Technomedia Journal (TMJ)
Vol. 10, No. 3, Februari, 2026, pp. 184∼193
E-ISSN: 2528-6544 | P-ISSN: 2620-3383, DOI: 10.33050

Cyber Threats to Press Freedom Resulting from Media Account Hijacking

Ancaman Siber terhadap Kebebasan Pers akibat Pembajakan Akun Media

Abdul Hamid Arribathi[1], Annisa Ardien[2*], Abdullah Arif Kamal[3]
[1]Faculty of Islamic Education Management, University of Raharja, Indonesia
[2]Master of Informatics Engineering, University of Raharja, Indonesia
[3]Faculty of Economics and Business, Eduaward Incorporation, United Kingdom
[1]abdulhamid@raharja.info, [2]annisa.ardien@raharja.info, [3]abdul.kamal@ilearning.co
***Penulis Korespondensi**

Article Info

Article History:

Penyerahan November 06, 2025
Revisi Februari 05, 2026
Diterima Februari 13, 2026
Diterbitkan Februari 18, 2026

Keywords:
Press Freedom
Cyber Threats
Media Account Hijacking
Digital Journalism
Cybersecurity

Kata Kunci:
Kebebasan Pers
Ancaman Siber
Pembajakan Akun Media
Jurnalisme Digital
Keamanan Siber

ABSTRACT

The development of digital **journalism has expanded** the reach of information distribution, while simultaneously increasing the vulnerability of media organizations and journalists to cyber threats that may undermine press freedom. The hacking case involving Narasi.tv demonstrates that media account hijacking is not merely an individual digital crime, but a form of systemic violence and intimidation that affects journalistic integrity and public trust. This study aims to **analyze the impact** of media account hijacking on press freedom and to develop an applicable technical mitigation framework for digital media organizations. The research **adopts a qualitative** approach using a case study of the Narasi.tv hacking incident, supported by document analysis, reports from journalist organizations, and a review of the literature on cybersecurity and digital journalism. The findings indicate that **collective cyberattacks** generate significant psychological and operational impacts and function as a mechanism to suppress critical journalism. This study proposes a layered mitigation framework consisting of preventive technical mitigation, newsroom operational mitigation, and public communication mitigation. Theoretically, this research extends the study of cyber threats from an individual-level vulnerability toward an institutional and systemic framework. From a managerial perspective, the findings emphasize that **cybersecurity** must be positioned as a strategic agenda in digital media transformation. This study is also aligned with the Sustainable Development Goals, particularly SDG 16, SDG 9, and SDG 4, in supporting the development of a secure, sustainable, and trustworthy digital media ecosystem.

ABSTRAK

Perkembangan jurnalisme digital memperluas jangkauan distribusi informasi, namun sekaligus meningkatkan kerentanan media dan jurnalis terhadap ancaman siber yang dapat mengganggu kebebasan pers. Kasus peretasan Narasi.tv menunjukkan bahwa pembajakan akun media bukan sekadar kejahatan digital individual, melainkan bentuk kekerasan dan intimidasi sistemik yang berdampak pada integritas pemberitaan dan kepercayaan publik. Penelitian ini bertujuan untuk **menganalisis dampak pembajakan** akun media terhadap kebebasan pers serta mengembangkan kerangka teknis mitigasi yang aplikatif bagi organisasi media digital. Metode penelitian menggunakan **pendekatan kualitatif** dengan studi kasus peretasan Narasi.tv, didukung analisis dokumen, laporan organisasi jurnalis, dan kajian literatur terkait keamanan siber dan

jurnalisme digital. Hasil penelitian menunjukkan bahwa **serangan siber kolektif** menimbulkan dampak psikologis dan operasional yang signifikan, serta berfungsi sebagai mekanisme pembungkaman jurnalisme kritis. Penelitian ini mengusulkan kerangka mitigasi berlapis yang mencakup mitigasi teknis preventif, mitigasi operasional redaksi, dan mitigasi komunikasi publik. Secara teoretis, studi ini memperluas kajian ancaman siber dari level individu menuju kerangka institusional dan sistemik. Secara manajerial, temuan menegaskan bahwa **keamanan siber** harus diposisikan sebagai agenda strategis dalam transformasi digital media. Penelitian ini juga relevan dengan *Sustainable Development Goals*, khususnya SDG 16, SDG 9, dan SDG 4, dalam upaya membangun ekosistem media digital yang aman, berkelanjutan, dan berintegritas.

DOI: https://doi.org/10.33050/tmj.v10i3.2563

1. PENDAHULUAN

Dalam era disrupsi digital, jurnalisme menghadapi tantangan yang semakin kompleks. Transformasi digital telah membuka ruang baru bagi penyebaran informasi yang cepat dan luas, namun pada saat yang sama juga menciptakan kerentanan baru bagi jurnalis dan organisasi media. Berbagai bentuk serangan digital, seperti peretasan akun, doxing, dan gangguan layanan, semakin sering terjadi dan berdampak langsung pada kebebasan pers serta keamanan kerja jurnalistik. Kondisi ini menunjukkan bahwa ruang digital tidak hanya menjadi medium produksi berita, tetapi juga medan baru bagi intimidasi dan tekanan terhadap pers [1].

Perkembangan teknologi digital telah mengubah cara media memproduksi dan mendistribusikan informasi, dengan media sosial dan platform digital menjadi kanal utama pemberitaan. Namun, ketergantungan pada teknologi ini membuka celah bagi serangan siber yang menargetkan akun media sosial, surel, dan sistem internal redaksi. Kasus pembajakan akun Narasi.tv pada tahun 2022 menjadi contoh nyata bagaimana serangan siber dapat mengganggu operasional redaksi, merusak independensi pemberitaan, serta mengancam kebebasan pers. Serangan tersebut tidak hanya berdampak pada individu jurnalis, tetapi juga melemahkan kepercayaan publik terhadap institusi media [2].

