Indonesia Economic Journal
Vol. 2, No. 2, Tahun 2026
doi.org/10.63822/f1pgm726
Hal. 1862-1880
https://ojs.indopublishing.or.id/index.php/iej
eISSN 3090-4552 & pISSN 3090-4609

Strategi Penguatan Deradikalisasi Melalui Media Sosial oleh BNPT: Analisis SWOT

Agus Surono[1], Djuni Thamrin[2], Hapzi Ali[3]
Fakultas Ekonomi dan Bisnis, Universitas Bhayangkara Jakarata Raya[1.2.3]

*Email Korespodensi: neoyka87@gmail.com

Diterima: 04-07-2026 | Disetujui: 11-07-2026 | Diterbitkan: 13-07-2026

ABSTRACT

The rapid advancement of digital technologies has fundamentally transformed the landscape of violent extremism, shifting the dissemination of radical ideologies from conventional offline networks to digitally mediated platforms. Social media has become a strategic ecosystem through which extremist groups disseminate propaganda, recruit supporters, construct collective identities, and sustain transnational ideological networks through algorithm-driven communication. This transformation presents significant challenges for Indonesia's National Counter Terrorism Agency (BNPT), requiring the development of more adaptive, technology-oriented, and evidence-based deradicalization strategies. This study aims to identify the internal and external factors influencing the effectiveness of BNPT's social media-based deradicalization programs and to formulate strategic policy recommendations using a SWOT (Strengths, Weaknesses, Opportunities, and Threats) framework. The research adopts a qualitative descriptive approach based on a systematic literature review and document analysis. Data were collected from official BNPT reports, government regulations, national and international scholarly publications, reports from international organizations, and BNPT's official social media content. The findings indicate that BNPT's principal strengths include strong institutional legitimacy, extensive interagency and international partnerships, and access to credible counter-narrative resources. Nevertheless, the agency faces several internal challenges, including limited digital creative capabilities, relatively formal communication practices, insufficient personalization of digital content, and evaluation systems that emphasize program outputs rather than behavioral outcomes. Externally, significant opportunities arise from Indonesia's high internet penetration, expanding digital literacy initiatives, technological advances in artificial intelligence, and increasing collaboration with digital platforms and civil society organizations. Conversely, emerging threats include encrypted communication channels, algorithm-driven echo chambers, AI-generated extremist propaganda, and the growing phenomenon of lone-actor radicalization. Based on these findings, the study proposes a strategic framework centered on strengthening digital literacy, enhancing collaboration with content creators and online communities, developing audience-centered and humanistic counter-narratives, integrating AI-based cyber monitoring systems, and implementing outcome-oriented evaluation mechanisms. The study contributes to the growing literature on digital deradicalization by integrating strategic management perspectives with contemporary security studies and offers practical policy recommendations for strengthening institutional resilience against digital radicalization in the era of artificial intelligence.

Keywords: *Digital deradicalization; National Counter Terrorism Agency (BNPT); social media; SWOT analysis; counter-narrative; artificial intelligence.*

ABSTRAK

Perkembangan teknologi informasi dan komunikasi telah mengubah pola penyebaran ideologi radikal dari ruang fisik ke ruang digital. Media sosial menjadi instrumen utama kelompok ekstrem dalam menyebarkan propaganda, melakukan rekrutmen, serta membangun jaringan ideologis lintas wilayah. Kondisi tersebut menuntut Badan Nasional Penanggulangan Terorisme (BNPT) untuk mengembangkan strategi deradikalisasi yang adaptif dan berbasis teknologi. Penelitian ini bertujuan menganalisis faktor internal dan eksternal yang memengaruhi efektivitas program deradikalisasi melalui media sosial oleh BNPT serta merumuskan strategi penguatan yang relevan melalui pendekatan SWOT. Penelitian menggunakan metode deskriptif kualitatif dengan studi literatur terhadap laporan BNPT, regulasi pemerintah, jurnal nasional dan internasional, serta publikasi terkait radikalisasi digital. Hasil penelitian menunjukkan bahwa BNPT memiliki kekuatan berupa legitimasi hukum yang kuat, jejaring kerja sama lintas sektor, dan akses terhadap sumber kontra narasi yang autentik. Namun demikian, terdapat kelemahan berupa keterbatasan sumber daya kreatif digital, pendekatan komunikasi yang masih formal, dan evaluasi program yang belum berorientasi pada perubahan perilaku audiens. Peluang berasal dari tingginya penetrasi internet, dukungan *platform digital* terhadap penanganan konten ekstrem, dan meningkatnya kesadaran masyarakat mengenai bahaya radikalisme. Ancaman utama muncul dari penggunaan kanal komunikasi terenkripsi, algoritma media sosial yang menciptakan *echo chamber*, serta perkembangan kecerdasan buatan yang dimanfaatkan kelompok ekstrem untuk memproduksi propaganda secara masif. Strategi yang direkomendasikan meliputi penguatan literasi digital, kolaborasi dengan influencer dan komunitas kreatif, pengembangan konten visual-humanis, serta optimalisasi sistem pemantauan siber berbasis A*rtificial Intelligence.*

