Jurnal Peperangan Asimetris
Volume 12, Nomor 1 2026 E-ISSN 2830-0475

Pemanfaatan Teknologi Digital oleh Densus 88 Anti Teror Polri dalam Penanggulangan Terorisme di ruang Siber

(Digital Technology Utilization by Densus 88 of the Indonesian National Police in Countering Terrorism in Cyberspace)

Albert Arisandy[1]*, Rudy Sutanto[2], Bastari[3], Azhar Aditama Djojosugito[4]
[1]Mahasiswa S2 Prodi Strategi Pertahanan Udara Universitas Pertahanan

* email: arisandy50@gmail.com

Abstrak. Perkembangan ruang siber telah dimanfaatkan oleh kelompok teroris untuk menyebarkan ideologi radikal, merekrut anggota, dan merencanakan aksi terorisme. Densus 88 Anti Teror Polri sebagai satuan penanggulangan terorisme di Indonesia dituntut untuk mengimbangi ancaman tersebut dengan memanfaatkan teknologi digital secara efektif. Penelitian ini bertujuan mengkaji pemanfaatan teknologi digital oleh Densus 88 dalam menanggulangi terorisme siber di media sosial, mengidentifikasi tantangan yang dihadapi, serta merumuskan strategi optimalisasi. Metode yang digunakan adalah kualitatif deskriptif berbasis obeservasi dan studi pustaka, dengan analisis data secara kualitatif. Hasil kajian menunjukkan bahwa Densus 88 telah menerapkan intelijen sumber terbuka dan pemantauan media sosial (OSINT/SOCMINT) untuk deteksi dini ancaman, namun masih menghadapi kendala seperti volume data yang besar, kemajuan teknik enkripsi oleh pelaku, serta keterbatasan koordinasi lintas lembaga. Strategi yang direkomendasikan mencakup penguatan kapasitas teknologi dan SDM, peningkatan kerjasama dengan instansi terkait dan platform digital, penyempurnaan regulasi, serta langkah-langkah pencegahan melalui literasi digital. Kesimpulannya, pemanfaatan teknologi digital secara optimal akan meningkatkan efektivitas Densus 88 dalam mencegah dan menanggulangi ancaman terorisme siber di Indonesia.

Kata kunci: Ancaman Terorisme, Ruang Siber, Teknologi Digital, Densus 88, Penanggulangan Terorisme, Media Sosial, Intelijen Digital

Abstract. *The rapid development of cyberspace has created new avenues for terrorist groups to disseminate radical ideologies, recruit members, and coordinate attacks. As Indonesia's primary counter terrorism unit, Densus 88 AT Polri is required to adopt advanced digital technologies to effectively detect and mitigate cybert errorism threats in online platforms. This study aims to analyze the utilization of digital technologies by Densus 88 in countering cyber terrorism on social*

media, identify the challenges encountered, and propose strategic optimizations. Employing a qualitative-descriptive methodology through observation and literature review, this research finds that Densus 88 has integrated Open Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT) to enable early detection of radical content. However, it faces significant obstacles, such as the massive volume of digital data, the increasing sophistication of encryption technologies, and coordination gaps among agencies. The study recommends enhancing technological infrastructure, improving human resources, strengthening inter-agency and international collaboration, and expanding digital literacy initiatives to build social resilience. The findings underscore that strategic and optimal use of digital technologies can substantially increase the effectiveness of Indonesia's counter terrorism efforts in the digital age.

Keywords: Terrorism Threat, Cyberspace, Digital Technology, Densus 88, Counter Terrorism, Social Media, Digital Intelligence

1. Pendahuluan

Pendahuluan Kemajuan teknologi informasi yang terintegrasi dengan internet memberikan manfaat yang signifikan dalam hal komunikasi dan kreativitas, akan tetapi juga menimbulkan tantangan serius bagi keamanan nasional. Digitalisasi memfasilitasi interaksi yang lebih efisien, namun juga membuka jalan bagi pemanfaatan negatif seperti kegiatan kriminal dan terorisme yang memanfaatkan ruang digital untuk menyebarkan propaganda, merekrut anggota, dan merencanakan serangan. Penelitian dari Asmadi et al. (2023) menunjukkan bahwa ketidak cukupan dalam penerapan kebijakan keamanan informasi dapat mengurangi efektivitas teknologi keamanan yang sudah diimplementasikan.

Di era digital saat ini, media sosial berfungsi sebagai platform utama dalam penyebaran propaganda dan ideologi radikal, yang dapat memicu aksi terorisme di banyak negara, termasuk Indonesia. Penelitian terkini menunjukkan bahwa media sosial tidak hanya berfungsi sebagai sarana komunikasi biasa, tetapi juga intensif digunakan oleh kelompok teroris untuk menyebarkan paham ekstrem dan merekrut anggota baru (Sholihin & Kurnia, 2023). Selain itu, konten radikal juga memiliki kemampuan untuk menjangkau audiens yang lebih luas, dengan memanfaatkan platform populer yang digunakan oleh generasi muda.

Berdasarkan data dari https://dipstrategy.co.id/ pengguna media sosial Indonesia pada tahun 2025 sebanyak 190 juta orang. Hal ini menyebabkan Indonesia menghadapi risiko tinggi terhadap penyebaran konten radikalisme secara daring. Laporan Badan Nasional Penanggulangan Terorisme (BNPT) menunjukkan adanya tren peningkatan aktivitas terorisme siber seiring bertambahnya jumlah pengguna internet di negara ini (Agustin et al., 2023). Berdasarakan data patroli siber Densus 88 Anti Teror Polri periode 2021-2024 terdapat 27.471 konten terorisme tersebar dalam berbagai platform media sosial. Penyebaran konten tersebut semakin meningkat setiap tahun. Fenomena ini menimbulkan pertanyaan kritis: bagaimana Densus 88 Anti Teror Polri dapat memanfaatkan teknologi digital dan media sosial untuk mendeteksi dan mencegah ancaman terorisme siber secara efektif.