Peretasan yang menargetkan jurnalis dan kru Narasi.tv terjadi secara masif dan terkoordinasi, melibatkan berbagai platform komunikasi dan akun media. Pola serangan ini menunjukkan bahwa ancaman siber tidak bersifat insidental, melainkan sistematis dan berpotensi digunakan sebagai alat pembungkaman pers, terutama ketika media melakukan liputan terhadap isu-isu sensitif. Kondisi ini menegaskan kerentanan jurnalis dalam ekosistem digital serta perlunya perlindungan data yang lebih kuat, baik dari sisi teknologi, tata kelola platform, maupun penegakan hukum oleh negara [3].

Meskipun ancaman siber terhadap media semakin nyata, kajian akademik di Indonesia masih relatif terbatas dan cenderung berfokus pada isu disinformasi atau hoaks, bukan pada serangan langsung terhadap institusi media dan jurnalis [4]. Oleh karena itu, penelitian ini berupaya mengisi kesenjangan tersebut dengan menganalisis secara mendalam dampak pembajakan akun media terhadap kebebasan pers dan integritas pemberitaan, serta implikasinya bagi keberlanjutan media digital [5].

Penelitian ini juga diharapkan memberikan kontribusi strategis dalam penguatan literasi keamanan digital di kalangan jurnalis dan perumusan strategi mitigasi siber bagi organisasi media. Dalam konteks global, kajian ini relevan dengan agenda *Sustainable Development Goals* (SDGs), khususnya SDG 16 (*Peace, Justice, and Strong Institutions*) melalui upaya perlindungan kebebasan pers dan tata kelola informasi yang akuntabel, SDG 9 (*Industry, Innovation, and Infrastructure*) melalui penguatan infrastruktur digital media yang aman dan berkelanjutan, serta SDG 4 (*Quality Education*) melalui pengembangan kapasitas dan literasi keamanan siber sebagai bagian dari pembelajaran organisasi dan *learning factory* di sektor media digital [6].

2. PERMASALAHAN

Perkembangan jurnalisme digital yang semakin bergantung pada platform media sosial dan sistem daring telah meningkatkan efisiensi produksi serta distribusi informasi, namun sekaligus membuka kerentanan baru terhadap serangan siber. Pembajakan akun media dan jurnalis menjadi salah satu ancaman paling serius

karena tidak hanya menyerang keamanan digital individu, tetapi juga mengganggu operasional redaksi dan independensi pemberitaan. Serangan yang bersifat terkoordinasi berpotensi digunakan sebagai alat intimidasi dan pembungkaman pers, sehingga melemahkan fungsi media sebagai pengawas kekuasaan dan penyalur informasi publik yang kredibel [6, 7].

Di sisi lain, *respons* organisasi media terhadap ancaman siber masih menghadapi berbagai keterbatasan, baik dari aspek literasi keamanan digital, tata kelola teknologi, maupun perlindungan hukum. Kajian akademik yang ada umumnya lebih menyoroti isu disinformasi dan hoaks, sementara analisis terhadap serangan langsung yang menargetkan institusi media masih relatif terbatas [8, 9]. Kondisi ini menimbulkan kesenjangan pemahaman mengenai dampak sistemik pembajakan akun media terhadap kebebasan pers dan integritas pemberitaan, serta kebutuhan akan kerangka mitigasi yang bersifat aplikatif dan berkelanjutan bagi organisasi media digital [10].

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif-deskriptif dengan metode studi kasus. Pendekatan ini memungkinkan peneliti memahami fenomena secara mendalam berdasarkan konteks empiris di lapangan [11]. Adapun prosedurnya, meliputi:

- Pengumpulan data: Data primer dikumpulkan melalui wawancara mendalam dengan jurnalis, editor, dan pakar keamanan siber yang pernah mengalami atau mendokumentasikan kasus pembajakan akun media. Data sekunder diperoleh dari laporan lembaga pers seperti (Aliansi Jurnalis Independen) AJI, pemberitaan media terkait insiden peretasan, dan literatur relevan mengenai ancaman siber terhadap jurnalisme [12].
- Studi kasus: Berfokus pada analisis kasus peretasan yang menimpa Narasi.tv pada September 2022, sebagaimana didokumentasikan oleh AJI Indonesia. Analisis mencakup kronologi serangan, modus operandi, dan *respons* yang diambil oleh pihak media [13, 14].
- Analisis data :Dilakukan pada pemberitaan sebelum dan sesudah insiden pembajakan untuk mengidentifikasi dampak langsung pada narasi. Selain itu, analisis tematik digunakan untuk mengidentifikasi pola-pola ancaman dan konsekuensi yang muncul dari wawancara dan dokumen [15].
- Wawancara Mendalam: Wawancara dilakukan dengan jurnalis dan staf Narasi.tv yang menjadi korban, perwakilan AJI, dan ahli keamanan siber untuk mendapatkan pemahaman mendalam mengenai kronologi, dampak psikologis, dan *respons* yang dilakukan [16].

Adapun obyek penelitian detail kasusnya sebagai berikut:

- Waktu kejadian: Upaya peretasan terdeteksi sejak 26 September 2022, dengan laporan terus bertambah dari para jurnalis dan kru [17].
- Target serangan: Serangan ini menargetkan individu, mencakup peretasan akun media sosial dan aplikasi pesan seperti *WhatsApp*, *Facebook*, *Telegram*, dan *Instagram*. Bahkan, komunikasi internal Narasi juga menjadi sasaran [18, 19].
- Jumlah korban: Hingga 30 September 2022, tercatat 37 jurnalis dan kru Narasi menjadi korban. Angka ini kemudian bertambah menjadi 38 kasus, termasuk peretasan terhadap akun media sosial dan situs utama Narasi.
- Modus operandi: Pelaku mengirimkan tautan (link) berbahaya melalui aplikasi *WhatsApp* kepada para korban. Setelah korban mengklik tautan tersebut, akun mereka diambil alih oleh peretas [20].

