QISTINA: Jurnal Multidisiplin Indonesia
P-ISSN: 2964-6278 E-ISSN: 2964-1268
Vol. 4 No. 1 Juni 2025

Kejahatan Cyber: Motif dan Implikasi terhadap Keamanan Nasional

Adim Isral Ayubi[1] Ahmadin[2] Bakhtiar[3]
Program Studi Pendidikan Hukum dan Kewarganegaraan, Program Pasca Sarjana, Universitas Negeri Makassar, Kota Makassar, Provinsi Sulawesi Selatan, Indonesia[1,2,3]
Email: adimisralayubi14052@gmail.com[1] ahmadin@unm.ac.id[2] bakhtiar@unm.ac.id[3]

Abstrak

Mendeskripsikan terkait kejahatan cyber atau cybercrime, motif-motif yang mendasari terjadinya kejahatan cyber, implikasi yang ditimbulkan akibat kejahatan cyber terhadap keamanan Nasional dan tujuan penelitian yang empat yaitu untuk mengetahui upaya pencegahan yang dapat dilakukan terhadap kejahatan cybercrime. Metode penelitian ini menggunakan studi kepustakaan (library research) yakni dengan mengumpulkan data yang diambil dari sejumlah literatur baik dari buku, jurnal, ataupun karya ilmiah lain yang mendukung dan berkaitan dengan penelitian ini. Analisis data yang penulis gunakan adalah analisis deskriptif, yaitu menganalisis semua sumber yang diperoleh terkait artikel ini, kemudian menemukan motif dan impliksinya kejahatan cybercrime. Tujuan dalam penelitian ini adalah untuk mengetahui bagaiman kejahatan cyber atau cybercrime, motif-motif kejahatan Cyber (Cybercrime) dan implikasinya serta upaya pencegahan kejahatan cyber terhadap Keamanan Nasional. Hasil penelitian ini adalah (1) Kejahatan cyber atau Cybercrime adalah ancaman yang nyata dan terus berkembang seiring kemajuan teknologi (2) Motif kejahatan cyber atau cybercrime terhadap keamanan Nasinoal yaitu motif individu,ekonomi,politik dan Kriminal. Motif para pelaku dalam melakukan kejahatan ini tidak hanya karena uang, tetapi juga untuk mencari kesenangan. Adapun motif berdasarkan pada kegiatannya (3) Implikasinya yang dapat berdampak terhadap keamanan nasinoal yaitu menargetkan infrastruktur kritis, mencuri data sensitif, menyebarkanluaskan propaganda dan disinformasi, melumpuhkan layanan publik, mengintimidasi dan membungkam suara kritis (4) Upaya pencegahan yaitu Untuk melindungi Keamanan Nasional dari kejahatan cyber, penegak hukum harus memperkuat kerja sama internasional dan mengembangkan kapasitas untuk secara efektif dalam mendeteksi, menyelidiki, dan menuntut pelaku kejahatan cyber atau cybercrime.

Kata Kunci: Kejahatan Cyber (Cybercrime); Motif ; Implikasi; Upaya Pencegahan, Keamanan Nasional

Abstract

This research describes cybercrime, the motives underlying the occurrence of cybercrime, the implications of cybercrime for national security and the fourth research objective is to find out the prevention efforts that can be done against cybercrime. This research method uses library research, namely by collecting data taken from a number of literatures from books, journals, or other scientific works that support and are related to this research. The data analysis that the author uses is descriptive analysis, which analyzes all sources obtained related to this article, then finds the motives and implications of cybercrime. The purpose of this research is to find out how cyber crime or cybercrime, motives of Cyber crime (Cybercrime) and its implications and efforts to prevent cyber crime against National Security. The results of this study are (1) Cyber crime or Cybercrime is a real threat and continues to grow as technology advances (2) The motives of cyber crime or cybercrime against national security are individual, economic, political and criminal motives. The motives of the perpetrators in committing this crime are not only for money, but also to seek pleasure. The motives are based on their activities (3) The implications that can have an impact on national security are targeting critical infrastructure, stealing sensitive data, disseminating propaganda and disinformation, paralyzing public services, intimidating and silencing critical voices (4) Prevention efforts are To protect National Security from cybercrime, law enforcement must strengthen international cooperation and develop the capacity to effectively detect, investigate, and prosecute perpetrators of cybercrime.