Kata kunci: Deradikalisasi, BNPT, Media Sosial, SWOT, Kontra Narasi

Bagaimana Cara Sitasi Artikel ini:

Surono, A. ., Thamrin, D., & Ali, H. . (2026). Strategi Penguatan Deradikalisasi Melalui Media Sosial oleh BNPT: Analisis SWOT. Indonesia Economic Journal, 2(2), 1862-1880. https://doi.org/10.63822/f1pgm726

PENDAHULUAN

Transformasi digital pada dua dekade terakhir telah mengubah secara fundamental lanskap keamanan global. Internet dan media sosial tidak lagi sekadar berfungsi sebagai sarana komunikasi, melainkan telah berkembang menjadi digital public sphere yang membentuk opini publik, identitas kolektif, mobilisasi politik, hingga dinamika keamanan nasional. Perkembangan Artificial Intelligence (AI), algoritma personalisasi, big data, komputasi awan, dan teknologi komunikasi berbasis platform telah mempercepat arus pertukaran informasi tanpa batas geografis maupun temporal. Fenomena tersebut melahirkan apa yang oleh Castells (2010) disebut sebagai network society, yaitu masyarakat yang hubungan sosial, ekonomi, dan politiknya semakin ditentukan oleh jaringan digital. Dalam masyarakat jaringan tersebut, distribusi kekuasaan tidak lagi dimonopoli oleh negara, tetapi juga oleh aktor non-negara yang mampu memanfaatkan teknologi informasi untuk memengaruhi persepsi publik dan membangun legitimasi politik.

Perubahan tersebut telah menggeser paradigma keamanan dari pendekatan tradisional yang berorientasi pada ancaman militer (traditional security) menuju paradigma keamanan non-tradisional (non-traditional security) yang mencakup ancaman siber, keamanan informasi, ekstremisme kekerasan, disinformasi, serta manipulasi opini publik melalui ruang digital (Buzan, Wæver, & de Wilde, 1998). Dalam perspektif Copenhagen School, ancaman keamanan tidak semata-mata ditentukan oleh keberadaan ancaman objektif, tetapi dibentuk melalui proses securitization, yaitu ketika suatu isu dikonstruksikan sebagai ancaman eksistensial melalui tindakan komunikasi (speech acts) sehingga memperoleh legitimasi untuk ditangani dengan kebijakan luar biasa (extraordinary measures). Dalam konteks ini, radikalisasi digital telah mengalami proses sekuritisasi di berbagai negara karena dipandang memiliki potensi mengancam stabilitas sosial, keamanan nasional, dan ketahanan demokrasi.

Di sisi lain, pendekatan Critical Security Studies mengingatkan bahwa keamanan tidak hanya berkaitan dengan perlindungan negara, tetapi juga keamanan manusia (human security). Penyebaran ideologi ekstrem melalui media sosial bukan hanya mengancam institusi negara, tetapi juga membahayakan individu melalui manipulasi identitas, eksploitasi psikologis, polarisasi sosial, serta normalisasi kekerasan. Oleh karena itu, strategi penanggulangan radikalisasi tidak cukup mengandalkan pendekatan represif, tetapi harus mengintegrasikan dimensi pencegahan, pemberdayaan masyarakat, literasi digital, serta pembangunan resiliensi sosial sebagai bagian dari strategi keamanan yang komprehensif.

Dalam perkembangan ilmu terorisme kontemporer, media sosial telah menjadi arena strategis bagi kelompok ekstrem untuk menjalankan berbagai aktivitas ideologis. Evolusi terorisme dari organisasi hierarkis menuju jaringan digital (networked terrorism) menunjukkan bahwa internet telah mengubah hampir seluruh siklus aktivitas kelompok ekstrem, mulai dari propaganda, rekrutmen, pelatihan, penggalangan dana, koordinasi operasi, hingga legitimasi ideologi (Conway, 2017; Weimann, 2016). Hoffman (2006) menjelaskan bahwa karakteristik utama terorisme modern terletak pada kemampuannya mengeksploitasi teknologi komunikasi guna menciptakan efek psikologis yang jauh lebih besar dibandingkan kapasitas fisik serangan itu sendiri. Dalam era digital, propaganda bahkan sering kali memiliki dampak strategis yang lebih luas dibandingkan tindakan kekerasan yang dilakukan.