4. HASIL DAN PEMBAHASAN

4.1. Modus Operandi Pembajakan Akun Media

Berdasarkan temuan dari studi kasus Narasi.tv, modus operandi pelaku pembajakan akun media umumnya melibatkan teknik rekayasa sosial (*social engineering*). Pelaku mengirimkan tautan atau pesan jebakan melalui platform komunikasi seperti *WhatsApp* atau *Telegram* yang dirancang menyerupai pesan resmi. Ketika

tautan tersebut diakses, pelaku dapat mengambil alih akun korban secara paksa [21]. Serangan yang menargetkan individu jurnalis sering kali menjadi pintu masuk untuk menguasai akun media yang lebih besar. Serangan dimulai pada 26 September 2022, sejumlah jurnalis dan kru Narasi.tv menerima tautan berbahaya melalui *WhatsApp* [22]. Menariknya, meskipun beberapa korban tidak mengklik tautan tersebut, akun mereka tetap berhasil dibajak, yang menunjukkan penggunaan metode serangan yang lebih canggih. Peretasan ini menargetkan berbagai platform, termasuk *WhatsApp*, *Facebook*, *Telegram*, dan *Instagram*, serta berlangsung selama beberapa hari dengan korban puluhan staf redaksi, mulai dari produser hingga reporter [23, 24].

Kasus Narasi.tv memperlihatkan pola serangan yang terkoordinasi dan diikuti dengan upaya penyebaran disinformasi setelah pengambilalihan akun. Pola ini mengindikasikan bahwa serangan siber tidak hanya bertujuan merusak keamanan akun, tetapi juga berpotensi digunakan sebagai instrumen pembungkaman suara kritis [25, 26]. Berdasarkan pola tersebut, penelitian ini mengembangkan sebuah kerangka analitis yang memetakan pembajakan akun media ke dalam tiga lapisan utama, yaitu lapisan teknis, lapisan operasional redaksi, dan lapisan dampak publik [27]. Kerangka ini memungkinkan identifikasi titik kerentanan teknologi, seperti autentikasi akun, keamanan aplikasi pesan, dan manajemen kredensial, sekaligus mengaitkannya dengan gangguan alur kerja jurnalistik serta implikasi terhadap kepercayaan publik. Pendekatan berlapis ini memberikan kontribusi saintifik dengan menjembatani analisis keamanan siber dan studi komunikasi dalam konteks jurnalisme digital [28].

4.2. Dampak Terhadap Kebebasan Pers dan Jurnalis

Menimbulkan dampak signifikan terhadap kebebasan pers karena berfungsi sebagai bentuk intimidasi digital yang menciptakan rasa takut di kalangan jurnalis dan sumber informasi, sehingga memicu efek *chilling* dalam praktik jurnalistik [29, 30]. Di luar pembahasan umum mengenai ancaman siber, penelitian ini memperkenalkan perspektif baru dengan memosisikan pembajakan akun media sebagai bentuk kekerasan digital terstruktur yang menargetkan institusi pers, bukan sekadar individu jurnalis [31, 32]. Serangan yang dilakukan secara terkoordinasi terbukti mengganggu otonomi redaksi, proses pengambilan keputusan editorial, serta kredibilitas institusi media secara simultan. Dimensi kolektif ini membedakan pembajakan akun media dari ancaman siber konvensional dan menempatkannya sebagai mekanisme sistemik pembungkaman pers dalam ekosistem jurnalisme digital [33]. Diantaranya :

- Disinformasi dan Manipulasi: Setelah akun berhasil dibajak, pelaku sering kali mengunggah konten palsu atau menyesatkan yang dapat menyebarkan disinformasi secara instan kepada audiens yang luas. Setelah akun dibajak, pelaku sering menyebarkan konten palsu yang merusak reputasi media [34, 35].
- Gangguan Operasional: Pembajakan akun mengganggu proses produksi berita, merusak infrastruktur digital redaksi, dan memaksa media untuk mengalihkan sumber daya untuk pemulihan, bukan untuk kegiatan jurnalistik. Redaksi harus memulihkan sistem keamanan dan kepercayaan publik yang hilang [36].
- Intimidasi dan Teror Digital: Serangan siber ini menimbulkan ketakutan dan rasa tidak aman di kalangan jurnalis. Kekhawatiran akan doxing atau peretasan lanjutan dapat mendorong jurnalis untuk melakukan sensor diri dan menghindari peliputan isu-isu sensitif, sehingga melemahkan peran pers sebagai pengawas kekuasaan. Jurnalis mengalami tekanan psikologis akibat serangan berulang yang mengancam keselamatan mereka [37].
- Penurunan Kepercayaan Publik: Krisis peretasan menguji kredibilitas Narasi.tv. Peretasan menimbulkan keraguan di kalangan publik mengenai keamanan informasi yang mereka sampaikan kepada media, sehingga berpotensi menurunkan kepercayaan [38].
- Tantangan Hukum dan Kurangnya Perlindungan: Gugatan yang diajukan salah satu produser Narasi.tv terhadap penyedia platform digital menunjukkan tantangan hukum yang signifikan. Ketiadaan Standar Operasional Prosedur (SOP) keamanan siber yang jelas di tingkat media dan lambannya penegakan hukum dalam mengusut kasus ini memperparah kerentanan jurnalis [39, 40].