Keywords: *Cybercrime; Motives; Implications; Prevention Efforts, National Security*

PENDAHULUAN

Perkembangan masyarakat sekarang ini semakin maju dan didukung oleh perkembangan teknologi dan komunikasi. Perkembangan dan kemajuan teknologi informasi yang sangat pesat telah menimbulkan perubahan dalam aktivitas kehidupan manusia di berbagai bidang, yang secara langsung berpengaruh terhadap lahirnya bentuk-bentuk perbuatan hukum baru, maka penggunaan dan pemanfaatan teknologi informasi harus lebih dikembangkan untuk menjaga, memelihara dan meningkatkan persatuan dan kesatuan bangsa yang dilandasi oleh peraturan perundang-undangan untuk kepentingan nasional, bahwa penggunaan teknologi informasi memegang peranan penting dalam perdagangan dan pertumbuhan ekonomi nasional untuk mewujudkan kesejahteraan masyarakat (Yuhandra et al., 2021). Dalam perkembangan teknologi dan informasi, kejahatan siber menjadi tantangan yang dapat mengancam keamanan dan ketahanan nasional suatu negara. Indonesia, sebagai salah satu negara dengan pengguna internet yang berkembang pesat, menghadapi meningkatnya risiko terkait dengan berkembangnya kejahatan teknologi informasi (Sitompul et al., 2024). Tentunya tidak dapat dipungkiri dampaknya terhadap perkembangan masyarakat Indonesia yang sedang membangun di era reformasi menghadapi berbagai krisis, baik politik, ekonomi, maupun sosial budaya, dan hal ini harus ditangani agar bangsa dan negara Indonesia tetap dianggap eksis di tengah bangsa-bangsa di dunia (Liviani, 2020). Penggunaan internet yang canggih dan cepat juga menimbulkan kejahatan yang sangat canggih dan sulit untuk diketahui oleh para pelakunya, hal ini dikarenakan internet merupakan media komunikasi yang bersifat tidak nyata (virtual), sehingga para pelaku kejahatan dapat dengan mudah menghilangkan jejak tanpa dapat mengetahui dengan jelas tujuan dan motif kejahatan yang dilakukan(Prasetiyo & Mukhtar, 2020)

Kemajuan teknologi yang pesat telah memunculkan kejahatan cyber, yang memiliki dampak positif dan negatif (Ghozali et al., 2024). Terdapat beragam jenis tindak pidana yang berpotensi terjadi, antara lain manipulasi data, spionase, sabotase, provokasi, pencucian uang, peretasan, pornografi, prostitusi online, pencurian perangkat lunak, dan perusakan perangkat keras. Namun demikian, kapasitas pemerintah untuk secara efektif mengatasi masalah kejahatan siber terhambat oleh munculnya ancaman cyber baru yang cepat, yang memperumit upaya untuk memerangi tantangan ini (Nugraha et al., 2022). Banyak kasus kejahatan siber yang muncul di Indonesia, termasuk pencurian kartu kredit, peretasan situs web, penyadapan data (misalnya, email), dan manipulasi data melalui penerapan perintah yang tidak diinginkan oleh para peretas. Ancaman cyber umumnya didefinisikan sebagai perolehan informasi rahasia milik orang lain melalui eksploitasi kerentanan sistem oleh program yang dibuat oleh seseorang yang berniat melakukan kejahatan cyber (Khamzina et al., 2022). Munculnya kejahatan cyber telah menimbulkan ancaman terhadap stabilitas, sehingga mempersulit upaya pemerintah untuk mengatur keseimbangan antara teknologi kriminal dan teknologi komputer, terutama yang berkaitan dengan jaringan internet dan sistem komputer (Irawati et al., 2021).

Cybercrime dapat dibagi menjadi dua kategori, yaitu kejahatan terhadap sistem komputer dan kejahatan yang menggunakan jaringan komputer (Widodo)(Umbara & Setiawan, 2022). Kejahatan cyber masih banyak terjadi, contoh tindakan seperti pencurian identitas (identity theft), penipuan online/pembobolan kartu kredit (carding), memata-matai target tertentu (cyber espionage) dan serangan cyber memberikan dampak negatif bagi masyarakat dan individu (Del-real) (Muharam & Budianto) (Ginanjar Laksana & Mulyani, 2024)(Ariyaningsih et al., 2023). Hal ini sejalan dengan pendapat (Sitompul et al., 2024)Perkembangan teknologi yang terus berkembang membuka celah bagi para pelaku kejahatan untuk menggunakan metode baru yang lebih kompleks seperti pencurian identitas,

penipuan online, dan serangan ransomware. Saat ini, ketergantungan masyarakat terhadap teknologi informasi semakin meningkat, dan risikonya semakin meningkat. Saat ini, semua aspek ekonomi, sosial, dan pertahanan negara sangat bergantung pada Internet. Perbankan, kegiatan ekonomi, pemeliharaan dan penggunaan transportasi, pengendalian senjata, dan komunikasi sosial, semuanya tidak dapat dipisahkan dari interkoneksi ini. Dalam konstelasi hukum pidana Indonesia, cybercrime tergolong kejahatan khusus, walaupun unsur pokoknya mungkin konsisten dengan berbagai ketentuan hukum pidana, namun dilakukan dengan cara (model) baru kejahatan ini, semacam semacam dokumen hukum yang lebih halus (Irawati et al., 2021)