Densus 88 AT Polri merupakan unit khusus kepolisian yang memiliki tanggung jawab melakukan penindakan dan pencegahan terorisme. Di tengah maraknya pemanfaatan media sosial oleh kelompok teroris, Densus 88 dituntut mengembangkan strategi kontra terorisme yang adaptif terhadap era digital. Berdasarkan latar belakang tersebut, maka penulis mengajukaan penelitian ini dengan judul; "Pemanfaatan teknologi digital oleh Densus 88 AT Polri dalam penanggulangan terorisme di ruang siber".

2. Tinjauan Pustaka

a. Terorisme di ruang Siber

Terorisme siber di ruang siber merujuk pada penggunaan platform digital untuk menyebarkan paham teroris, merekrut simpatisan, menggalang dukungan, atau merencanakan aksi teror di dunia maya. Media sosial menyediakan jangkauan yang sangat luas dan tingkat anonimitas relatif tinggi, sehingga menjadi alat yang menarik bagi kelompok teroris modern (Weimann, 2015). Menurut Berger (2018), internet merupakan sarana ampuh bagi kelompok teroris untuk menyebarkan pesan dan merekrut pengikut; dengan demikian, upaya kontra-terorisme harus turut menangani dimensi online dari proses radikalisasi. Gabriel Weimann bahkan menjelaskan bahwa

media sosial adalah "platform yang sangat efektif bagi kelompok teroris untuk berkomunikasi, berkoordinasi, dan mempengaruhi publik," yang berarti ancaman terorisme di dunia maya memiliki multi-dimensi: tidak hanya berupa serangan siber terhadap infrastruktur, tetapi terutama berupa manipulasi informasi dan propaganda untuk menanamkan ideologi kekerasan dalam masyarakat. Penyebaran konten radikal melalui media sosial dapat menimbulkan efek jangka panjang berupa terbentuknya simpatisan teroris baru secara online.

b. Intelijen Digital dan Teknologi Kontra-Terorisme.

Dalam menghadapi ancaman di ranah siber, aparat penegak hukum di berbagai negara semakin mengandalkan Open Source Intelligence (OSINT) dan Social Media Intelligence (SOCMINT) sebagai bagian dari strategi kontra-terorisme modern. OSINT melibatkan pengumpulan informasi dari sumber terbuka seperti media sosial, blog, dan forum publik dengan pendekatan legal dan sistematis, memungkinkan penegak hukum untuk mendapatkan wawasan berharga tentang perilaku dan potensi ancaman terorisme (Chaudhary & Bansal, 2022). Sementara itu, SOCMINT berfokus secara khusus pada analisis interaksi di platform media sosial untuk mengidentifikasi pola propaganda ideologis dan proses rekrutmen kelompok teroris.

Penerapan teknologi keamanan digital seperti data mining dan kecerdasan buatan (AI) merupakan bagian penting dalam upaya kontra-terorisme modern. Data mining memungkinkan aparat untuk menganalisis dan memproses volume besar data daring untuk mendeteksi anomali atau pola yang dapat mengindikasikan aktivitas terorisme (Mohammed, 2024). Dengan memanfaatkan metode analisis ini Densus 88 dapat lebih efektif dalam mengidentifikasi risiko dan meningkatkan respon terhadap ancaman teroris.

c. Landasan Hukum Penanggulangan Terorisme Siber

Dalam konteks Indonesia, upaya Densus 88 Polri menanggulangi terorisme termasuk di dunia maya didukung oleh kerangka hukum yang terus diperkuat. Undang-

Undang No. 5 Tahun 2018 (perubahan atas UU No.15/2003 tentang Pemberantasan Tindak Pidana Terorisme) memberikan landasan yuridis yang lebih komprehensif bagi aparat penegak hukum untuk mencegah dan memberantas terorisme. UU ini mendefinisikan tindak pidana terorisme secara luas, mencakup perbuatan kekerasan atau ancaman kekerasan yang menimbulkan suasana teror dengan motif ideologi atau politik, serta menegaskan bahwa terorisme bukan lagi dikategorikan sebagai kejahatan politik (sehingga pelaku dapat diekstradisi). Regulasi tersebut memperluas kewenangan Polri (termasuk Densus 88) untuk melakukan penyelidikan aktivitas terorisme di ranah siber, seperti patroli dunia maya dan pemblokiran konten bekerja sama dengan Kementerian Komunikasi dan Informatika (Kominfo). Sinergi antar-lembaga juga diatur: Densus 88 berkoordinasi dengan TNI, BNPT, BSSN, Kominfo, dan intelijen lain dalam penanganan ancaman terorisme digital (Mursid, 2021).

Walaupun landasan hukum sudah lebih kuat, penerapannya harus tetap sejalan dengan penghormatan hak asasi manusia dan hukum lain seperti UU Informasi dan Transaksi Elektronik (UU ITE) agar penanggulangan terorisme siber berjalan efektif sekaligus akuntabel. Saat ini, tantangan yang muncul adalah ketiadaan aturan teknis spesifik terkait penanganan terorisme siber (misalnya prosedur pengawasan digital atau tata kelola intelijen siber), yang menimbulkan grey area dalam penindakan di lapangan. Kekosongan pengaturan teknis ini berpotensi menghambat optimalisasi peran Densus 88 di dunia maya dan akan dibahas lebih lanjut pada bagian tantangan.

d. Kerangka Teoretis: Teori Aktivitas Rutin

Teori aktivitas rutin yang dikemukakan Felson menjelaskan bahwa kejahatan terjadi ketika ada tiga komponen: pelaku bermotivasi, target yang sesuai, dan tidak adanya penjaga kapabel yang mampu mencegah kejahatan (Felson & Clarke, 1998). Dalam analisis fenomena terorisme siber, Teori Aktivitas Rutin (RAT) memberikan kerangka penting untuk memahami interaksi antara pelaku, target, dan pengawasan dalam konteks dunia maya. Teori ini menyatakan bahwa kejahatan, termasuk terorisme siber, terjadi ketika ada tiga kondisi: keberadaan pelaku yang termotivasi, target yang

sesuai, dan ketidakhadiran pengawas yang kapabel. Penelitian Whitty (2019) menunjukkan bahwa peningkatan akses ke teknologi dan penggunaan internet tanpa pengawasan dapat menciptakan peluang bagi pelaku terorisme siber untuk melakukan serangan, akibatnya, individu atau organisasi menjadi target yang mudah.

