Jupiter: Publikasi Ilmu Keteknikan Industri, Teknik Elektro dan Informatika
Vol.2, No.1 Januari 2024
e-ISSN: 3031-349X; p-ISSN: 3031-500X, Hal 179-189
DOI : https://doi.org/10.61132/jupiter.v2i1.68

Penyalahgunaan Teknologi Komputer untuk Tindakan Kriminal Siber dalam Novel Simvlacrm Karya Cassandra & Noorca Marendra Massardi

Awang Ihtisyamuddin
Universitas Teknologi Yogyakarta

Fauzi Hartanto
Universitas Teknologi Yogyakarta

Eva Dwi Kurniawan
Universitas Teknologi Yogyakarta

Alamat: Jl. RingRoad Utara, Mlati Krajan, Sumberadi, Kec. Mlati, Kab. Sleman
Korespondensi penulis: eva.dwi.kurniawan@staff.uty.ac.id

Abstract: *This research aimed to explore information related to the misuse of computer technology for criminal activities in the novel Simvlacrm by Cassandra & Noorca Marendra Massardi. With the goal of preventing similar cybercriminal actions in real life, this research employed a descriptive method, involving activities such as reading, analyzing, and writing key points from the literary work. The primary findings encompass the misuse of computer technology as a tool for cybercrime, particularly in the forms of hoaxes and wiretapping. It is anticipated that this research will contribute to a deeper understanding of the potential risks of computer technology to cybersecurity.*

Keywords: *Cybercrime, Hoax, Hacking, Computer Technology, Literature*

Abstrak. Penelitian ini bertujuan untuk menggali informasi terkait penggunaan teknologi komputer yang disalahgunakan untuk tindakan kriminal dalam novel *Simvlacrm* karya Cassandra & Noorca Marendra Massardi. Dengan tujuan pencegahan terhadap tindakan kriminal siber sejenis di kehidupan nyata, penelitian ini menggunakan metode deskriptif, melibatkan kegiatan membaca, menganalisis, dan menulis poin penting dari karya sastra tersebut. Temuan utama mencakup penyalahgunaan teknologi komputer sebagai alat untuk melakukan kejahatan siber, khususnya dalam bentuk hoaks dan penyadapan. Penelitian ini diharapkan dapat memberikan kontribusi dalam pemahaman lebih lanjut tentang potensi risiko teknologi komputer terhadap keamanan siber.

Kata kunci: *Cybercrime*, *Hoax*, *Hacking*, Teknologi Komputer, Sastra

LATAR BELAKANG

Kejahatan adalah tindakan melanggar aturan yang dilakukan oleh seseorang atau kelompok. Pada zaman ini, kejahatan dapat dibagi menjadi dua kategori, yaitu kejahatan dunia nyata dan kejahatan dunia maya. Dunia maya merujuk pada lingkungan digital atau virtual, di mana kejahatan dapat terjadi dengan tingkat keparahan yang bahkan dapat melebihi kejahatan di dunia nyata.

Kejahatan merupakan delik hukum, yakni peristiwa-peristiwa yang berlawanan atau bertentangan dengan asas-asas hukum yang hidup di dalam keyakinan hidup manusia dan terlepas dari undang-undang (Bawengan, 1974: 22).

Received Desember 07, 2023; Accepted Januari 08, 2024; Published Januari 31, 2024
* Eva Dwi Kurniawan, eva.dwi.kurniawan@staff.uty.ac.id

Contoh kasus kejahatan dunia maya termasuk penyebaran informasi palsu, atau yang lebih dikenal dengan istilah "*hoax*," yang sering kali berujung pada tindakan fitnah. Pelaku kejahatan siber, atau yang dikenal dengan istilah *cybercrime*, cenderung menggunakan berbagai cara dengan maksud untuk mendapatkan popularitas atau perhatian publik.

Pengertian *cybercrime* merupakan setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, dan komputer sebagai sasaran (Widodo, 2013:22).

