terus diperbarui agar tetap relevan dengan perkembangan modus operandi kejahatan digital. Namun, penguatan substansi hukum harus diiringi dengan peningkatan kapasitas kelembagaan, seperti membentuk atau memperkuat unit siber kepolisian dan kejaksaan yang dibekali alat forensik digital mutakhir dan pelatihan teknis secara berkala (Mabes Polri, 2024). Selain itu, kerja sama internasional menjadi elemen penting. Ratifikasi dan implementasi Budapest Convention on Cybercrime dapat memperkuat posisi Indonesia dalam kerja sama lintas batas dalam penegakan hukum terhadap pelaku siber lintas negara (https://www.coe.int , 2025).

2. **Peningkatan Keamanan Teknologi: Strategi Protektif Proaktif**

   Langkah teknologis menjadi lapisan pertama dalam mencegah kejahatan siber. Strategi keamanan siber tidak bisa lagi bersifat pasif, melainkan harus mengadopsi prinsip defense in depth. Institusi—baik pemerintah maupun swasta—wajib menerapkan standar keamanan digital seperti ISO/IEC 27001, membangun arsitektur keamanan siber berlapis, serta rutin melakukan audit dan simulasi penetrasi sistem (penetration test). Penggunaan teknologi seperti enkripsi data, autentikasi dua faktor (2FA), sistem pemantauan real-time, dan AI-based threat detection juga harus didorong secara masif untuk memperkecil celah serangan (Kominfo, 2023).

3. **Edukasi dan Literasi Digital: Pencegahan Berbasis Masyarakat**

   Salah satu temuan penting dalam penelitian ini adalah bahwa sebagian besar serangan siber berhasil karena kelalaian atau ketidaktahuan pengguna, bukan semata-mata karena kecanggihan pelaku. Oleh karena itu, peningkatan literasi digital masyarakat menjadi kebutuhan mendesak. Pendidikan keamanan digital harus diintegrasikan mulai dari jenjang sekolah dasar hingga perguruan tinggi, termasuk pelatihan rutin di lingkungan kerja. Program-program cyber hygiene, sosialisasi cara mengenali phishing, dan kampanye anti-click bait perlu digalakkan secara nasional. Di samping itu, pelibatan komunitas lokal dalam mendeteksi potensi ancaman digital juga bisa menjadi strategi pencegahan berbasis komunitas yang efektif (https://www.ibm.com).

4. Kolaborasi Multistakeholder: Membangun Ekosistem Ketahanan Siber

Tidak ada satu institusi pun yang mampu menangani kejahatan siber secara sendiri. Oleh karena itu, kolaborasi lintas sektor menjadi kunci utama dalam membangun resiliensi digital nasional. Pemerintah, swasta, akademisi, lembaga internasional, dan masyarakat sipil perlu membentuk aliansi strategis, seperti:

a. Public-Private Partnership (PPP) dalam pertukaran informasi ancaman siber.
b. Forum Respons Insiden Bersama (misalnya CERT/CSIRT nasional).
c. Kolaborasi Riset & Inovasi dalam pengembangan alat deteksi dan respon ancaman baru.
d. Perjanjian ekstradisi digital dan mutual legal assistance treaty (MLAT) untuk pelaku lintas negara (https://bssn.go.id).

Pendekatan ini sesuai dengan konsep networked governance, di mana keamanan tidak hanya menjadi tanggung jawab negara, tetapi juga produk dari kerja sama dan tanggung jawab bersama antar-aktor dalam sistem sosial digital.

KESIMPULAN DAN SARAN

Berdasarkan penelitian dalam jurnal ini dapat disimpulkan bahwa kejahatan siber merupakan fenomena kriminal modern yang sangat kompleks dan terus berkembang secara dinamis, baik dalam hal motif, modus operandi, maupun bentuk kejahatannya. Kompleksitas ini tercermin dari beragamnya latar belakang pelaku, skala serangan, dan dampak yang ditimbulkan. Motif kejahatan siber tidak dapat disederhanakan hanya pada keuntungan ekonomi semata, tetapi juga meliputi motif ideologis (seperti hacktivism), psikologis (seperti kebutuhan akan pengakuan), dan personal (seperti balas dendam atau rekayasa sosial berbasis emosi). Hal ini menunjukkan bahwa pelaku kejahatan siber tidak selalu berasal dari kalangan kriminal profesional, melainkan bisa juga merupakan individu biasa yang memiliki akses terhadap teknologi digital dan dorongan motivasional tertentu.