Dalam konteks media sosial, terutama terkait dengan peran "penjaga" yang mampu mencegah kejahatan. Kehadiran penjaga seperti aparat keamanan siber dan moderator platform dapat mengurangi peluang terjadinya kejahatan terorisme siber dengan mengawasi dan memblokir konten berbahaya. Penelitian dari Puente & Hernández (2022) menunjukkan bahwa ketidakhadiran penjaga yang mampu berasosiasi positif dengan pelaku yang termotivasi dan target yang sesuai, secara signifikan meningkatkan kerentanan terhadap kejahatan di dunia maya. Sebaliknya, kehadiran Densus 88, TNI, BNPT, BSSN, Komdigi, dan stakeholder terkaut yang aktif akan membantu menekan aktivitas terorisme siber, mendukung hipotesis bahwa pengawasan yang efektif dapat mengurangi peluang pelaku untuk menemukan target yang rentan.

3. Metode Penelitian

Metode Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan observasi dan studi pustaka. Data dan informasi dikumpulkan dari berbagai sumber sekunder, antara lain buku, artikel jurnal ilmiah, laporan resmi, peraturan perundang-undangan, serta publikasi media massa yang relevan dengan topik terorisme siber dan pemanfaatan teknologi oleh aparat keamanan. Selanjutnya, data dianalisis secara kualitatif untuk menggambarkan situasi dan menjawab rumusan masalah yang telah ditetapkan.

Secara prosedural, penelitian dimulai dengan tahap observasi, pengumpulan literatur, dan data sekunder. Setelah itu, dilakukan pemetaan konsep dan teori kunci (misalnya konsep terorisme siber, OSINT/SOCMINT, kerangka hukum, teori aktivitas rutin). Pada tahap analisis, penulis mengevaluasi temuan observasi, studi pustaka, dan

data sekunder untuk: (1) menguraikan potensi ancaman terorisme di media sosial dan (2) menilai upaya dan kapabilitas yang dimiliki Densus 88 saat ini beserta rekomendasi strategis. Hasil analisis kemudian disajikan dalam bentuk narasi pembahasan yang terstruktur mengikuti aspek-aspek rumusan masalah. Dengan metode dan pendekatan ini, diharapkan kesimpulan yang dihasilkan bersifat komprehensif dan didukung oleh bukti serta teori yang kuat.

4. Hasil dan Diskusi

a. Potensi Ancaman Terorisme di ruang Siber.

Media sosial telah menjadi sarana utama penyebaran paham radikal di era digital. Berbagai platform populer seperti Facebook, Twitter, Instagram, dan YouTube, serta aplikasi pesan terenkripsi seperti Telegram, dimanfaatkan oleh kelompok teroris untuk propaganda dan komunikasi rahasia. Penelitian Nugroho et al. (2024) menunjukkan bahwa konten radikal di media sosial meningkat signifikan – sekitar 37% dalam dua tahun terakhir – seiring kemajuan teknologi digital, kemudahan akses, dan cepatnya arus informasi di media sosial. Kondisi ini membuat penyebaran ideologi radikal terjadi lebih cepat dan masif, yang jelas berbahaya bagi keamanan nasional. Berikut data patrol siber yang dilakukan oleh Densus 88 AT Polri yang dikolompokan sesuai kategori konten yang ditemukan.

Tabel 1 Data Patroli Siber Densus 88 AT Polri 2021-2024

Sumber: Densus 88 AT Polri

Kategori	2021	2022	2023	2024
PROPAGANDA	5243	6345	6448	4044
INFO TEROR GLOBAL	398	1539	987	351
PROMOSI SENJATA (SENPI/AIRSOFT)	266	264	166	36
PENDANAAN	228	237	11	22
IDEOLOG	22	31	122	646
TUTORIAL BOM	12	23	10	0
PROMOSI SAJAM	0	0	0	8
TUTORIAL PERAKITAN SENJATA	3	2	6	1
Total	6172	8441	7750	5108
				22.363

Data patroli siber Densus 88 AT Polri pada 2021–2024 menunjukkan dinamika ancaman digital yang signifikan di Indonesia, khususnya terkait propaganda dan aktivitas terorisme daring. Terdapat peningkatan tajam jumlah konten propaganda teror: dari 5.243 kasus pada 2021, memuncak hingga 6.448 kasus pada 2023, sebelum menurun menjadi 4.044 kasus pada 2024. Penurunan pada 2024 ini belum tentu menandakan redanya aktivitas, melainkan bisa merefleksikan perubahan pola komunikasi pelaku atau hasil dari filterisasi digital yang diterapkan aparat. Fenomena mencolok lain adalah lonjakan laporan kategori "Info Teror Global" pada 2022 (1.539 kasus, dibanding 398 kasus di 2021). Kenaikan ini diduga dipicu eskalasi konflik geopolitik global yang dieksploitasi jaringan teroris untuk memperkuat propaganda dan rekrutmen. Sementara itu, kategori Ideologi melonjak drastis pada 2024 menjadi 646 laporan dibandingkan tahun 2023 sebanyak 122 laporan, hal menandai pergeseran ancaman dari aksi fisik menuju ancaman berbasis ideologi atau narasi ekstrem. Perubahan tren ini

mengindikasikan fokus kelompok teroris yang semakin menekankan perang informasi dan pengaruh ideologis di dunia maya. Secara umum, temuan observasi lapangan, studi literatur, dan data sekunder mengungkap bahwa ancaman terorisme siber di media sosial bersifat multidimensional, meliputi beberapa aspek berikut:

Propaganda Radikal dan Rekrutmen Digital. Kelompok teroris memanfaatkan media sosial sebagai medium efektif untuk menyebarkan propaganda radikal sekaligus merekrut anggota baru secara virtual. Algoritma platform yang mendorong keterlibatan pengguna dapat memperkuat jangkauan konten ekstrem melalui efek echo chamber, sehingga proses radikalisasi massal terjadi dalam waktu singkat. Di saat yang sama, fitur komunikasi privat dan anonimitas identitas memfasilitasi rekrutmen terselubung. Kelompok teroris dapat mendekati calon anggota (terutama pemuda) dengan pendekatan ideologis dan emosional secara bertahap tanpa perlu tatap muka (teknik *virtual grooming*), membentuk ikatan ekstremisme tanpa terdeteksi.

Koordinasi Operasi dan Mobilisasi Kekerasan. Platform komunikasi terenkripsi seperti Telegram dan WhatsApp digunakan teroris untuk mengoordinasikan operasi teror. Mereka dapat menyusun rencana serangan, berbagi tutorial pembuatan bom, dan membentuk sel-sel tidur secara rahasia melalui saluran yang sulit diawasi aparat. Sementara itu, seruan jihad di media sosial terbuka bisa viral dalam menit, memicu efek domino pada simpatisan. Individu yang teradikalisasi dapat terdorong melakukan serangan spontan sebagai lone wolf tanpa komando langsung dari jaringan pusat.

Manipulasi Informasi dan Disinformasi. Kelompok teroris juga mengoperasikan strategi manipulasi psikologis melalui penyebaran disinformasi berbasis sentimen agama atau identitas. Narasi-narasi palsu, teori konspirasi, dan konten provokatif sengaja disebarkan untuk menciptakan polarisasi sosial serta memperbesar rasa ketidakpercayaan terhadap pemerintah. Dengan mengadu domba kelompok masyarakat dan memicu konflik horizontal, para pelaku teror berusaha menanamkan kondisi sosial-politik yang dianggap subur bagi tumbuhnya ideologi ekstremisme.

Eksploitasi Teknologi AI dan Deepfake. Kemajuan teknologi turut dimanfaatkan oleh teroris, misalnya melalui pembuatan konten deepfake dengan bantuan kecerdasan buatan (AI). Kelompok ekstremis telah mulai menggunakan teknik deepfake berbasis kecerdasan buatan untuk menciptakan video manipulatif, termasuk simulasi pidato para pemimpin jihad yang tampak autentik. Tujuannya adalah menipu dan menghasut khalayak sekaligus membangun legitimasi palsu atas narasi kekerasan yang mereka usung. Konten deepfake semacam ini sangat sulit diverifikasi secara cepat oleh publik, sehingga dapat dengan mudah dimanfaatkan untuk menyebarluaskan propaganda radikal sebelum kebenarannya terungkap.

Pendanaan dan Pelatihan melalui Media Sosial. Media sosial tidak hanya dimanfaatkan untuk propaganda, tetapi juga untuk mendukung logistik terorisme seperti penggalangan dana dan pelatihan jarak jauh. Menurut berita dari Tempo pada tanggal 26 November 2017, kelompok teroris menggunakan fitur donasi online dan dompet digital guna mengumpulkan dana bagi kegiatan mereka. Dengan metode terstruktur (misalnya yang diterapkan ISIS), para ekstremis mampu menarik simpati dan donasi dari kalangan muda yang terpapar pesan radikal. Pendekatan ini menjadikan media sosial bukan sekadar alat komunikasi, melainkan pula platform rekrutmen dan pendanaan yang secara signifikan meningkatkan jangkauan serta kecepatan penyebaran ideologi terorisme.

Rangkaian potensi ancaman di atas menunjukkan bahwa media sosial tidak lagi sekadar alat komunikasi biasa, melainkan platform efektif bagi kelompok teroris untuk memperluas operasi mereka. Media sosial secara signifikan meningkatkan jangkauan dan kecepatan penyebaran ideologi terorisme, memperbesar skala dampak radikalisasi di masyarakat.

Lebih lanjut, kelompok teroris terus beradaptasi agar terhindar dari deteksi dan identifikasi aparat. Mereka beralih ke platform-platform terenkripsi dan menggunakan istilah atau kode sandi khusus dalam komunikasi daring. Taktik ini menciptakan tantangan besar bagi aparat penegak hukum seperti Densus 88 dalam memantau kegiatan teroris secara real time. Keberadaan dark web turut memperburuk situasi,

karena menyediakan lapisan anonimitas yang tinggi bagi pelaku teror untuk berkomunikasi dan berkolaborasi tanpa terdeteksi. Akibat paparan konten radikal yang masif, muncul fenomena teroris "lone wolf" maupun sel tidur yang proses radikalisasinya berlangsung sepenuhnya di dunia maya dan nyaris mustahil terdeteksi dengan metode intelijen konvensional. Tanpa penanganan yang tepat, media sosial dapat menjadi lahan subur bagi tumbuh kembangnya terorisme gaya baru yang sulit diberantas.

Dari perspektif teori aktivitas rutin, maraknya terorisme siber di media sosial ini terjadi karena ketiga elemen kejahatan terpenuhi secara bersamaan di ruang siber. Pelaku teroris digital memanfaatkan peluang terbuka berupa akses internet yang mudah, arus informasi cepat, dan anonimitas tinggi; target potensial berupa pengguna rentan (misalnya remaja dengan literasi digital rendah) tersedia dalam jumlah besar; dan penjaga kapabel nyaris tidak ada akibat lemahnya moderasi platform dan terbatasnya kapasitas pengawasan aparat. Konvergensi pelaku, target, dan minimnya penjaga inilah yang membuat media sosial menjadi ladang subur bagi aksi terorisme siber.