Kejahatan siber dapat menargetkan siapa saja yang terhubung dalam jaringan internet. Ancaman yang terjadi dapat berupa pencurian informasi, pemerasan, pembajakan, dan lain-lain. Motivasi serangan siber pun beragam, tergantung pada kelompok ancamannya. Kelompok ancaman siber dapat dikategorikan ke dalam *hacktivist*, *cybercriminal*, dan aktor negara (Amarullah, 2021:18).

Dengan topik tersebut, kami menulis jurnal ini dengan kemampuan analisis berdasarkan apa yang terjadi pada novel *Simvlacrm* karya Cassandra Massardi & Noorca Marendra Massardi.

Kejahatan dunia maya semakin mengglobal seiring dengan perkembangan teknologi informasi. Fenomena ini menjadi tantangan serius bagi penegak hukum dan pemerintah di seluruh dunia. Kejahatan siber tidak mengenal batas negara, dan pelaku dapat dengan mudah menyusup ke sistem komputer di berbagai belahan dunia. Oleh karena itu, kerja sama internasional dalam penanggulangan kejahatan siber menjadi sangat penting agar dapat menghadapi ancaman tersebut secara efektif.

Kejahatan siber tidak hanya merugikan individu atau perusahaan, tetapi juga dapat berdampak serius pada keamanan nasional suatu negara. Serangan siber yang ditujukan pada infrastruktur kritis, seperti listrik, air, atau sistem keuangan, dapat menyebabkan kerusakan besar dan mengancam stabilitas suatu negara. Oleh karena itu, perlindungan terhadap infrastruktur kritis menjadi fokus utama dalam upaya pencegahan dan penanggulangan kejahatan siber.

Salah satu aspek menarik dari kejahatan dunia maya adalah berkembangnya pasar gelap digital. Di dalamnya, berbagai jenis data pribadi, kartu kredit, dan bahkan senjata digital dapat diperoleh dengan mudah. Fenomena ini menimbulkan

kekhawatiran akan potensi penyalahgunaan data dan menyulitkan penegakan hukum dalam melacak dan menangkap pelaku kejahatan siber.

Peran masyarakat dalam melawan kejahatan dunia maya juga semakin penting. Kesadaran akan risiko kejahatan siber perlu ditingkatkan, dan edukasi mengenai praktik keamanan digital menjadi kunci dalam melindungi diri dari ancaman tersebut. Selain itu, laporan tindakan mencurigakan atau serangan siber yang terdeteksi dapat membantu penegak hukum dalam mengidentifikasi dan menangkap pelaku kejahatan dunia maya.

Hukum dan regulasi terkait kejahatan siber perlu terus diperbaharui dan disesuaikan dengan perkembangan teknologi. Dalam hal ini, kerja sama antara sektor publik, swasta, dan akademisi sangat penting untuk menciptakan lingkungan hukum yang responsif dan efektif. Upaya ini dapat mencakup pembentukan tim penanggulangan kejahatan siber, pelatihan tenaga ahli, dan perumusan kebijakan yang mendukung penanganan kejahatan dunia maya secara holistik.

KAJIAN TEORITIS

Kajian teoritis dalam penelitian ini mencakup tinjauan terhadap teori-teori yang relevan dengan fenomena kejahatan siber, khususnya dalam konteks penyebaran berita hoaks dan tindakan penyadapan di dunia maya. Perkembangan teknologi informasi yang pesat membawa implikasi serius terhadap keamanan siber, membuka celah untuk berbagai tindakan kriminal yang dapat merugikan pihak lain.

Salah satu teori yang relevan dalam konteks kejahatan siber adalah teori "*Routine Activity*" yang dikemukakan oleh Cohen dan Felson (1979:589). Teori ini mengemukakan bahwa kejahatan terjadi ketika ada konvergensi dari tiga elemen, yaitu motivasi pelaku, target yang rentan, dan ketiadaan pengawasan. Dalam konteks kejahatan siber, teori ini dapat diaplikasikan dengan melihat motivasi pelaku kejahatan siber, kerentanan sistem keamanan, dan tingkat pengawasan dalam lingkungan digital.