4.3. Konsekuensi Terhadap Pemberitaan dan Kepercayaan Publik

Peretasan akun media dapat merusak reputasi media dan mengurangi kepercayaan publik. Ketika sebuah akun media yang terpercaya tiba-tiba menyebarkan konten palsu, publik akan mulai meragukan integritas

media tersebut secara keseluruhan [41]. Hal ini menguntungkan pihak-pihak yang berusaha mendiskreditkan pers dan memanipulasi opini publik. Dalam menghadapi krisis, Narasi.tv menunjukkan transparansi kepada publik dengan mengumumkan insiden tersebut dan berkoordinasi dengan organisasi seperti AJI dan tim *respons* cepat. Komunikasi yang proaktif ini bertujuan untuk memulihkan kepercayaan publik dan menunjukkan keseriusan media dalam menangani ancaman tersebut. Kepercayaan publik terhadap media merupakan aset vital dalam demokrasi. Ketika akun resmi media disusupi dan menyebarkan konten menyesatkan, kredibilitas institusi terganggu. Fenomena ini menyebabkan efek domino berupa penurunan kepercayaan terhadap media secara umum [42, 43].

Dalam konteks transformasi digital, temuan ini menegaskan pentingnya kepemimpinan transformasi digital (digital *transformation leadership*) dalam organisasi media. Serangan siber terhadap akun media menunjukkan bahwa keberlanjutan media digital tidak hanya ditentukan oleh kemampuan produksi konten, tetapi juga oleh kapasitas pimpinan redaksi dan manajemen dalam mengelola risiko teknologi, mendorong inovasi berbasis sistem keamanan digital, serta mengintegrasikan tata kelola teknologi ke dalam model bisnis media digital [44, 45]. Dengan demikian, keamanan siber menjadi bagian dari inovasi berbasis teknologi (*tech-driven innovation*) yang mendukung keberlanjutan organisasi pers di era ekonomi digital [46].

Penelitian ini mengusulkan sebuah kerangka kerja mitigasi pembajakan akun media yang bersifat aplikatif dan dapat diimplementasikan oleh organisasi pers digital. Kerangka ini terdiri dari tiga komponen utama. Pertama, mitigasi teknis *preventif*, yang mencakup penerapan autentikasi multi-faktor, segmentasi akses akun redaksi, serta pemantauan aktivitas login secara *real-time*. Kedua, mitigasi operasional redaksi, yaitu penguatan protokol keamanan internal, pelatihan literasi keamanan siber bagi jurnalis, serta prosedur *respons* cepat saat insiden peretasan terjadi [47, 48]. Ketiga, mitigasi komunikasi publik, yang menekankan transparansi media dalam menyampaikan insiden siber kepada publik guna menjaga kepercayaan dan integritas institusi pers. Secara teoretis, penelitian ini berkontribusi dengan memperluas kajian ancaman siber dalam jurnalisme dari pendekatan individual dan teknis menuju kerangka institusional dan sistemik. Dengan memosisikan pembajakan akun media sebagai bentuk kekerasan digital terstruktur, studi ini mengintegrasikan perspektif keamanan siber, tata kelola organisasi, dan teori kebebasan pers dalam satu kerangka analitis. Kontribusi ini memperkaya literatur jurnalisme digital dengan menjembatani studi komunikasi, manajemen teknologi, dan transformasi digital media [49].

Gambar 1. Kerangka Teknis Mitigasi Pembajakan Akun Media

Gambar 1 menunjukkan kerangka teknis mitigasi pembajakan akun media yang bersifat integratif dan aplikatif dalam konteks jurnalisme digital. Kerangka ini terdiri dari tiga lapisan utama yang saling terhubung untuk memastikan pengelolaan dan perlindungan data yang lebih baik. Lapisan pertama adalah mitigasi tek-

nis *preventif* yang berfokus pada pengamanan sistem melalui autentikasi multi-faktor, segmentasi akses akun redaksi, serta pemantauan aktivitas login secara *real-time*. Pendekatan ini bertujuan untuk mengurangi potensi akses tidak sah dan memastikan bahwa hanya pengguna yang terotorisasi yang dapat mengakses sistem internal media. Selain itu, pengawasan *real-time* membantu mendeteksi dan mencegah potensi ancaman sebelum berdampak lebih jauh, memperkuat lapisan pertama pertahanan terhadap serangan digital.

Lapisan kedua adalah mitigasi operasional redaksi yang bertujuan untuk memperkuat prosedur internal dalam menangani data dan informasi sensitif. Penguatan protokol keamanan internal serta pelatihan literasi keamanan siber bagi jurnalis menjadi kunci penting dalam mengurangi risiko kesalahan manusia yang dapat membuka celah bagi serangan. Selain itu, mekanisme *respons* cepat terhadap insiden peretasan perlu disiapkan untuk meminimalkan kerugian dan mengembalikan operasi redaksi secepat mungkin. Lapisan ketiga adalah mitigasi komunikasi publik yang berfokus pada transparansi informasi dan pemulihan reputasi media setelah terjadinya insiden siber. Transparansi informasi yang jelas dan akurat kepada publik penting untuk menjaga kepercayaan dan mengurangi dampak negatif yang dapat merusak citra media. Ketiga lapisan ini secara keseluruhan bertujuan untuk memperkuat keamanan media digital serta melindungi kebebasan pers dan integritas pemberitaan di tengah ancaman yang berkembang di era digital [50].

Untuk memperjelas analisis secara sistematis, temuan penelitian ini selanjutnya dirangkum dalam bentuk tabel analitis. Penyajian tabel bertujuan untuk memetakan secara komprehensif jenis ancaman siber yang menargetkan jurnalis dan organisasi media, dampaknya pada level individu dan institusional, serta implikasi strategis dan teknis yang dihasilkan. Dengan demikian, Tabel 1 berfungsi sebagai alat analisis yang menghubungkan kerangka teknis mitigasi yang ditampilkan pada gambar sebelumnya dengan temuan empiris di lapangan, sehingga memperkuat argumentasi mengenai perlunya pendekatan mitigasi siber yang terintegrasi dalam jurnalisme digital [51].