Kelemahan peran "penjaga" digital di media sosial jelas dieksploitasi oleh para teroris. Penjaga di sini mencakup moderator platform, regulator pemerintah, aparat penegak hukum (seperti Densus 88), serta komunitas pengguna internet itu sendiri. Ketika moderasi konten oleh platform tidak memadai dan kapasitas intelijen siber aparat terbatas, penyebaran ideologi radikal hampir tak terbendung dan pelaku dapat beraksi nyaris tanpa hambatan. Untuk itu, sangat diperlukan penguatan peran penjaga digital di berbagai lini. Aparat keamanan siber harus meningkatkan kapasitas dengan memanfaatkan teknologi intelijen mutakhir (OSINT, SOCMINT, AI) guna mendeteksi pola radikalisasi daring sedini mungkin. Kerja sama antara platform media sosial, pemerintah, dan masyarakat sipil juga krusial untuk menutup celah pengawasan serta mempercepat respons terhadap ancaman. Di samping itu, peningkatan literasi digital di kalangan pengguna akan mengurangi jumlah target rentan yang mudah terpapar propaganda. Dengan strategi terpadu yang membatasi ruang gerak pelaku, memperkuat

ketahanan calon korban, dan mengoptimalkan peran penjaga, ancaman terorisme siber di media sosial dapat ditekan seminimal mungkin.

b. Pemanfaatan Teknologi Digital oleh Densus 88 AT Polri.

Perkembangan teknologi digital telah mengubah secara fundamental pola dan taktik operasional kelompok teroris di ruang siber. Para pelaku teror kini memanfaatkan sarana komunikasi yang terenkripsi dan relatif aman untuk menghindari deteksi aparat keamanan. Sebagai respons atas ancaman yang terus berevolusi ini, Detasemen Khusus 88 Antiteror Polri telah mengintegrasikan penggunaan teknologi digital dan intelijen siber ke dalam operasional penanggulangan terorisme. Misalnya, Densus 88 membentuk tim siber khusus yang bertugas memantau konten di media sosial sebagai bagian dari kegiatan intelijen proaktif. Langkah ini memungkinkan deteksi ancaman dan aktivitas teroris secara lebih dini dan efektif di berbagai platform online yang rutin digunakan pelaku. Upaya tersebut sekaligus merepresentasikan hadirnya guardian (penjaga) di ranah siber sesuai teori aktivitas rutin Densus 88 berusaha mengisi kekosongan pengawasan dengan menghadirkan "penjaga digital" yang memantau aktivitas teror di dunia maya.

Integrasi teknologi canggih, termasuk pemanfaatan analitik media sosial, menjadi kunci bagi Densus 88 untuk memahami dan mencegah penyebaran ideologi teroris secara efektif di internet. Dengan mengadopsi teknologi digital terkini, Densus 88 diharapkan mampu mendeteksi potensi ancaman sedini mungkin dan menghentikannya sebelum eskalasi menjadi aksi teror nyata. Dalam inisiatif ini, Densus 88 memanfaatkan metode Open Source Intelligence (OSINT) untuk mengumpulkan informasi dari berbagai sumber terbuka mulai dari platform media sosial, forum daring, hingga website yang berpotensi terkait aktivitas terorisme. Beragam alat dan teknik analitik canggih dalam kerangka OSINT terbukti membantu Densus 88 melakukan deteksi dini secara intelijen serta meningkatkan efektivitas pengawasan atas aktivitas mencurigakan di berbagai platform. OSINT juga memungkinkan integrasi data lintas sumber, memberikan gambaran menyeluruh mengenai pola komunikasi dan perekrutan dalam

komunitas teroris di dunia maya. Dengan demikian, OSINT menjadi elemen krusial untuk memperkuat upaya pencegahan terorisme oleh Densus 88. Melalui OSINT, aparat dapat mendeteksi dan mengidentifikasi akun-akun mencurigakan, percakapan yang mengandung paham ekstrem, maupun penyebaran materi propaganda secara daring sejak tahap awal.

Selain OSINT, Densus 88 menerapkan Social Media Intelligence (SOCMINT), yaitu teknik analisis khusus terhadap pola interaksi dan jejaring sosial di berbagai platform media sosial (Facebook, Twitter, Instagram, Telegram, dll.). SOCMINT membantu memetakan relasi antar akun, mengungkap jaringan dalam grup diskusi tertutup, serta mengidentifikasi tren percakapan yang mengarah pada penyebaran ideologi radikal. Dengan teknik ini, Densus 88 mampu mendeteksi pola perekrutan anggota baru secara online misalnya melalui pemantauan kelompok tertutup yang sering berbagi konten jihad atau informasi terkait terorisme (Saputra,2024). SOCMINT tidak hanya menganalisis isi konten, tetapi juga memberikan wawasan mengenai dinamika sosial di balik interaksi komunitas ekstremis. Hal ini memungkinkan Densus 88 mengidentifikasi dan menggagalkan potensi ancaman sebelum berkembang lebih jauh menjadi aksi teror. Dari sudut pandang teori aktivitas rutin, pemanfaatan OSINT/SOCMINT tersebut meningkatkan kapabilitas guardian di dunia maya: penegak hukum memanfaatkan informasi rutin yang tersedia di media sosial untuk mengintervensi pertemuan antara pelaku dan target sebelum kejahatan terjadi.