Selain itu, teori "*Social Learning*" juga relevan untuk memahami perilaku pelaku kejahatan siber. Teori ini menekankan bahwa individu belajar melalui interaksi sosial dan pengaruh dari lingkungan sekitarnya. Dalam dunia maya, pengaruh dari teman sebaya, kelompok, dan lingkungan digital dapat memainkan peran penting dalam membentuk perilaku penyebaran berita hoaks dan tindakan penyadapan.

Beberapa penelitian sebelumnya yang relevan dengan topik ini telah memberikan kontribusi penting. Penelitian terdahulu menyoroti dampak sosial dari penyebaran berita hoaks dan menggambarkan bagaimana informasi palsu dapat merusak kepercayaan masyarakat. Studi kasus oleh Johnson et al mengidentifikasi motif di balik tindakan penyadapan dan memperlihatkan bagaimana celah keamanan dalam infrastruktur teknologi dapat dimanfaatkan oleh pelaku kejahatan siber.

Dengan merujuk pada kerangka teoritis dan penelitian terdahulu, penelitian ini diarahkan untuk mengeksplorasi lebih lanjut tentang karakteristik dan dinamika dari penyebaran berita hoaks serta tindakan penyadapan di dunia maya, dengan tujuan memberikan kontribusi pada pemahaman dan upaya pencegahan terhadap kejahatan siber.

METODE PENELITIAN

Berdasarkan uraian permasalahan yang telah dijabarkan, kami sebagai peneliti menjalankan penelitian dengan menggunakan metode deskriptif. Pemilihan metode ini dipertimbangkan karena sumber informasi yang kami manfaatkan bersumber dari karya sastra berupa novel. Dalam melakukan analisis terhadap novel, kami menerapkan teknik membaca keseluruhan novel, kemudian mencatat poin-poin penting, dan melakukan analisis terperinci terhadap setiap poin yang dianggap signifikan. Sebagai hasil dari penelitian yang kami lakukan, kami menyusun jurnal ini untuk mengungkapkan temuan analisis terhadap poin-poin penting yang telah diidentifikasi.

HASIL DAN PEMBAHASAN

Dengan kemajuan teknologi pada zaman sekarang, semua pihak dapat mengakses internet dengan mudah dan cepat di mana saja dan kapan saja. Internet memiliki aspek positif dan negatif. Sebagai contoh, terdapat penyebaran berita bohong yang dikenal dengan istilah "*hoax*" dan upaya penyadapan perangkat komputer untuk melakukan manipulasi atau mengeksploitasi kesalahan manusia dengan tujuan memperoleh akses ke informasi pribadi dan data berharga.

Penyebaran berita dalam dunia maya atau internet berlangsung dengan cepat dan dapat diakses oleh siapa pun. Sehingga, siapa pun dapat mengakses internet dengan mudah melalui ponsel, komputer, dan perangkat pintar lainnya. Berita yang tersebar di

dunia maya sangat mudah ditemukan di internet. Namun, perlu diwaspadai bahwa beberapa berita yang tersebar di internet terdapat beberapa berita yang tidak valid karena adanya campur tangan pihak tidak bertanggung jawab yang menyalahgunakan informasi tersebar demi kepentingan individu maupun kelompok.

Terdapat pula kejahatan siber lain yaitu tindakan penyadapan. Penyadapan atau intersepsi adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan atau mencatat transmisi informasi elektronik dan atau Dokumen elektronik yang bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti elektromagnetis atau Radio (Pasal 31 Ayat (1) Undang-Undang Nomor 11 Tahun 2008). Tindakan penyadapan biasanya dilakukan oleh seseorang atau kelompok dengan tujuan memperoleh informasi rahasia.

Bentuk *cybercrime* dalam novel *Simvlacrm* karya Cassandra Massardi & Noorca M. Massardi berupa *hoax* dan penyadapan. Menurut Moore (2005:2) *Cybercrime* atau kejahatan berbasis komputer, adalah kejahatan yang melibatkan komputer dan jaringan (*network*).