Dari pemanfaatan teknologi informasi khususnya internet kita mendapatkan banyak peluang, dan tidak dapat dipungkiri bahwa teknologi informasi khususnya internet dapat digunakan untuk melakukan kejahatan yang awalnya hanya bersifat pengakuan, seperti pencurian, penipuan, ancaman, informasi hoax, dll. Media komputer dengan risiko yang sangat kecil untuk disadap (Ariyaningsih et al., 2023). Dampak negatif lainnya dalam perkembangan jaringan internet, sebagaimana dikemukakan oleh Roy Suryo, seorang pakar tekhnologi informasi, dalam penelitiannya yang dikutip oleh harian Kompas menyatakan: "Kejahatan cyber (cybercrime) kini marak di lima kota besar di Indonesia dan dalam taraf yang cukup memperhatikan serta yang dilakukan oleh para hacker yang rata-rata anak muda yang keliatannya kreatif, tetapi sesunggunya mereka mencuri nomor kartu kredit melalui internet (Nugraha et al., 2022). Keamanan, media yang digunakan oleh pelaku cybercrime berbeda dengan pelaku tindak pidana pada umumnya, pelaku cybercrime menggunakan akses internet yang ndapat digunakan dimana saja baik di tempat tertutup maupun terbuka. Namun, sistem keamanan yang dimiliki oleh internet masih belum dapat dikatakan aman, sehingga dapat membuat siapa pun bebas melakukan aktivitasnya di dunia maya tanpa sadar akan batasan yang dapat mendorong pertumbuhan cybercrime (Umbara & Setiawan, 2022). Kejahatan siber kini lebih dari sekadar ancaman teknologi, yang menjadi instrumen dalam perang asimetris yang dapat meruntuhkan stabilitas politik, ekonomi, dan sosial di berbagai negara (Atara et al., 2025). Para pelaku cyber crime ini memanfaatkan jaringan internet yang terkoneksi secara global sehingga dapat mengancam keamanan nasional suatu negara (Maskun) (Saramuke et al., 2025). Pada penelitian ini bertujuan untuk memahami motif dibalik kejahatan cyber (Cybercrime) serta mengkaji implikasinya terhadap keamanan nasinoal. Dengan memahami motivasi pelaku,diharapakan dapat ditemukan strategi pencegahan yang efektif.

METODE PENELITIAN

Metode penelitian ini adalah menggunakan studi kepustakaan (library research) yakni dengan mengumpulkan data yang diambil dari sejumlah literatur baik dari buku, jurnal, ataupun karya ilmiah lain yang mendukung dan berkaitan dengan penelitian ini (Adlini dkk.) (Tamhidah, 2023). Metode dari penelitian ini adalah metode penulis mengambil data yaitu tulisan-tulisan yang terkait dengan kejahatan cybercrime. Sumber data yang penulis ambil berupa buku dan artikel-artikel ilmiah. Analisis data yang penulis gunakan adalah analisis deskriptif, yaitu menganalisis semua sumber yang diperoleh terkait artikel ini, kemudain menemukan motif dan impliksinya kejahatan cybercrime. Tujuan dalam penelitian ini adalah untuk mengetahui bagaimana kejahatan cyber atau cybercrime, motif-motif kejahatan Cyber (Cybercrime) dan implikasinya serta upaya pencegahan kejahatan Cyber (Cybercrime) terhadap keamanan Nasional.

HASIL PENELITIAN DAN PEMBAHASAN

Kejahatan Cyber (Cybercrime)

Cyber crime adalah kejahatan yang berhubungan dengan komputer dan perangkat jaringan, biasanya dilakukan secara online. Kejahatan siber tidak hanya dilakukan oleh individu, tetapi juga dapat melibatkan kelompok atau organisasi dengan tujuan tertentu, baik finansial maupun non-finansial. Cybercrime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yangmendapat perhatian luas dunia internasional (Amin & Muslih, 2023). Kejahatan ini mencakup berbagai jenis aktivitas kriminal, seperti peretasan (hacking), pencurian data, penipuan online, penyebaran virus, dan eksploitasi kelemahan sistem keamanan. Hal ini sejalan dengan pendapat (Mudjiyanto et al., 2024) Cybercrime adalah tindakan kriminal atau sejenis aktifitas ilegal yang memanfaatkan kecerdasan teknologi untuk merugikan kepentingan atau merampas hak-hak orang lain, seperti pencurian, peretasan, penipuan, penyebaran virus, dan jenis kejahatan digital lainnya.