Selain itu, modus operandi kejahatan siber telah mengalami transformasi signifikan, dari tindakan sporadis dan individual seperti peretasan akun media sosial atau pengubahan halaman situs (defacing), menjadi serangan siber yang terstruktur, terorganisir, dan berskala lintas negara. Fenomena Crime-as-a-Service (CaaS) memperlihatkan adanya industrialisasi dalam dunia kejahatan digital, di mana alat bantu kejahatan, malware, ransomware, hingga jasa serangan seperti DDoS attack dapat dibeli atau disewa secara anonim melalui pasar gelap internet (dark web). Kondisi ini memperbesar potensi serangan, karena pelaku tidak lagi harus memiliki kompetensi teknis tinggi untuk melancarkan aksinya—cukup dengan dana dan niat.

Salah satu temuan penting dari penelitian ini adalah bahwa faktor kelemahan pengguna masih menjadi celah terbesar dalam terjadinya serangan siber. Serangan yang berhasil umumnya tidak hanya disebabkan oleh kecanggihan teknologi yang digunakan oleh pelaku, tetapi juga akibat rendahnya kesadaran keamanan digital, kurangnya literasi siber, dan kelalaian individu atau institusi dalam menerapkan langkah-langkah preventif dasar. Dengan demikian, penanggulangan kejahatan siber tidak cukup apabila hanya mengandalkan pendekatan legal-formal atau peningkatan perangkat teknologi. Diperlukan pendekatan yang holistik, terintegrasi, dan multidisipliner yang mencakup ranah hukum, teknologi informasi, pendidikan, sosiologi, hingga kriminologi.

Lebih jauh lagi, strategi yang efektif dalam menanggulangi kejahatan siber harus menyertakan kolaborasi multipihak dalam ekosistem digital, di mana tanggung jawab keamanan tidak hanya berada di tangan negara, tetapi juga merupakan hasil dari keterlibatan aktif sektor swasta, akademisi, lembaga internasional, dan masyarakat sipil. Dengan pendekatan yang menyeluruh ini, diharapkan sistem keamanan siber Indonesia dapat lebih adaptif dan tangguh dalam menghadapi tantangan kejahatan digital yang semakin kompleks dan transnasional.

Sebagai rekomendasi penulis juga menyarankan untuk menanggulangi kejahatan siber secara eketif disarankan agar, penanggulangan kejahatan siber di Indonesia tidak dapat dilakukan secara parsial atau sesaat, melainkan memerlukan suatu strategi nasional yang terstruktur, sistematis, dan terukur, yang melibatkan berbagai unsur yang mempunyai kepentingan secara terpadu. Pemerintah memiliki peran sentral dalam membangun ekosistem keamanan digital melalui peningkatan literasi dan kesadaran masyarakat terhadap pentingnya keamanan siber. Hal ini dapat diwujudkan dengan mengintegrasikan materi tentang cyber hygiene ke dalam kurikulum pendidikan formal sejak dini, menyelenggarakan pelatihan keamanan digital secara rutin di lingkungan kerja, serta menggencarkan kampanye edukatif secara berkelanjutan di media massa dan media sosial, guna menjangkau seluruh lapisan masyarakat.

Dari sisi kebijakan hukum, penguatan regulasi sangat mendesak dilakukan, termasuk revisi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan penyusunan peraturan turunan yang lebih adaptif terhadap bentuk-bentuk kejahatan siber terbaru. Selain itu, aparat penegak hukum perlu dibekali kompetensi forensik digital dan penguasaan teknologi investigasi siber mutakhir, agar mampu menanggapi insiden dengan cepat dan efektif. Regulasi yang kuat harus disertai dengan penegakan hukum yang profesional, transparan, dan berorientasi pada keadilan.