Cybercrimes dapat didefinisikan sebagai Pelanggaran yang dilakukan terhadap individu atau sekelompok orang dengan niat kriminal untuk sengaja merusak reputasi atau menyebabkan kerugian fisik, mental, atau materi menggunakan teknologi komunikasi modern seperti Internet, telepon genggam atau perangkat sejenis. Ini mencakup tindakan *cyberbullying* yang melibatkan penyebaran informasi palsu, penghinaan daring, pencemaran karakter, pencurian identitas, ancaman, dan pelecehan seksual secara daring. Kejahatan dunia maya ini dapat memiliki dampak serius, termasuk kerugian mental dan emosional, serta merugikan reputasi korban. Berikut merupakan bentuk kejahatan siber pada menurut novel *Simvlacrm* karya Cassandra Massardi & Noorca Marendra Massardi.yang akan dipaparkan di bawah ini.

Hoax

Ketika kita melakukan browsing di internet, dengan mudahnya kita dapat mengakses semua informasi yang tersedia. Karena terlalu mudahnya semua orang mengakses internet, kita pasti akan mendapati kejahatan criminal siber dengan memalsukan sebuah kabar atau berita yang sering kita sebut sebagai berita bohong atau *hoax*. *Hoax* dalam novel Cassandra Massardi & Noorca Marendra Massardi digambarkan dipakai sebagai alat untuk menjatuhkan reputasi mulai dari politisi,

pejabat sipil, pejabat militer, pihak kepolisian, aparat pemerintahan, pengusaha swasta, pesohor, dan calon pesohor.

"Sekali hoaks, dua tiga tujuan terlampau," (Cassandra & Noorca, 2023:26).

Teks sebelumnya menjelaskan bahwa Aline merupakan tokoh yang memiliki tanggungan kebutuhan harian dan masalah keuangan, sebab ia memiliki sejumlah hutang serta tanggungan untuk biaya suster yang merawat ibunya di Kampung. Sehingga ia bekerja sebagai karyawati di perusahaan illegal yang memproduksi hoaks dan fitnah sesuai pesanan oknum yang order. Dengan orderan dari oknum tersebut Aline mendapatkan bonus dari pelbagai iklan yang masuk. Dengan begitu Aline memang sengaja ingin mengejar sebanyak mungkin *viewers* dengan berbagai karya hoaks yang Aline ciptakan. Oleh sebab itu Aline selalu mengucapkan slogannya karena itu yang Aline inginkan, dengan satu hoaks yang Aline ciptakan, dua tiga tujuan untuk mendapatkan uang dan pemenuhan kebutuhan bisa tercapai.

Kasus hoaks sendiri memang sering dijumpai, bahkan beberapa kasus sempat menggegerkan public. Pada tahun 1983, sebuah majalah mingguan Jerman bernama Stern, membeli 60 volume jurnal yang dipercaya milik Adolf Hitler seharga US$ 5,5 juta dan mempublikasikannya. Menurut Gerd Heidemann, yang merupakan seorang wartawan dari Majalah Stern buku harian tersebut tersebut didapatkan dari bangkai pesawat yang mengangkut barang pribadi dari pemimpin Nazi tersebut, di dekat Kota Dresden, Jerman, pada bulan April 1945. Catatan harian itu diklaim telah melewati uji tulisan tangan, dan berdasarkan sampel isinya, dinyatakan akurat secara historis. Namun selang beberapa minggu kemudian Badan Arsip Federal Jerman menyatakan jika buku harian tersebut palsu. Karena catatan sejarah yang terdapat dalam buku itu tidak akurat dan pada zaman Hitler hidup, tinta pena belum ditemukan dan kertas yang dipakai untuk menulis berasal dari masa modern (Dian, 2018).

Hoax tidak hanya menjadi isu dalam lingkup nasional, tetapi juga dalam arena politik global. Serangan siber yang menggunakan berita palsu dapat menjadi senjata ampuh dalam memengaruhi opini publik dan mengubah arah politik suatu negara. Kasus-kasus di berbagai negara menunjukkan bagaimana kejahatan siber dapat digunakan untuk memanipulasi proses demokrasi dan menciptakan ketidakstabilan politik.