Di samping intelijen sumber terbuka, Densus 88 menjalin kerja sama erat dengan Kominfo dan perusahaan platform digital untuk menghapus konten terorisme secara cepat. Ketika konten bernuansa teror (misalnya video propaganda ISIS atau ajakan pembuatan bom) terdeteksi, tim siber Polri segera berkoordinasi dengan Kominfo untuk memblokir atau menurunkan (take-down) konten tersebut sesuai prosedur hukum yang berlaku. Langkah preventif ini bertujuan memutus rantai penyebaran konten radikal sejak tahap awal sebelum meluas di masyarakat. Secara internal, Densus 88 juga telah mengembangkan sistem pemantauan siber real-time untuk meningkatkan kesiapsiagaan. Inisiatif ini mendorong peningkatan pemanfaatan teknologi digital dan

media sosial dalam operasi intelijen, khususnya melalui implementasi analitik big data. Transformasi strategi Densus 88 dari metode konvensional menuju sistem intelijen modern ditandai oleh kemampuan menyaring dan menganalisis data berjumlah besar dari berbagai platform media sosial. Hasilnya adalah dashboard informasi terpadu yang memetakan insiden terorisme dan perilaku mencurigakan secara komprehensif dan real-time, sehingga mendukung pengambilan keputusan cepat berbasis data.

Penerapan analitik big data telah terbukti efektif memberikan wawasan mendalam dan meningkatkan kapasitas intelijen di berbagai sektor, termasuk keamanan nasional dan upaya kontra-terorisme. Langkah Densus 88 menerapkan teknologi canggih seperti Artificial Intelligence (AI) dan algoritma machine learning merupakan strategi penting untuk menghadapi ancaman terorisme di era digital. Salah satu aplikasi AI yang sudah diimplementasikan adalah analisis sentimen, yaitu teknik pemrosesan bahasa alami untuk mendeteksi emosi atau polarisasi pendapat dalam teks yang diunggah di media sosial. Dengan memanfaatkan algoritma pembelajaran mesin terkini, Densus 88 dapat menganalisis arus opini publik di dunia maya serta mengenali pola-pola percakapan yang berpotensi menandakan aktivitas terorisme. Sebagai ilustrasi, sistem analisis sentimen membantu mengidentifikasi pola emosional dalam teks – misalnya lonjakan kemarahan atau dukungan terhadap ideologi radikal – yang bisa menjadi indikator dini rencana aksi teror. Di sini, analisis sentimen berperan menyaring "rutinitas" komunikasi online untuk menemukan anomali yang relevan dengan ancaman keamanan. Selain analisis teks, AI juga dimanfaatkan dalam penyaringan konten visual. Teknik deep learning (pembelajaran mendalam) digunakan untuk memindai gambar atau video yang mengandung simbol terlarang atau konten ekstremis lainnya di platform media sosial. Teknologi ini membantu mengidentifikasi elemen-elemen visual terkait terorisme secara otomatis, sehingga meningkatkan kecepatan dan akurasi respon Densus 88 terhadap potensi ancaman. Secara keseluruhan, pemanfaatan teknologi mutakhir oleh Densus 88 memperlihatkan bagaimana peningkatan penjagaan digital melalui pemanfaatan AI dapat mengurangi peluang bagi pelaku teror memanfaatkan ruang siber, sejalan dengan prediksi teori aktivitas rutin.

Walaupun inovasi dan adaptasi teknologi digital oleh Densus 88 telah menunjukkan hasil positif, penelitian ini mengidentifikasi berbagai tantangan dan hambatan signifikan dalam penanggulangan terorisme siber saat ini. Tantangan tersebut mencakup aspek teknis, sumber daya manusia, koordinasi kelembagaan, hingga kebijakan, yang diuraikan sebagai berikut:

Volume data yang berlebihan (Overload Data). Platform digital menghasilkan data dalam volume sangat besar secara konstan. Kondisi ini menyulitkan Densus 88 untuk memilah intelijen yang relevan dari noise informasi yang tidak penting, sehingga berpotensi menyebabkan keterlambatan dalam deteksi dini. Beban data yang berlebih juga meningkatkan risiko kesalahan identifikasi target karena sulitnya menyaring sinyal ancaman yang akurat di tengah limpahan informasi rutin yang kurang relevan.

Enkripsi *end-to-end* dan *dark web*. Meluasnya penggunaan aplikasi komunikasi ber-enkripsi (misalnya Telegram atau Signal) serta forum tersembunyi di *dark web* membatasi akses penegak hukum terhadap isi komunikasi antar pelaku teror. Situasi ini menciptakan titik buta intelijen yang serius dalam investigasi siber, karena percakapan daring para pelaku terlindungi oleh enkripsi yang sulit ditembus (Halkis,2025). Selain itu, keterlibatan pelaku teror dalam dark web mempersulit infiltrasi ke jaringan radikal, sehingga aparat kehilangan penjagaan efektif pada ruang komunikasi tersebut. Akibatnya, peluang kejahatan meningkat karena pelaku dapat beraksi tanpa terdeteksi (*absence of capable guardian* sesuai teori aktivitas rutin).

Keterbatasan infrastruktur teknologi dan algoritma lokal. Sistem analitik big data dan AI yang tersedia bagi Densus 88 saat ini masih berada pada tahap awal pengembangan. Algoritma yang digunakan umumnya bersifat generik dan belum terkalibrasi khusus untuk karakteristik sosial budaya serta pola ancaman terorisme lokal di Indonesia. Keterbatasan ini berarti bahwa beberapa pola komunikasi unik (misalnya penggunaan bahasa daerah atau kode terselubung) mungkin luput dari deteksi sistem. Infrastruktur teknologi yang belum optimal dan kurangnya algoritma yang disesuaikan

dengan konteks domestik mengurangi efektivitas sistem intelijen siber secara keseluruhan.

Kurangnya kompetensi SDM intelijen digital. Jumlah dan kapasitas personel Densus 88 dengan keahlian tinggi di bidang teknologi informasi masih terbatas. Keahlian khusus seperti pemrograman, data science, forensik digital, analisis media sosial, serta penguasaan bahasa asing sangat dibutuhkan dalam operasi siber modern. Terbatasnya SDM dengan kompetensi tersebut menyebabkan pemanfaatan teknologi digital untuk proses investigasi dan prediksi belum optimal. Hal ini menunjukkan tantangan internal dalam meningkatkan kapabilitas penjaga di lingkungan Densus 88 sendiri, karena teknologi canggih memerlukan operator dan analis yang terlatih.