Menurut pendapat (Amin & Muslih, 2023) Cybercrime sendiri sebagai kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, memiliki karakteristik yang khas dibandingkan kejahatan konvensional, karakteristik unik dari kejahatan di dunia maya tersebut anatara lain menyangkut lima berikut: 1) ruang lingkup, 2) sifat kejahatan, 3) pelaku kejahatan, 4) modus kejahatan, dan 5) jenis kerugian yang ditimbulkan. Sedangkan jenis-jenis kejahatan cybercrime bisa dibedakan berdasarkan; 1) modus atau jenis aktifitasnya, contohnya: Anauthorized Acces, Illegal Contens, Penyebaran virus secara sengaja, Data Forgery, Cyber Espionage, Sabotage and Extortion, Cyberstalking, Carding, Hacking dan Cracker, Cybersquatting and Typosquatting, Hijacking dan Cyber Terosrism; 2) berdasarkan motif kegiatannya yaitu: Cybercrime sebagai tindak kejahatan murni dan Cybercrime sebagai tindak kejahatan abu-abu, 3) berdasarkan sasaran kejahatan diantaranya: Cybercrime yang menyerang individu (Againts Person), Cybercrime menyerang hak milik (Againts Property), Cybercrime menyerang pemerintah (Againts Government).

Adapun beberapa faktor utama yang menyebabkan timbulnya kejahatan siber itu sendiri adalah sebagai berikut:(a) Kurangnya sosialisasi atau pengarahan baik dari akademisi umum seperti sekolah atau edukasi dari orang tua mengenai manfaat internet,sehingga banyak penyalahgunaan yang terjadi; (b) Semakin maju sebuah negara, tapi tidak diimbangi kesejahteraan masyarakatnya, maka makin besarnya kesenjangan sosial terjadi; (c) Makin maraknya sosial media, media elektornik, dan media penyimpanan virtual (cloud), sehingga membuat manusia menjadi makin tergandrungi akan akses internet di dalam kehidupannya; (d) Gaya hidup; (e) Kelalaian daripada manusianya itu sendiri; (f) Adanya keinginan pengakuan dari orang lain; (g) Bertambah majunya teknologi dan mudahnya mengakses jaringan internet anytime anywhere tanpa ada batasan waktu (Umbara & Setiawan, 2022).

Motif Kejahatan Cyber (Cybercrime) terhadap Keamanan Nasional

Pada pelaku kejahatan cyber memiliki berbagai alasan yang mendorong dalam melakukan aksinya seperti motif individu, ekonomi, politik dan keriminal. Motif melakukan kejahatan ini di samping karena uang juga untuk mencari kesengan. Kejahatan ini juga muncul dari ketidakmampuan hukum, termasuk pihak berwengang dalam menjangkaunya. Kejahatan ini bersifat maya dimana pelaku tidak tampak secara fisik. Begitu hebatnya kejahatan ini bahkan dapat meresahkan dunia internasional(Amin & Muslih, 2023). Motivasi pelaku adalah salah satu faktor penentu yang paling penting dalam kejahatan siber. Ada berbagai motif yang mendorong seseorang untuk terlibat dalam kejahatan siber, termasuk motivasi keuangan, balas dendam, dan kepuasan pribadi (Khamzina et al., 2022). Ancaman kejahatan siber yang merupakan bentuk ancaman perang era modern atau non militer yang dapat memicu

terjadinya disintegrasi bangsa melalui motif kepentingan individu atau kelompok tertentu(Ariyaningsih et al., 2023).

Hal ini sejalan dengan Menurut pendapat (Umbara & Setiawan, 2022) Motif Kejahatan siber pada umumnya dapat dikelompokkan menjadi dua (2) katergori, yaitu sebagai berikut: (a) Motif Intelektual kejahatan yang dilakukan hanya untuk kepuasan pribadi dan menunjukkan bahwa dirinya telaah mampu untuk merekayasa dan mengimplementasikan bidang teknologi informasi. Kejahatan dengan motif ini pada umumnya dilakukan oleh seseorang secara individual. (b) Motif ekonomi, politik dan kriminal yaitu kejahatan yang dilakukan untuk keuntungan pribadi atau golongan tertentu yang berdampak pada kerugian secara ekonomi dan politik pada pihak lain. Karena memiliki tujuan yang dapat berdampak besar, kejahatan dengan motif ini pada umumnya dilakukan oleh sebuah korporasi. Adapun menurut pendapat (Wati et al., 2024) Beberapa tipikal kejahatan yang terjadi di internet ialah sebagai berikut:

1. Illegal contents atau konten yang tidak sah, yaitu memasukkan data palsu, tidak sah, dan melanggar hukum serta mengganggu ketertiban umum dalam internet.
2. Illegal acces/unauthorized access to computer system and service atau akses ilegal/akses tidak sah terhadap sistem dan layanan komputer, yaitu bentuk kejahatan yang dilakukan menggunakan cara meretas/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang disadapnya.
3. Cyber espionage atau spionase dunia maya, yaitu bentuk kejahatan yang menggunakan jaringan internet dengan cara memasuki sistem jaringan komputer pihak yang akan ditargetkan atau korban untuk dijadikan sasaran untuk dimata-matai.
4. Data forgery atau pemalsuan data, yaitu tindakan modus kriminal di sosial media yang dilakukan dengan cara memalsukan data dokumen penting yang disimpan sebagai dokumen tanpa kertas melalui internet. Kejahatan sejenis ini biasanya menargetkan dokumen e-commerce, seolah-olah adanya "typo" yang pada akhirnya akan merugikan korban, karena korban akan memasukkan data pribadi dan nomor kartu kredit kepada pelaku
5. Cyber sabotage and extortion atau sabotase dan pemerasan dunia maya, yaitu modus yang dijalankan dengan cara mengganggu, merusak, atau menghancurkan data yang terhubung ke internet, program komputer, atau sistem jaringan komputer. Biasanya kejahatan semacam ini dilakukan dengan cara memasukkan logic bomb, seperti virus komputer atau program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak bisa dipakai dan tidak dapat berjalan secara normal atau tidak dapat berjalan, tetapi telah dikendalikan oleh pelaku sesuai kebutuhan.
6. Infringements of privacy, yaitu suatu kejahatan yang menargetkan informasi pribadi yang disimpan dalam formulir data hak milik personal yang tersimpan secara computerized, apabila orang lain mengetahuinya, maka hal itu dapat menyebabkan kerugian terhadap korban secara materiil maupun immaterial, seperti bocornya nomor PIN ATM, dan lainnya.
7. Offense against intellectual property atau (pelanggaran terhadap Hak atas Kekayaan Intelektual), yaitu tindakan kejahatan yang menyasar hak kekayaan intelektual yang dimiliki pihak lain di Internet. Contohnya mempraktikkan tampilan website orang lain secara illegal.

Berdasarkan motif kegiatannya menurut pendapat (Amin & Muslih, 2023), cybercrime dapat digolongkan menjadi beberapa jenis diantaranya sebagai berikut:

1. Cybercrime sebagai tindak kejahatan murni. Kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Misalnya carding: mencuri kode PIN ATM milik orang lain buat digunakan dalam transaksi online di internet, dan pemanfaatan media internet (webserver, mailing list) untuk mengedarkan alat-alat pembajakan. Pengirim e-mail anonim yang bermuatan iklan (spamming) juga dapat dicantumkan dalam contoh kejahatan yang memanfaatkan internet sebagai medianya dan dapat dituntut dengan tuduhan pelanggaran privasi (Liviani, 2020).
2. Cybercrime sebagai tindak kejahatan abu-abu. Pada jenis kejahatan di internet yang termasuk dalam wilayah "abu-abu" cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah probing atau portscanning. Ini adalah sebutan untuk semacam tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari system yang diintai, termasuk sistem operasi yang digunakan, port-port yang ada, baik yang terbuka maupun yang tertutup, dan sebagainya (Eliasta Ketaren). Hal ini sejalan dengan pendapat (Liviani, 2020) Salah satu contohnya adalah probing atau portscanning. Ini adalah istilah yang digunakan untuk memantau sistem orang lain, dan disalahgunakan dengan mengumpulkan informasi sebanyak mungkin dari system.
3. Cybercrime yang menyerang individu (Againts Person). Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Adapun beberapa contoh sasaran kejahatan yaitu Pornografi, Cyberstalking Cyber Tresspass, Cybercrime menyerang hak milik (Againts Property), Cybercrime menyerang pemerintah (Againts Government).

Implikasi Keamanan Nasional terhadap Kejahatan Cyber atau Cybercrime

Kejahatan Cyber memilki dampak yang sangat luas baik bagi individu, perusahan maupun negara. Menurut pendapat (Wati et al., 2024) Implikasi kejahatan cyber crime dapat mengganggu keamanan nasional dalam berbagai unsur, yaitu sebagai berikut:

1. Menargetkan Infrastruktur Kritis. Cyber crime bisa melumpuhkan infrastruktur kritis seperti jaringan listrik, air, dan transportasi, yang dapat menimbulkan kekacauan dan kerusakan yang fatal. Contohnya, yang terjadi di tahun 2017, munculnya serangan WannaCry ransomware melumpuhkan komputer di rumah sakit, bank, dan perusahaan di seluruh dunia. Gangguan pada infrastruktur kritis tersebut bisa mengganggu keselamatan umum, merusak perekonomian, hingga memicu konflik sosial.
2. Mencuri Data Sensitif. Cyber crima bisa mencuri data sensitif seperti data pemerintah, data keuangan, dan data individu. Data ini dapat dipakai untuk tujuan kriminal seperti penipuan identitas, pemerasan, atau bahkan spionase. Kebocoran data sensitif bisa merusak kepercayaan publik terhadap pemerintah dan institusi, dan menimbulkan berdampak negatif pada reputasi negara di mata internasional.
3. Menyebarkanluaskan Propaganda dan Disinformasi. Cyber crime bisa dimanfaatkan untuk menyebarkanluaskan propaganda dan disinformasi guna adanya kerusuhan sosial, merusak stabilitas politik, dan merusak citra negara. Contohnya seperti yang terjadi di tahun 2016, intervensi siber difitnah dilakukan guna memengaruhi hasil pemilihan presiden Amerika Serikat.
4. Melumpuhkan Layanan Publik. Cyber crime bisa mengurangi layanan publik seperti situs web pemerintah, layanan e-government, dan sistem perbankan. Hal ini bisa mengganggu akses masyarakat kepada layanan penting dan menghambat aktivitas ekonomi. Gangguan

layanan publik dapat mengakibatkan frustrasi dan kemarahan dari masyarakat, dan dapat merusak kepercayaan publik terhadap pemerintah.
5. Mengintimidasi dan Membungkam Suara Kritis. Cyber crime dapat dimanfaatkan untuk mengintimidasi dan membungkam suara kritis, seperti jurnalis, aktivis, dan pembela hak asasi manusia. Hal tersebut mengakibatkan penyusutan ruang publik dan demokrasi, dan dapat menghambat kemajuan sosial.

Dalam Peraturan Menteri Pertahanan Republik Indonesia No. 82 Tahun 2014 tentang Pedoman Pertahanan Siber, menurut pendapat (Saramuke et al., 2025) dijelaskan mengenai beberapa bentuk ancaman siber, yaitu:
1. Advanced Persistent Threats (APT), Denial of Service (DoS), dan Distributed Denial of Service (DDoD) Serangan ini bertujuan untuk membebani kapasitas sistem sehingga mencegah pengguna sah untuk mengakses layanan. Akibatnya, sistem menjadi crash dan tidak dapat beroperasi. Ancaman ini sangat berbahaya bagi organisasi yang sangat bergantung pada internet untuk menjalankan aktivitasnya.
2. Defacement Serangan ini dilakukan dengan mengubah atau memodifikasi halaman web sehingga isi web berubah sesuai dengan motif penyerang.
3. Phising Penyerang dalam serangan ini membuat situs web palsu yang menyerupai situs asli untuk mencuri informasi sensitif, seperti username, password, atau data pribadi lainnya.
4. Malware Merupakan program berbahaya yang mengganggu operasi sistem komputer. Tujuannya dapat berupa keuntungan finansial atau lainnya. Jenis malware yang umum terjadi mencakup virus, ransomware, spyware, dan trojan. Serangan ini sering menyebar melalui perangkat lunak berbahaya atau spam.
5. Penyusupan siber Serangan ini dilakukan dengan berbagai metode untuk mendapatkan akses ilegal ke sistem, seperti menebak password, menggunakan akun yang tidak terlindungi, rekayasa sosial atau berpura-pura menjadi administrator untuk meminta data pribadi, penyadapan komunikasi yang tidak terenkripsi, menggunakan program palsu untuk mencuri kredensial pengguna, serangan brute force atau serangan kamus untuk memecahkan password yang terenkripsi, serta pemantauan aktivitas menggunakan spyware untuk merekam parameter koneksi pengguna.
6. Spam Merupakan pengiriman email massal yang tidak diinginkan dengan tujuan seperti promosi komersial, Penyebaran malware, virus, atau upaya phishing.
7. Penyalahgunaan Protokol Komunikasi, Ancaman Keamanan Siber dan Peran Aktor Non-Negara di Dunia Digital Penyerang memanfaatkan kelemahan protokol komunikasi seperti Transmission Control Protocol (TCP). Salah satu contohnya adalah serangan spoofing nomor port TCP, yang memungkinkan penyerang melewati firewall untuk membuat koneksi antara sistem target dan penyerang.