Dalam era media sosial, penyebaran *hoax* menjadi semakin masif dan cepat. Fitur-fitur berbagi dan komentar di platform-platform seperti Facebook, Twitter, dan WhatsApp memungkinkan informasi palsu menyebar dengan sangat luas. Hal ini menimbulkan tantangan baru dalam memerangi kejahatan siber, karena penyebaran *hoax* dapat terjadi tanpa kendali dan dengan sangat cepat, menciptakan dampak yang signifikan pada masyarakat.

Selain dampak politik, kejahatan siber juga memberikan kontribusi terhadap ketidakpercayaan masyarakat terhadap media. Ketika berita palsu dengan mudahnya tersebar, masyarakat dapat kesulitan membedakan antara informasi yang benar dan hoaks. Ini dapat merusak integritas jurnalisme dan melemahkan kepercayaan masyarakat terhadap sumber informasi.

Kejahatan siber tidak hanya dilakukan oleh individu atau kelompok tertentu, tetapi juga dapat melibatkan negara atau pihak-pihak yang memiliki kepentingan politik tertentu. Serangan siber yang dilakukan oleh negara-negara tertentu dapat mencakup operasi pengintaian, sabotase, atau kampanye propaganda yang bertujuan untuk menciptakan ketidakstabilan di negara-negara lain.

Upaya pencegahan dan penanggulangan kejahatan siber memerlukan kerja sama lintas sektor. Peran lembaga pemerintah, sektor swasta, akademisi, dan masyarakat sipil menjadi kunci dalam mengatasi tantangan keamanan digital. Pembentukan tim keamanan *cyber*, pelatihan bagi tenaga ahli keamanan, dan kampanye edukasi publik dapat menjadi langkah-langkah penting dalam melawan kejahatan siber dan mengurangi dampaknya pada masyarakat.

Penyadapan

Penyadapan merupakan suatu tindakan yang tidak terpuji karena dapat merugikan pihak yang tidak bersalah. Mengutip *Convention on Cyber Crime*. Penyadapan atau *llegal access / Unauthorized Access to Computer System and Service*. (Akses tidak sah ke sistem komputer dan jasa), adalah suatu bentuk kejahatan yang dilakukan dengan cara meretas atau memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, atau tanpa izin atau tanpa sepengetahuan dari si pemilik *system* jaringan komputer yang dimasukinya (Antoni, 2017: 261-274). Tindakan *criminal cyber* yaitu penyadapan yang terjadi pada novel *Simvlacrm*

Cassandra Massardi & Noorca M. Massardi adalah ketika sebuah panggilan yang masuk ke ponsel pintar Tiara.

"Kalau benar, nomor di teleponmu itu mungkin sudah dibuang tiga bulan lalu untuk menghindari penyadapan," (Cassandra & Noorca, 2023:42).

Percakapan tersebut merupakan penjelasan pada paragraf sebelumnya yaitu ponsel pintar milik Tiara menerima panggilan yang sempat ia kira merupakan panggilan dari komandannya, Brigjen Polisi Danumerta. Tiara mendapatkan perintah untuk menghadap komandannya, dari panggilan tersebut Tiara diminta untuk turun dari kantor DACC-Sus yang berada dilantai paling atas untuk ke lantai bawah, kantor Komandan Danumerta gedung kepolisian.

Tujuan penyadapan pada nomor komandan Danumerta merupakan pengalihan tersangka supaya pelaku pengeboman yaitu pasukan ACA (*Amin Cyber Army*) dapat memasuki area kantor DACC-Sus. Upaya penyadapan tersebut berhasil dengan masuknya pelaku yang menyamar sebagai tukang antar pizza yang saat itu sempat berpapasan dengan Tiara tepat saat Tiara keluar dari lift. Pengantar pizza tersebut merupakan pembawa bom yang menjadi penyebab terjadinya ledakan di kantor DACC-Sus. Bukti keberhasilan dari tindakan tersebut yaitu tertulis dalam paragraph.