Fragmentasi dan ego sektoral antar lembaga. Koordinasi antara Densus 88 dan lembaga keamanan terkait lainnya (seperti TNI, BSSN, BNPT, Kominfo, dan BIN) belum terintegrasi secara sistemik. Perbedaan prosedur operasional, ketidaksinkronan alur komando, perbedaan format data, serta kecenderungan ego sektoral di masing-masing institusi menghambat pertukaran informasi secara real-time. Akibatnya, respons nasional terhadap ancaman teror siber sering kali terfragmentasi dan kurang terpadu. Dari perspektif teori, kondisi ini memperlemah "penjaga kolektif" karena berbagai entitas yang seharusnya berperan sebagai guardian tidak bertindak secara koordinatif.

Belum adanya regulasi teknis yang adaptif dan responsif. Meskipun Indonesia telah memiliki landasan hukum umum penanggulangan terorisme (misalnya UU No. 5 Tahun 2018), hingga kini belum ada aturan teknis turunan yang spesifik dan luwes untuk mengatur operasi kontra-terorisme di ranah digital. Ketiadaan regulasi teknis yang adaptif ini mencakup kekosongan pedoman mengenai prosedur pengawasan digital, tata kelola data intelijen siber, batasan legal penyadapan atau akses ke informasi pribadi, serta kerangka kolaborasi antara pemerintah dengan penyedia platform digital. Kekosongan regulasi tersebut menimbulkan ketidakpastian hukum dan etika bagi Densus 88 dalam bertindak sebagai "penjaga" di dunia maya. Selain itu, pelaku teror dapat mengeksploitasi grey area regulasi ini, misalnya dengan beroperasi di platform

yang belum diatur, sehingga meningkatkan peluang kejahatan siber terjadi tanpa hambatan hukum yang jelas.

5. Kesimpulan

Pemanfaatan teknologi digital oleh Densus 88 AT Polri merupakan hal yang sangat penting dalam menghadapi era baru terorisme yang memanfaatkan ruang siber. Dari pembahasan di atas, dapat disimpulkan beberapa hal penting. Ancaman terorisme siber melalui media sosial di Indonesia nyata dan berkembang pesat. Platform digital digunakan oleh kelompok teroris untuk propaganda, rekrutmen, koordinasi, hingga pendanaan, yang semuanya dapat terjadi secara tersembunyi di balik lalu lintas informasi sehari-hari.

Densus 88 telah mulai bertranformasi dengan memanfaatkan OSINT, SOCMINT, analisis big data, dan AI dalam operasi intelijennya. Meskipun demikian, Densus 88 menghadapi tantangan berupa keterbatasan sumber daya teknologi dan manusia, masifnya data yang harus dipantau, canggihnya pola komunikasi teroris, serta kebutuhan koordinasi lintas sektor yang lebih solid. Rekomendasi strategis meliputi penguatan aspek teknologi, pengembangan kemampuan dan perekrutan SDM intelijen digital, koordinasi dan kolaborasi antar institusi terkait, dan penguatan kerangka regulasi dalam penanggulangan terorisme siber.

Sebagai garda terdepan pemberantasan terorisme, Densus 88 perlu terus berinovasi, beradaptasi, dan berinvestasi seiring kemajuan teknologi. Dukungan penuh dari segi anggaran, kebijakan, serta kolaborasi antar-pemangku kepentingan akan sangat menentukan keberhasilan strategi digital ini ke depan. Apabila pemanfaatan teknologi digital dapat dioptimalkan, potensi ancaman terorisme siber di media sosial dapat ditekan seminimal mungkin. Pada gilirannya, hal ini berkontribusi pada terciptanya ruang digital dan lingkungan masyarakat yang lebih aman, sekaligus memperkuat ketahanan Indonesia dalam menghadapi tantangan terorisme di era Society 5.0.

Penelitian selanjutnya dapat difokuskan pada evaluasi empiris efektivitas langkah-langkah yang telah diambil Densus 88 serta pemantauan perkembangan

ancaman-ancaman baru, sehingga strategi penanggulangan dapat terus diperbarui secara empiris sesuai situasi terkini. Di samping itu, kolaborasi antara akademisi, praktisi keamanan siber, dan pembuat kebijakan perlu ditingkatkan untuk mendukung pendekatan penanggulangan terorisme yang komprehensif dan berkelanjutan.

Daftar Pustaka (APA Style)

1. Buku

Awan, I. (2017). Cyber-Extremism: ISIS and the Power of Social Media. Routledge.

Berger, J. M. (2018). EXTREMISM. Cambridge, MA : The MIT Press, https://mitpress.mit.edu/9780262535878/extremism/

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief: practical theory for crime prevention. Police Research Series, Paper 98. Policing and Reducing Crime Unit, Research, Development and Statistics Directorate. https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf

Weimann, G. (2015). Terrorism in cyberspace. In the next generation. Woodrow Wilson Center Press. https://www.wilsoncenter.org/book/terrorism-cyberspace-the-next-generation

2. Jurnal

Agustin, I. C., Tantimin, S. H., & Situmeang, S. (2023). Peran Badan Nasional Penanggulangan Terorisme (BNPT) Dalam Menanggulangi Radikalisme Dan Terorisme Di Indonesia. Fundamental Jurnal Ilmiah Hukum, 12(2), 354–383. https://doi.org/10.34304/jf.v12i2.188

Argastya, A. Y., & Supanto. (2022). Penerapan Hukum Pidana Pada Penyidikan Kepolisian Untuk Menanggulangi Kejahatan Cyber-Terrorism. Recidive : Jurnal Hukum Pidana Dan Penanggulangan Kejahatan, 11(1), 10. https://doi.org/10.20961/recidive.v11i1.67425

Asmadi, A., Almutahar, H., Sukamto, S., Zulkarnaen, Z., Listiani, E. I., & Sikwan, A. (2023). Digital Information Security Policy in the National Security Strategy.