Upaya pencegahan kejahatan cyber (cybercrime) terhadap keamanan Nasional

Penegkan hukum di Indonesia memiliki peran penting dalam menciptkan strategi pencegahan tehadap kejahatan cyber(cybercrime). Secara keseluruhan, untuk melindungi masyarakat dan perusahaan dari risiko kejahatan teknologi informasi, perubahan regulasi yang cermat dan peningkatan kapasitas lembaga penegak hukum perlu diimplementasikan seiring dengan upaya pencegahan dan kerjasama lintas sector (Sitompul et al., 2024). Pencegahan dan pengendalian dengan baik, terutama di lingkungan pemerintah dan lembaga terkait, serta dengan sinergi non-pemerintah merupakan tanggung jawab kita bersama(Irawati et al., 2021). Menurut pendapat (Irawati et al., 2021) Paradigma keamanan nasional bergerak ke sisi yang lebih luas, termasuk perlindungan warga negara. Tugas utama

negara adalah memberikan ketenangan pikiran bagi warga negara, termasuk pencegahan berbagai kejahatan dunia maya. Penghuni selalu dapat merasa bahwa properti mereka berada di bawah ancaman. Kebijakan keamanan sistem informasi yang paling penting adalah sistem hukum nasional berupa hukum siber, yang mengatur tindakan siber seperti sanksi untuk tindakan jahat dan merugikan. Pemantauan hukum Internet telah berkembang relatif baru-baru ini. Tindak pidana cybercrime memakan korban dengan jumlah sangat besar, terutama dari segi finansial. Selain itu menurut pendapat (Liviani, 2020) Adapun beberapa pencegahan yang dapat dilakukan terhadap kejahatan cyber atau cybercrime yaitu berupa:

1. Educate user (memberikan pengetahuan baru tentang Cyber Crime dan dunia internet)
2. Use hacker's perspective (menggunakan pemikiran hacker untuk melindungi sistem anda)
3. Patch system (menutup lubang-lubang kelemahan pada sistem)
4. Policy (menetapkan kebijakan dan aturan untuk melindungi sistem Anda dari orang-orang yang tidak berwenang)
5. IDS (Intrusion Detection System) bundled with IPS (Intrusion Prevention System)
6. Firewall
7. Anti Virus.

Selain itu, Penegakan UUD 1945 yang tepat menjadi peran utama dalam mencapai tujuan tersebut khususnya untuk mencegah kejahatan cyber crime (Wati et al., 2024). Penegakan hukum perlu ditingkatkan dengan penguatan kapasitas, baik melalui pelatihan dan pendidikan bagi petugas penegak hukum maupun dengan menyusun undang-undang yang tepat sesuai dengan perkembangan teknologi dan tren cyber crime yang baru. Beberapa landasan hukum KUHP yang digunakan oleh apparat penegak hukum adalah pasal 167 KUHP; Pasal 406 ayat 1 KUHP; Pasal 282, pasal 378, pasal 112, pasal 362 dan pasal 372 KUHP. Selain Undang- Undang pidana, tentunya ada Undang-Undang terkait hal ini, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang di dalamnya diverifikasi bahwa aturan tindak pidana yang terjadi mengancam pengguna internet (Wati et al., 2024).

KESIMPULAN

Berdasarkan hasil penelitian dapat disimpulkan sebagai berikut:

1. Kejahatan cyber atau cybercrime adalah suatu tindakan atau ancaman yang nyata dan terus berkembang seiring kemajuan teknologi berkaitan dengan komputer maupun perangkat jaringan, biasanya kejahatan ini dilakukan secara online. Kejahatan ini mencakup berbagai jenis aktivitas kriminal, seperti peretasan (hacking), pencurian data, penipuan online, penyebaran virus, dan eksploitasi kelemahan sistem keamanan.
2. Motif kejahatan cyber atau cybercrime terhadap keamanan Nasinoal yaitu motif individu,ekonomi,politik dan Kriminal. Motif pelaku dalam melakukan kejahatan ini di samping karena uang tetapi juga iseng. Adapun motif berdasarkan pada kegiatannya Adapun motif berdasarkan pada kegiatannya seperti Cybercrime sebagai tindak kejahatan murni, Cybercrime sebagai tindak kejahatan abu-abu, Cybercrime yang menyerang individu (Againts Person).
3. Implikasinya yang dapat berdampak terhadap keamanan nasinoal yaitu menargetkan infrastruktur kritis, mencuri data sensitif, menyebarkanluaskan propaganda dan disinformasi, melumpuhkan layanan publik, mengintimidasi dan membungkam suara kritis.
4. Upaya pencegahan yang harus dilakukan dalam penanggulangan kejahatan cyber atau cybercrime terhadap keamanan nasioanl yaitu Untuk melindungi keamanan nasional dari

kejahatan cyber, penegak hukum harus memperkuat kerja sama internasional dan mengembangkan kapasitas untuk secara efektif dalam mendeteksi, menyelidiki, dan menuntut pelaku kejahatan cyber atau cybercrime. Penegakan hukum di Indonesia dapat memainkan peran penting dalam menciptakan strategi penanggulangan terhadap kasus tersebut.