"Ketika itulah tubuh Tiara tiba-tiba terhuyung, bersamaan dengan terdengarnya suara dentuman keras. Ia merasakan guncangan di dalam lift. Seperti ada gempa bumi. Pada detik berikutnya, lampu lift mati. Saluran listrik di seluruh gedung putus mendadak. Kemudian, terdengar bunyi alarm." (Cassandra & Noorca, 2023:6).

Pada teks di atas menjelaskan keadaan Tiara yang sedang menuju lantai atas menggunakan lift, Tiara merasakan sebuah goncangan dan mendengar suara ledakan pada saat di dalam lift. Lift tersebut berhenti setelah ledakan itu terjadi karena ledakan tersebut menyebabkan semua listrik pada gedung terputus atau mati.

Mengenai peristiwa penyadapan, pada awal kemunculan internet, pemrogram komputer Rusia Vladimir Levin berhasil mencuri 10 juta dolar AS, namun tidak secara online. Levin meretas sistem telepon Citibank dan mencuri kredensial akun, yaitu kata sandi dan nomor rekening dari pelanggan saat mereka mengatakannya dengan keras kepada perwakilan layanan. Levin kemudian menggunakan kredensial tersebut untuk mentransfer jutaan dolar secara elektronik ke berbagai akun di seluruh dunia. Dia akhirnya ditangkap, dijatuhi hukuman tiga tahun penjara, dan semua kecuali 400.000

dolar AS dipulihkan. Ini menjadi salah satu aksi pencurian elektronik publik dan profil tinggi pertama dari lembaga keuangan (Purnama, 2022).

Penyadapan, selain menjadi ancaman dalam ranah *cybercrime*, juga seringkali terjadi dalam konteks mata-mata dan intelijen. Negara-negara sering menggunakan teknik penyadapan untuk mendapatkan informasi rahasia dari negara lain. Hal ini menciptakan kompleksitas dan tantangan baru dalam diplomasi internasional, di mana kegiatan penyadapan dapat memicu konflik antarnegara. Dalam kasus novel *Simvlacrm* Cassandra Massardi & Noorca M. Massardi, tindakan penyadapan pada panggilan Tiara menunjukkan bahwa keamanan siber tidak hanya relevan di dunia maya tetapi juga dapat memiliki dampak nyata dalam kehidupan sehari-hari.

Keberhasilan tindakan penyadapan dalam novel *Simvlacrm* menyoroti kelemahan dalam sistem keamanan yang ada. Hal ini menciptakan kebutuhan mendesak untuk meningkatkan keamanan siber dalam segala aspek kehidupan, baik di tingkat pribadi, bisnis, maupun pemerintahan. Perkembangan teknologi harus diiringi dengan peningkatan keamanan dan perlindungan data agar masyarakat dapat menggunakan teknologi dengan aman dan tanpa takut menjadi korban penyadapan atau kejahatan siber lainnya.

Kasus penyadapan pada novel juga memberikan gambaran bahwa tindakan kriminal di dunia maya tidak hanya dilakukan oleh individu atau kelompok tertentu, tetapi juga dapat melibatkan elemen organisasi atau kelompok tertentu dengan tujuan tertentu. Keberadaan *Amin Cyber Army* (ACA) dalam novel sebagai pelaku pengeboman yang berhasil masuk melalui penyadapan menunjukkan kompleksitas dan profesionalisme kelompok-kelompok kejahatan siber, memerlukan penanganan serius dari aparat penegak hukum dan keamanan.

Dampak sosial dari tindakan penyadapan dapat melampaui kerugian finansial atau kerusakan fisik. Kepercayaan masyarakat terhadap teknologi dan keamanan informasi dapat terkikis, menciptakan atmosfer ketidakpercayaan dan ketidakpastian. Oleh karena itu, perlu adanya upaya pencegahan dan edukasi terhadap masyarakat agar mereka dapat lebih sadar akan risiko penyadapan dan mengambil langkah-langkah untuk melindungi diri mereka sendiri secara proaktif.