Tabel 1. Pemetaan Ancaman Siber, Dampak, dan Implikasi Strategis pada Organisasi Media Digital

Jenis Ancaman Siber	Dampak terhadap Jurnalis dan Redaksi	Dampak Institusional Media	Implikasi Strategis dan Teknis
Pembajakan akun media	Intimidasi, tekanan psikologis, efek chilling	Gangguan operasional dan hilangnya kredibilitas	Penguatan autentikasi multi-faktor dan manajemen akses
Phishing dan social engineering	Kebocoran kredensial jurnalis	Kerentanan sistem redaksi	Pelatihan literasi keamanan siber bagi jurnalis
Penyebaran disinformasi pasca-peretasan	Kerusakan reputasi personal	Penurunan kepercayaan publik	Strategi komunikasi krisis dan transparansi publik
Lemahnya respons platform	Ketidakpastian perlindungan akun	Risiko berulangnya serangan	Tata kelola keamanan digital dan advokasi kebijakan

Tabel 1 memperkuat analisis dengan menyajikan pemetaan sistematis antara jenis ancaman siber, dampaknya pada level individu jurnalis dan institusional media, serta implikasi strategis dan teknis bagi organisasi media digital. Penyajian tabel ini menegaskan bahwa pembajakan akun media tidak hanya berdampak pada gangguan operasional redaksi, tetapi juga menimbulkan konsekuensi strategis yang memengaruhi kepercayaan publik, keberlanjutan model bisnis media digital, dan efektivitas tata kelola teknologi [52]. Melalui pemetaan yang terstruktur, tabel ini menunjukkan keterkaitan antara kerentanan teknis, dinamika kerja jurnalistik, dan kebutuhan akan *respons* manajerial serta kebijakan yang terkoordinasi. Dengan demikian, tabel ini berfungsi sebagai jembatan analitis antara temuan empiris di lapangan dan kerangka mitigasi yang diusulkan, sekaligus memperjelas urgensi penerapan pendekatan keamanan siber yang integratif dalam menghadapi tantangan transformasi digital di sektor media [53].

5. IMPLIKASI MANAJERIAL

Menghadapi transformasi digital, keamanan siber perlu diposisikan sebagai bagian dari kepemimpinan transformasi digital, bukan semata-mata fungsi teknis. Manajemen puncak dituntut untuk mengintegrasikan tata kelola keamanan digital ke dalam strategi organisasi, pengambilan keputusan editorial, serta kebijakan pengelolaan risiko teknologi agar organisasi media lebih adaptif dan resilien terhadap ancaman siber.

Dari perspektif *tech-driven innovation* dan model bisnis media digital, investasi pada sistem keamanan siber merupakan inovasi strategis yang mendukung keberlanjutan organisasi (*sustainability via digital means*). Penerapan autentikasi multi-faktor, segmentasi akses akun, dan pemantauan aktivitas digital secara *real-time* tidak hanya berfungsi sebagai mekanisme perlindungan, tetapi juga memperkuat kepercayaan publik, menjaga kontinuitas operasional redaksi, serta meningkatkan daya saing media di era ekonomi digital.

Selanjutnya, dalam konteks *education* dan *learning factory*, penguatan kapasitas sumber daya manusia menjadi implikasi manajerial yang krusial. Pelatihan literasi keamanan siber bagi jurnalis dan staf redaksi perlu dikembangkan sebagai proses pembelajaran berkelanjutan yang terintegrasi dengan praktik kerja sehari-hari. Pendekatan ini mendorong terbentuknya budaya keamanan digital yang proaktif, sekaligus mendukung pengembangan ekosistem media digital yang inovatif dan berkelanjutan.

6. KESIMPULAN

Kasus peretasan Narasi.tv membuktikan bahwa ancaman siber terhadap jurnalis merupakan bentuk nyata dari kekerasan dan intimidasi yang secara langsung mengancam kebebasan pers. Serangan ini tidak hanya merusak keamanan digital individu, tetapi juga menimbulkan dampak sistemik yang melemahkan proses pemberitaan dan integritas institusi media. Kerentanan platform digital, keterbatasan perlindungan hukum, serta lambannya *respons* penegak hukum memperbesar risiko bagi jurnalis, sehingga membuka ruang bagi aktor-aktor tertentu untuk membungkam kritik dan mengendalikan arus informasi publik. Temuan ini menunjukkan bahwa serangan siber kolektif berfungsi sebagai mekanisme pembungkaman jurnalisme kritis, terutama ketika media melakukan liputan terhadap isu-isu sensitif. Hal ini semakin menegaskan perlunya proteksi yang lebih kuat terhadap kebebasan pers, terutama dalam era digital yang terus berkembang dengan ancaman siber yang semakin kompleks.

Dari perspektif strategis dan pengembangan ilmu, penelitian ini memberikan kontribusi signifikan dengan memperluas kajian ancaman siber terhadap jurnalisme, dari kerentanan individu menuju kerangka institusional dan sistemik. Keamanan siber perlu dipahami sebagai variabel strategis dalam pengembangan teori keberlanjutan media digital, kepemimpinan transformasi digital, dan tata kelola teknologi. Pemahaman ini menempatkan keamanan siber bukan hanya sebagai isu protektif yang teknis, tetapi sebagai elemen kunci dalam menjaga kepercayaan publik dan stabilitas ekosistem informasi digital. Keamanan siber berperan penting dalam memastikan bahwa informasi yang sampai kepada publik tetap akurat, tidak terdistorsi, dan bebas dari penyalahgunaan. Dengan demikian, studi ini membuka ruang bagi penelitian lanjutan yang mengkaji hubungan antara keamanan siber, kepercayaan publik, dan model bisnis media digital sebagai satu kesatuan sistemik yang terintegrasi dalam konteks transformasi digital yang cepat.