DAFTAR PUSTAKA

Amin, S., & Muslih, M. (2023). Karakteristik cybercrime di indonesia. *EduLaw : Journal of Islamic Law and Yurisprudance*, *5*(2), 15–26.

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum*, *1*(1), 1–11. https://doi.org/10.56457/jjih.v1i1.38

Atara, I., Syallomeita, S., Raffi, A., & Baihaqi, H. (2025). Analisis Kriminologi Terhadap Pencurian Data Pribadi Di Era Digital: Studi Kasus Kebocoran Data Pengguna Aplikasi Mypertamina Tahun 2023. *KAMPUS AKADEMIK PUBLISHER Jurnal Ilmiah Penelitian Mahasiswa*, *3*(2), 129–140.

Ghozali, M., Liana, N., Afra, C., Siregar, Z., Nurfahni, N., Malahayati, M., & Hatta, M. (2024). Kejahatan Siber (Cyber Crime) dan Implikasi Hukumnya : Studi Kasus Peretasan Bank Syariah Indonesia (BSI). *CENDEKIA: Jurnal Hukum, Sosial & Humaniora*, *2*(4), 797–809.

Ginanjar Laksana, T., & Mulyani, S. (2024). Faktor-Faktor Mendasar Kejahatan Siber Terhadap Kemanusiaan. *Jurnal Hukum Prioris*, *11*(2), 136–160. https://doi.org/10.25105/prio.v11i2.18960

Irawati, A., Fadholi, H. B., Alamsyah, A. N., Dwipayana, D. P., & Moh, M. (2021). Urgensi Cyber Law Dalam Kehidupan Masyarakat Indonesia Di Era Digital. *Proceeding of Conference on Law and Social Studies*.

Khamzina, B., Roza, N., Zhussupbekova, G., Shaizhanova, K., Aten, A., & Meirkhanovna, B. A. (2022). Determination of Cyber Security Issues and Awareness Training for University Students. *International Journal of Emerging Technologies in Learning*, *17*(18), 177–190. https://doi.org/10.3991/ijet.v17i18.32193

Liviani, M. R. H. (2020). *Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia*. *23*(2).

Mudjiyanto, B., Launa, & Leonardi, A. (2024). Cybercrime, Perlindungan Data Warga Negara, dan Integritas Pemilu. *Jurnal Oratio Directa*, *5*(2), 1058–1085.

Nugraha, A. A., Lukitaningtyas, Y. K. R. D., Ridho, A., Wulansari, H., & Al Romadhona, R. A. (2022). Cybercrime, Pancasila, and Society: Various Challenges in the Era of the Industrial Revolution 4.0. *Indonesian Journal of Pancasila and Global Constitutionalism*, *1*(2), 307–390. https://doi.org/10.15294/ijpgc.v1i2.59802

Prasetiyo, P., & Mukhtar, Z. (2020). *Penegakan Hukum oleh Aparat Penyidik Cyber Crime dalam Kejahatan Dunia Maya (Cyber Crime) di Wilayah Hukum Polda DIY*. *1*(2), 79–88. https://doi.org/10.18196/ijclc.v1i2.9611

Saramuke, S. S., Putri, V. A., Sormin, A. M., & Muthia, N. (2025). Ancaman Keamanan Siber dan Peran Aktor Non-Negara di Dunia Digital. *JOURNAL SYNTAX IDEA*, *6*(02), 141–152.

Sitompul, F., Petrus, A., Manik, P., Sinaga, C. D., Purba, A. T., Satria, A., Hukum, F., & Area, U. M. (2024). *Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Hukum Indonesia*. *2*(2), 222–228.

Tamhidah, M. A. R. (2023). Pengaruh Media Sosial Terhadap Penyebaran Informasi Palsu Dan Kejahatan Siber. *Innovative: Journal Of Social Science Research*, *3*(6), 9133–9147.

https://j-innovative.org/index.php/Innovative/article/view/7197/5176

Umbara, A., & Setiawan, D. A. (2022). *Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19*. 81–88.

Wati, D. S., Nurhaliza, S., Sari, M. W., & Amallia, R. (2024). Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum. *Jurnal Bevinding*, *2*(1), 44–55.

Yuhandra, E., Akhmaddhian, S., & Fathanudien, A. (2021). Tindak Pidana Cyber dan Dampak Penggunaan Media Sosial. *Empowerment : Jurnal Pengabdian Masyarakat*, *4*(02), 149–155. https://doi.org/10.25134/empowerment.v4i02.4659