Pengalaman kasus penyadapan sepanjang sejarah, seperti yang dialami Citibank oleh Vladimir Levin, memberikan pelajaran berharga untuk mengembangkan strategi

keamanan *cyber* yang lebih efektif. Studi kasus seperti ini membantu para profesional keamanan siber dan penegak hukum untuk memahami metode dan taktik yang digunakan oleh pelaku kejahatan siber sehingga mereka dapat merancang sistem keamanan yang lebih tangguh dan responsif terhadap ancaman yang berkembang.

KESIMPULAN DAN SARAN

Melalui kajian teoritis dan penelitian ini, dapat disimpulkan bahwa fenomena kejahatan siber, terutama dalam penyebaran berita hoaks dan tindakan penyadapan di dunia maya, merupakan dampak langsung dari kemajuan teknologi informasi. Berbagai teori seperti *"Routine Activity"* dan *"Social Learning"* memberikan pemahaman mendalam terhadap faktor-faktor yang memengaruhi terjadinya kejahatan siber. Penelitian ini menghadirkan kontribusi dalam memahami karakteristik dan dinamika dari dua jenis kejahatan siber tersebut.

Penyebaran berita hoaks memiliki dampak serius terhadap kepercayaan masyarakat dan memerlukan upaya bersama dalam meningkatkan literasi digital dan kritis. Sementara itu, tindakan penyadapan, seperti yang diilustrasikan dalam novel *Simvlacrm*, menunjukkan kompleksitas tantangan keamanan siber, di mana upaya pencegahan harus lebih diperkuat.

Keterbatasan penelitian ini mencakup cakupan yang terbatas pada fenomena kejahatan siber yang diilustrasikan dalam novel tertentu. Oleh karena itu, penelitian selanjutnya dapat memperluas cakupan dengan melibatkan data empiris lebih lanjut dan melibatkan sektor yang lebih luas dalam masyarakat. Rekomendasi untuk penelitian mendatang mencakup pengembangan strategi pencegahan kejahatan siber, kerja sama lintas sektor, dan upaya meningkatkan keamanan siber di tingkat individu dan organisasi.

Secara keseluruhan, penelitian ini memberikan kontribusi pada pemahaman mendalam tentang kejahatan siber dalam konteks penyebaran berita hoaks dan penyadapan. Upaya lanjutan dalam memahami, mencegah, dan menanggulangi kejahatan siber akan menjadi esensial dalam menghadapi kompleksitas dunia maya yang terus berkembang.

DAFTAR REFERENSI

Amarullah, Abdul Hanief. (2021). *Analisis Ancaman Kejahatan Siber Bagi Keamanan Nasional Pada Masa Pandemi COVID-19*.

Antoni. (2017). *Kejahatan Dunia Maya (Cybercrime) dalam Simak Online*. Jurnal Nuraini, 17(2), 261-274.

Bawengan, GW. (1974). *Teknik Interogasi dan Kasus-Kasus Kriminil*. Jakarta: Pradnya Paramita.

Casssandra & Noorca M. Massardi (2023). *Simvlacrm*. Jakarta: Buku Kompas.

Cohen, Lawrence and Felson, M. (1979). *Social change and crime rate trends:A routine activity approach. American Sociological Review* 44, 588-608.

Dian, M. (2018). *5 Kasus Hoax Terbesar di Dunia yang Sempat Dipercaya Publik*. https://journal.sociolla.com/lifestyle/kasus-*hoax*-terbesar-di-dunia-yang-sempat-dipercaya-publik. Diakses pada 16 November 2023 pukul 19:30

Moore, R. (2005). *Cyber Crime: Investigating High-Technology Computer Crime*. Cleveland, Mississippi: Anderson Publishing.

Pemerintah Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 31 Ayat (1).

Purnama, K. I. (2022). *Inilah 5 Aksi Peretasan Terbesar di Dunia*. https://dunia.tempo.co/read/1633137/inilah-5-aksi-peretasan-terbesar-di-dunia. Diakses pada 16 November 2023 pukul 19:00

Widodo. (2013). *Memerangi Cybercrime (Karakteristik, Motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi*. Yogyakarta: Aswaja Presindo.