Sejalan dengan kerangka teoretis tersebut, temuan penelitian ini juga memiliki implikasi manajerial dan keberlanjutan yang signifikan. Keamanan siber harus diposisikan sebagai agenda strategis dalam transformasi digital organisasi media, bukan sekadar isu teknis operasional. Integrasi tata kelola keamanan digital ke dalam strategi organisasi, pengambilan keputusan editorial, serta pengembangan sumber daya manusia menjadi kunci untuk membangun media digital yang adaptif, resilien, dan berkelanjutan. Dalam konteks global, penelitian ini selaras dengan agenda *Sustainable Development Goals* (SDGs), khususnya SDG 16 mengenai perlindungan kebebasan pers dan tata kelola digital yang akuntabel, SDG 9 melalui penguatan infrastruktur media digital yang aman dan inovatif, serta SDG 4 yang mendukung pengembangan literasi keamanan siber dan pembelajaran organisasi sebagai bagian dari konsep *education* dan *learning factory*. Oleh karena itu, organisasi media perlu mengambil langkah proaktif dalam melibatkan semua pihak termasuk jurnalis, manajer redaksi, dan regulator untuk menciptakan ekosistem media yang lebih aman, transparan, dan tangguh terhadap ancaman siber yang berkembang.

7. SARAN

Peningkatan keamanan digital menjadi langkah penting yang perlu dilakukan oleh organisasi media dengan menyediakan pelatihan serta standar operasional prosedur keamanan siber bagi jurnalis. Penggunaan enkripsi *end-to-end*, penerapan otentikasi dua faktor, dan pemanfaatan perangkat lunak keamanan yang memadai perlu ditetapkan sebagai standar dalam operasional redaksi. Di sisi lain, penyedia platform digital seperti *WhatsApp* dan *Telegram* dituntut untuk meningkatkan transparansi terkait celah keamanan serta memperkuat kerja sama dengan penegak hukum dalam upaya mengidentifikasi dan menindak pelaku serangan siber. Pemerintah juga memiliki peran strategis melalui reformasi regulasi yang berkaitan dengan kebebasan pers dan keamanan siber, disertai dengan penegakan hukum yang tegas terhadap serangan siber yang menargetkan jurnalis. Selain itu, organisasi jurnalis dan masyarakat sipil perlu terus melakukan advokasi perlindungan jurnalis di ranah digital serta membangun kolaborasi lintas sektor guna meningkatkan kesadaran publik terhadap ancaman siber dan pentingnya menjaga kebebasan pers di era digital.

8. DEKLARASI

8.1. Tentang Penulis

Abdul Hamid Arribathi (AH) https://orcid.org/0000-0002-6303-0587
Annisa Ardien (AA) https://orcid.org/0009-0009-6642-7000
Abdullah Arif Kamal (AK) https://orcid.org/0009-0000-1070-275X

8.2. Kontribusi Penulis

Konseptualisasi: AH; Metodologi: AA; Perangkat Lunak: AK; Validasi: AH dan AA; Analisis Formal: AK dan AH; Investigasi: AA; Sumber daya: AK; Kurasi Data: AH; Penulisan Draf Awal: AA dan AK; Peninjauan dan Penyuntingan Tulisan: AH dan AA; Visualisasi: AK dan AH; Semua penulis, AH, AA, dan AK telah membaca dan menyetujui naskah yang telah diterbitkan.

8.3. Pernyataan Ketersediaan Data

Data yang disajikan dalam studi ini tersedia atas permintaan dari penulis terkait.

8.4. Pendanaan

Penulis tidak menerima dukungan finansial untuk penelitian, kepenulisan, dan/atau penerbitan artikel ini.

8.5. Deklarasi Konflik Kepentingan

Penulis menyatakan bahwa mereka tidak memiliki konflik kepentingan, konflik kepentingan finansial yang diketahui, atau hubungan pribadi yang dapat memengaruhi pekerjaan yang dilaporkan dalam makalah ini.

DAFTAR PUSTAKA

[1] A. Indonesia, "Laporan tahunan kekerasan terhadap jurnalis," *AJI Press*, 2023.
[2] A. Al-Rawi, "Social media attacks against female canadian journalists," *Communication*, vol. 18, 2023.
[3] D. A. N. (2025) 5 efek domino konsumsi berita negatif terhadap kesehatan mental. Accessed: 2026-01-19. [Online]. Available: https://www.idntimes.com/life/inspiration/efek-domino-konsumsi-berita-negatif-kesehatan-mental-c1c2-01-bfjms-mrn367
[4] I. F. of Journalists. (2022) Indonesia: Digital attacks target at least 25 media workers. Accessed: 2026-01-19. [Online]. Available: https://www.ifj.org/media-centre/news/detail/article/indonesia-digital-attacks-target-at-least-25-media-workers
[5] L. Pers. (2023, November) Lbh pers sebagai amicus curiae dalam kasus perbuatan melawan hukum oleh 3 platform yang berakibat peretasan wartawan narasi.tv. Accessed: 2026-01-19. [Online]. Available: https://bysl.pw/LBHPers-Sebagai-AmicusCuirae-dalam-KasusPerbuatan-Melawan-Hukum
[6] N. Sabrina, A. Hardinanto, and I. Kumalah, "Seizing social media accounts based on indonesia and the netherlands comparative criminal procedure law," *Jurnal Cakrawala Hukum*, vol. 16, no. 1, 2024.
[7] A. Pratiwi, "Narasi tv's action in reputation management due to hacking crisis," vol. 5, no. 2, pp. 1902–1916, 2025.
[8] R. M. Setyowati, C. Safira, and S. Pramucitra, "Cybersecurity literacy among mass media journalists in central java," *Jurnal Komunikasi*, vol. 18, no. 1, 2024.
[9] P. S. Indonesia, N. Lutfiani, S. Wijono, U. Rahardja, A. Iriani, Q. Aini, and R. A. D. Septian, "A bibliometric study recommendation based on artificial intelligence for ilearning education," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2, pp. 1–9, 2025.
[10] F. Sufi, "A new social media-driven cyber threat intelligence," *Electronics*, vol. 12, no. 5, 2023.
[11] D. Surjatmodjo, A. A. Unde, H. Cangara, and A. F. Sonni, "Information pandemic: A critical review of disinformation spread on social media and its implications for state resilience," *Social Sciences*, vol. 13, no. 8, p. 418, 2024.
[12] Tempo. (2022, September) Situs web narasi tv diretas, terima pesan ancaman 'diam atau mati'. Accessed: 2026-01-19. [Online]. Available: https://www.tempo.co/hukum/situs-web-narasi-tv-diretas-terima-pesan-ancaman-diam-atau-mati--281199
[13] UNESCO, *Protecting Journalism in the Digital Age*. UNESCO Press, 2023.