Lebih jauh, penerapan standar keamanan digital wajib menjadi prioritas nasional. Setiap lembaga pemerintahan, badan usaha, dan institusi pendidikan wajib menerapkan sistem manajemen keamanan informasi berbasis ISO/IEC 27001, menggunakan teknologi enkripsi data, autentikasi dua faktor (2FA), serta sistem deteksi ancaman berbasis kecerdasan buatan (AI-based threat detection) untuk mengurangi risiko kebocoran data dan serangan siber. Audit sistem secara berkala dan simulasi uji penetrasi (penetration test) juga harus menjadi prosedur standar untuk mengevaluasi kerentanan sistem digital secara proaktif.

Dalam konteks tata kelola, kolaborasi multistakeholder menjadi kunci keberhasilan. Pemerintah perlu membangun dan memfasilitasi kerja sama lintas sektor melalui kemitraan publik-swasta (Public-Private Partnership/PPP), forum pertukaran informasi intelijen, dan kerja sama riset pengembangan teknologi keamanan antara lembaga riset, universitas, dan perusahaan teknologi. Selain itu, dibutuhkan respons insiden siber yang terpadu dan cepat, melalui pembentukan dan penguatan Computer Security Incident Response Team (CSIRT) secara nasional dan sektoral yang mampu berkoordinasi baik secara domestik maupun internasional.

Terakhir, di dunia akademik memiliki tanggung jawab besar dalam membangun fondasi ilmiah yang kuat melalui pengembangan kajian kriminologi siber yang berbasis interdisipliner—mengkaji aspek sosiologis, psikologis, hukum, dan teknologi dari pelaku dan jaringan kejahatan siber. Dengan begitu, kebijakan dan strategi penanggulangan dapat didasarkan pada data empiris dan pendekatan yang lebih holistik. Dengan kolaborasi yang erat antara seluruh elemen bangsa—pemerintah, masyarakat, sektor swasta, dan akademisi—maka Indonesia dapat membangun

ketahanan digital nasional yang adaptif, inklusif, dan berkelanjutan dalam menghadapi ancaman kejahatan siber yang semakin kompleks.

DAFTAR PUSTAKA

3. ID-SIRTII/CC, Laporan Tahunan Keamanan Siber Indonesia 2023, Jakarta: Kominfo, 2023, hlm. 42–45.
https://idsirtii.or.id

Badan Reserse Kriminal Polri. Kajian Kriminologi terhadap Kejahatan Siber di Indonesia. Jakarta: Bareskrim Polri, 2022.

Badan Siber dan Sandi Negara (BSSN), Strategi Keamanan Siber Nasional 2020–2024, hlm. 12–13. Diakses dari: https://bssn.go.id

Council of Europe. "Convention on Cybercrime (ETS No.185)," https://www.coe.int, diakses 10 Juli 2025.

David S. Wall, Cybercrime: The Transformation of Crime in the Information Age, Polity Press, 2007, hlm. 1–2.

Direktorat Tindak Pidana Siber Bareskrim Polri. Laporan Tahunan Kejahatan Siber 2023. Jakarta: Mabes Polri, 2024.

Fajar Nur, "Penegakan Hukum terhadap Kejahatan Siber di Indonesia," Jurnal Kriminologi Indonesia, Vol. 5 No. 2, 2023, hlm. 100–102.

http://digilib.uinsa.ac.id/18974/5/Bab%203.pdf

https://ipssj.com/index.php/ojs/article/view/363

https://journal.cattleyadf.org/index.php/Judge/article/download/1182/686/

https://rayyanjurnal.com/index.php/qistina/article/download/6027/pdf

https://www.cloudcomputing.id/berita/3-faktor-penyebab-kejahatan-siber

https://www.sciencedirect.com/topics/social-sciences/routine-activity-theory

IBM Security. Cost of a Data Breach Report 2021. https://www.ibm.com/reports/data-breach.

Lihat Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta perubahan melalui UU No. 19 Tahun 2016.

Majid Yar, Cybercrime and Society, Sage Publications, 2013, hlm. 23–25.

Maras, Marie-Helen. Cybercriminology. Oxford University Press, 2016.

Moleong, Lexy J. Metodologi Penelitian Kualitatif. Bandung: Remaja Rosdakarya, 2012.

Yar, Majid. Cybercrime and Society. London: SAGE Publications, 2013.