International Journal of Multidisciplinary Approach Research and Science, 1(02), 96–103. https://doi.org/10.59653/ijmars.v1i02.6

Chaudhary, M., & Bansal, D. (2022). Open Source Intelligence Extraction for Terrorism-related Information: A Review. Wiley Interdisciplinary Reviews Data Mining and Knowledge Discovery, 12(5). https://doi.org/10.1002/widm.1473

Halkis, M., & Bagus, I. Y. S. (2025). *Military operations for law enforcement: Joint operation of the Army Special Forces Command and the police during the "Nemangkawi" operation in Papua 2018*. **Social Development and Security, 15**(4). https://doi.org/10.33445/sds.2025.15.4.2

Mohammed, B. (2024). The Impact of Artificial Intelligence on Cyberspace Security and Market Dynamics. Brazilian Journal of Technology, 7(4), e74677. https://doi.org/10.38152/bjtv7n4-019

Mursid, F. (2021, June 24). Kominfo Telah Blokir 21.330 Konten Radikal Terorisme. Republika. Retrieved from https://www.republika.co.id/berita/qv6jhs396/kominfo-telah-blokir-21330-konten-radikal-terorisme

Muttaqin, A., Widyaningsih, R., & Riswan, Y. (2024). Awaking Awareness of Communication Patterns in the Cyber Radicalism: Covid-19 Pandemic Case Study. Komunika Jurnal Dakwah Dan Komunikasi, 18(1), 71–84. https://doi.org/10.24090/komunika.v18i1.10637

Nugroho, P., Sutrisno, A., & Aminudin, C. (2024). Media Sosial Dan Radikalisme: Bagaimana Teknologi Informasi Mempengaruhi Pemikiran Ekstrem. HMRM, 1(4), 110–115. https://doi.org/10.37010/hmr.v1i4.31

Puente, S. M., & Hernández, I. N. R. (2022). Cyber Victimization Within the Routine Activity Theory Framework in the Digital Age. Revista De Psicología, 40(1), 265–291. https://doi.org/10.18800/psico.202201.009

Saputra, E., Halkis, M., Suhirwan, & Mardina, D. (2024). Menyingkap tabir 'teror suci'. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *11*(8), 3304–3316

Sholihin, A., & Kurnia, H. (2023). Internet Sebagai Media Penyebaran Ideologi Radikal: Dampak, Tantangan, Dan Upaya Penanggulangannya. AoSSaGCJ, 3(1), 24–30. https://doi.org/10.47200/aossagcj.v3i1.1844

Tempo. (2017). Teroris di Indonesia Beralih ke Media Sosial untuk Galang Dana. https://www.tempo.co/internasional/teroris-di-indonesia-beralih-ke-media-sosial-untuk-galang-dana-1145846

Whitty, M. T. (2019). Predicting Susceptibility to Cyber-Fraud Victimhood. Journal of Financial Crime, 26(1), 277–292. https://doi.org/10.1108/jfc-10-2017-0095

Johnson, L., & Smith, K. (2019). Pengaruh media sosial terhadap kesehatan mental. *Jurnal Psikologi Sosial, 15*(2), 123-134. https://doi.org/10.1234/jps.2019.002

Tentang Penulis

Penulis bernama lengkap Albert Arisandy, S.I.K., M.H. lahir di Palembang pada tanggal 4 Oktober 1988 dari pasangan seorang Ayah Soli Rozak dan Ibu Dwi Andhika Fitri. Penulis menempuh pendidikan dasar pada tahun 1994 di SDN 27 Palembang dan lulus tahun 2000. Setelah lulus penulis melanjutkan di SMPN 27 Palembang dan lulus tahun 2003. Pada jenjang pendidikan berikutnya penulis melanjutkan pendidikan di SMAN 17 Palembang dan lulus tahun 2006. Peneliti melaksanakan pendidikan kepolisian di mulai dari Akademi Kepolisian (Akpol) dan lulus tahun 2009. Setelah lulus Akpol penulis ditempatkan di Markas Komando Korps Brimob Polri. Riwayat Jabatan penulis dimulai dari Resimen II Pelopor Korps Brimob Polri sebagai Danton 4 Kompi 4 Batalyon B pada tahun 2010. Selanjutnya sebagai Pasi Ops Den B Satbrimob Polda Sulut, Danki 2 Den B Satbrimob Polda Sulut, Danki 1 Den B Satbrimob Polda Sulut. Pada Tahun 2016 Penulis menempuh pendidikan di Perguruan Tinggi Ilmu Kepolisian dan lulus pada tahun 2018, Selanjutnya penulis

bertugas di Densus 88 Anti Teror Polri sebagai Panit Operasional unit Intelijen Satgaswil DKI Jakarta, selanjutnya sebagai Kasubnit Operasional unit Intelijen Satgaswil DKI Jakarta pada tahun 2021, pada tahun 2022 penulis menjabat sebagai kasubnit analis dan tekintel unit intel Satgaswil DKI Jakarta. Pada tahun 2025 peneliti menyelesaikan pendidikan di Seskoau Angkatan 62 dan saat ini peneliti menjabat sebagai Kani Intelijen Satgaswil Sumut Densus 88 AT Polri.

Peneliti menikah pada tanggal 28 Februari 2014 di Kotamobagu, Sulawesi Utara dengan wanita pujaannya bernama Pingkan Pardede. Dari pernikahan ini, penulis dikaruniai 3 orang anak. Yang pertama yaitu anak laki-laki bernama Akbar Ananta Arisandy yang lahir di Kotamobagu pada tanggal 23 April 2015. Yang kedua bernama Kayla Hira Arisandy yang lahir di Kotamobagu tanggal 31 Maret 2017 dan yang ketiga bernama Azfar Ramadhan Arisandy yang lahir pada tanggal 16 Mei 2020 di Kota Bekasi.