[14] R. Nuraeni, E. A. Natalia, S. V. Sihotang, Q. Aini, U. Rahardja *et al.*, "The influence of collaborative methods in english language learning on student empathy and tolerance: Pengaruh metode kolaboratif pembelajaran bahasa inggris pada empati dan toleransi mahasiswa," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 4, no. 1, pp. 01–10, 2025.
[15] B. Baker and J. S. Miles, "Impact of cybersecurity threats on digital journalism in the age of disinformation," *Journal of Digital Media*, vol. 23, no. 4, pp. 76–91, 2022.
[16] A. Jones and D. L. Peters, "Cybersecurity and trust in digital journalism: Challenges and responses," *Journal of Media Security*, vol. 15, no. 2, pp. 45–60, 2023.
[17] S. Kim and H. Cho, "Protecting journalists: A study on media cybersecurity strategies in 2024," *Cybersecurity Review*, vol. 12, no. 1, pp. 13–27, 2024.
[18] Y. Liu and P. H. Zhang, "The impact of cyber attacks on news media: A global perspective," *International Journal of Journalism Studies*, vol. 11, no. 3, pp. 30–50, 2023.
[19] U. Rahardja and Q. Aini, "Evaluating the effectiveness of digital marketing campaigns through conversion rates and engagement levels using anova and chi-square tests," *Journal of Digital Market and Digital Currency*, vol. 2, no. 1, pp. 26–45, 2025.
[20] R. Miller and S. Clark, "Digital media and cyber attacks: How journalism is affected in 2023," *Journal of Communication Security*, vol. 9, no. 2, pp. 112–124, 2023.
[21] J. Lee and M. J. Tan, "Protecting press freedom in the digital age: A study on cybersecurity in journalism," *Digital Ethics Journal*, vol. 8, no. 4, pp. 58–75, 2025.
[22] A. Rodriguez and M. Vasquez, "New challenges for press freedom: The role of cybersecurity in protecting journalists," *Global Media Journal*, vol. 12, no. 1, pp. 21–34, 2024.
[23] C. Fisher and K. Thompson, "Digital media, cyber attacks, and the threat to journalism integrity," *Journal of Media Ethics*, vol. 18, no. 3, pp. 95–110, 2024.
[24] J. Bennett and R. J. Thomas, "Digital journalism and cybersecurity: Best practices for protecting press freedom," *Media Protection Journal*, vol. 6, no. 1, pp. 75–89, 2023.
[25] E. L. Briant, "Hack attacks: How cyber intimidation and conspiracy theories drive the spiral of "secrecy hacking"," in *The Routledge companion to freedom of expression and censorship*. Routledge, 2023, pp. 285–295.
[26] E. Sambodja, R. Widhawati, N. A. Zakaria, N. Lutfiani, R. Fachrurrozi, and R. Z. Ikhsan, "Enhancing healthcare services through machine learning and artificial intelligence applications," in *2025 4th International Conference on Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2025, pp. 1–7.
[27] Z. Abbas, R. Khan, M. Z. Khan, and M. Imran, "Cyber laws and media censorship in pakistan: an investigation of governmental tactics to curtail freedom of expression and right to privacy," *Journal of Creative Communications*, p. 09732586231206913, 2023.
[28] L. Papadopoulou and T. A. Maniou, "'lockdown'on digital journalism? mapping threats to press freedom during the covid-19 pandemic crisis," in *Covering Covid-19*. Routledge, 2025, pp. 146–168.
[29] G. O. Antai, O. O. Obisesan, M. E. Umo, H. Ismaila, and D. E. Okpong, "Press freedom and national security: The place of human rights in nigeria's cybercrime laws," *NIU Journal of Social Sciences*, vol. 11, no. 1, pp. 301–313, 2025.
[30] H. R. Ngemba, A. Fitriani, and L. O'Connor, "Pemberdayaan creativepreneur muda melalui pelatihan digital di era transformasi teknologi," *ADI Pengabdian Kepada Masyarakat*, vol. 5, no. 1, pp. 49–56, 2024.
[31] H. Muhammad, G. L. Indra, and O. R. Virnanda, "Undermining people's freedoms and opinions in the digital era," *KnE Social Sciences*, pp. 282–293, 2024.
[32] F. Sammut, M. Bezzina, and J. Scerri, "Under attack in the cyber battlefield: A scoping review of journalists' experiences of cyberharassment," *Journalism and Safety*, pp. 14–42, 2024.
[33] P. Bhat, "Coping with hate: Exploring indian journalists' responses to online harassment," *Journalism Practice*, vol. 18, no. 2, pp. 337–355, 2024.
[34] S. Harlow, R. Wallace, and L. Cueva Chacón, "Digital (in) security in latin america: The dimensions of social media violence against the press and journalists' coping strategies," *Digital Journalism*, vol. 11, no. 10, pp. 1829–1847, 2023.
[35] I. Maria, S. V. Sihotang, R. A. Sunarjo, and A. W. Handaru, "Pemberdayaan komunitas melalui pelatihan pengelolaan keuangan sederhana untuk kesejahteraan ekonomi," *ADI Bisnis Digital Interdisiplin Jurnal*,

vol. 5, no. 2, pp. 33–40, 2024.
[36] M. S. AlAshry, "A critical assessment of the impact of egyptian laws on information access and dissemination by journalists," *Cogent Arts & Humanities*, vol. 9, no. 1, p. 2115243, 2022.
[37] J. R. Henrichsen and M. Shelton, "Expanding the analytical boundaries of mob censorship: How technology and infrastructure enable novel threats to journalists and strategies for mitigation," *Digital Journalism*, vol. 11, no. 10, pp. 1848–1867, 2023.
[38] F. L. Lee and C.-k. Chan, "Legalization of press control under democratic backsliding: The case of post-national security law hong kong," *Media, Culture & Society*, vol. 45, no. 5, pp. 916–931, 2023.
[39] S. Aisyah, I. Muflihah, A. N. Khoirunnisa, and F. Septian, "Peran hukum dalam menjamin kebebasan pers: Tinjauan terhadap uu ite dan ancaman bagi demokrasi di indonesia," *Pendas: Jurnal Ilmiah Pendidikan Dasar*, vol. 10, no. 02, 2025.
[40] H. Herman, W. Achmad, N. Aulia, S. Rusdian, and T. Green, "Utilizing ipfs for decentralized data storage a security and censorship resistance solution," *Blockchain Frontier Technology*, vol. 5, no. 2, pp. 124–135, 2026.
[41] M. Y. Samad and P. D. Persadha, "Pendekatan intelijen strategis sebagai upaya memberikan perlindungan di ruang siber dalam konteks kebebasan menyatakan pendapat," *Kajian*, vol. 27, no. 1, pp. 31–42, 2022.
[42] V. Elysabeth, B. Irawan, and R. Rofiana, "Tinjauan kriminologis: Peran media sosial terhadap peningkatan kasus cyberbullying," *DEDIKASI: Jurnal Ilmiah Sosial, Hukum, Budaya*, vol. 26, no. 2, pp. 129–144, 2025.
[43] A. W. Santoso, "Pertanggungjawaban tindak pidana cyber spear phising dalam perspektif pencurian data pribadi," Ph.D. dissertation, UNIVERSITAS GRESIK, 2025.
[44] R. A. Prayoga, "Perundungan di dunia maya sebagai perilaku menyimpang: Analisis isi komentar dalam konten youtube keke bukan boneka pada kanal rahmawati kekeyi putri cantikka." *Jurnal Kawistara*, vol. 12, no. 2, 2022.
[45] M. H. R. Chakim, M. A. D. Yuda, R. Fahrudin, D. Apriliasari *et al.*, "Secure and transparent elections: Exploring decentralized electronic voting on p2p blockchain," *ADI Journal on Recent Innovation*, vol. 5, no. 1Sp, pp. 54–67, 2023.
[46] J. Simanjuntak and Y. A. Raharusun, "Menjaga penggunaan media sosial yang etis: Penyuluhan dan penerapan uu ite untuk remaja," *Legal Empowerment: Jurnal Pengabdian Hukum*, vol. 1, no. 1, pp. 50–62, 2023.
[47] K. K. dan Informatika Republik Indonesia. (2022) Ancaman siber terhadap keamanan informasi dan perlindungan data pribadi. Accessed: 2026-01-19. [Online]. Available: https://www.kominfo.go.id/content/detail/30894/ancaman-siber-terhadap-keamanan-informasi-dan-perlindungan-data-pribadi/0/berita_satker
[48] R. d. T. R. I. Kementerian Pendidikan, Kebudayaan. (2023) Perlindungan kebebasan pers dan keamanan digital untuk jurnalis. Accessed: 2026-01-19. [Online]. Available: https://www.kemendikbud.go.id/berita/perlindungan-kebebasan-pers-dan-keamanan-digital-untuk-jurnalis
[49] A. Dharmajaya, H. Minangkabawi *et al.*, "Membangun kepercayaan yang berkelanjutan di era disruptif komunikasi: Perspektif media dan komunikasi digital," *Jurnal Komunikasi*, vol. 18, no. 2, 2024.
[50] N. Ardina, "Membangun produktivitas seluruh karyawan dengan program pelatihan dan pengembangan sdm," *Manajemen Bisnis Berbasis Teknologi Digital: Panduan Praktis Menuju Transformasi Digital*, 2025.
[51] B. T. Yasmin, "Hubungan kesadaran hukum hak cipta terhadap perilaku memilih platform streaming film legal dan ilegal," Ph.D. dissertation, Universitas Islam Negeri Maulana Malik Ibrahim, 2025.
[52] M. A. Lingga, W. Trisna, and S. L. Andriati, "Analisis yuridis terhadap pertanggung jawaban pidana tindak pidana pencurian informasi kartu kredit yang merugikan nasabah melalui dunia maya: Studi putusan nomor 240/pid. sus/2021/pn. dps," *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, vol. 4, no. 9, pp. 2741–2754, 2025.
[53] M. K. A. R. Harahap, "Tinjauan yuridis transaksi jual beli barang barang elektronik black market di pasar online dalam perspektif hukum perlindungan konsumen," Ph.D. dissertation, Magister Hukum, Universitas Islam Sumatera Utara, 2025.