Fenomena tersebut sejalan dengan berkembangnya konsep online radicalization, yaitu proses bertahap ketika individu mengalami perubahan sikap, keyakinan, dan perilaku menuju penerimaan terhadap penggunaan kekerasan melalui interaksi yang berlangsung di ruang digital (Neumann, 2013). Berbeda dengan model radikalisasi konvensional yang mengandalkan interaksi tatap muka, radikalisasi daring

berlangsung secara lebih individual, personal, anonim, dan sering kali tidak melibatkan struktur organisasi formal. Hal ini menjadikan proses deteksi maupun intervensi menjadi jauh lebih kompleks.

Berbagai model teoritis telah berupaya menjelaskan proses tersebut. Staircase to Terrorism Model yang dikembangkan oleh Moghaddam (2005) menggambarkan bahwa seseorang bergerak secara bertahap dari rasa ketidakadilan menuju penerimaan terhadap tindakan terorisme melalui serangkaian proses psikologis. Sementara itu, Four-Stage Radicalization Model dari Silber dan Bhatt (2007) menjelaskan bahwa proses radikalisasi terdiri atas tahap pre-radicalization, self-identification, indoctrination, dan jihadization. Dalam konteks digital, setiap tahapan tersebut dapat berlangsung jauh lebih cepat karena diperkuat oleh algoritma media sosial yang secara terus-menerus menyediakan konten yang memperkuat preferensi pengguna.

Perkembangan literatur terbaru menunjukkan bahwa algoritma media sosial bukan lagi sekadar instrumen teknis, melainkan telah menjadi aktor yang memengaruhi dinamika keamanan digital. Melalui mekanisme algorithmic amplification, echo chamber, dan filter bubble, sistem rekomendasi platform digital secara tidak langsung memperbesar peluang pengguna terpapar secara berulang terhadap narasi yang seragam (Cinelli et al., 2021). Paparan berulang tersebut memperkuat confirmation bias, meningkatkan polarisasi, dan mempercepat pembentukan identitas kelompok yang eksklusif. Ribeiro et al. (2020) menunjukkan bahwa proses migrasi pengguna dari komunitas daring biasa menuju komunitas ekstrem sering kali difasilitasi oleh sistem rekomendasi platform digital, bukan semata-mata karena pilihan individual pengguna.

Fenomena ini dapat dijelaskan melalui Social Identity Theory (Tajfel & Turner, 1979), yang menyatakan bahwa individu cenderung mengidentifikasi dirinya dengan kelompok yang dianggap memberikan rasa memiliki (sense of belonging). Di ruang digital, identitas tersebut diperkuat melalui interaksi yang berulang, validasi sosial, serta eksklusivitas kelompok yang dibangun melalui narasi ideologis. Semakin kuat identitas kelompok terbentuk, semakin tinggi pula kemungkinan individu menerima legitimasi penggunaan kekerasan demi mempertahankan identitas tersebut.

Selain itu, Social Learning Theory (Bandura, 1977) menjelaskan bahwa perilaku radikal dapat dipelajari melalui observasi terhadap model perilaku yang terus-menerus muncul di media sosial. Konten propaganda, video kekerasan, simbol ideologis, maupun narasi heroisme kelompok ekstrem berfungsi sebagai observational learning yang memengaruhi pembentukan sikap individu. Proses ini menjadi semakin efektif ketika didukung oleh algoritma yang secara otomatis meningkatkan frekuensi paparan terhadap konten serupa.

Dalam perspektif komunikasi strategis, penyebaran propaganda ekstrem juga dapat dipahami melalui Framing Theory dan Agenda Setting Theory. Kelompok ekstrem tidak hanya menyampaikan informasi, tetapi membingkai realitas sedemikian rupa sehingga menciptakan persepsi mengenai adanya ketidakadilan, ancaman terhadap identitas kelompok, maupun kewajiban moral untuk melakukan tindakan tertentu. Dengan demikian, media sosial tidak hanya menjadi saluran komunikasi, tetapi juga arena kontestasi makna (battle of narratives) antara negara dan kelompok ekstrem.

Indonesia merupakan salah satu negara dengan tingkat penetrasi internet terbesar di dunia sehingga menghadapi tantangan yang sangat kompleks dalam menjaga keamanan ruang digital. Jumlah pengguna internet yang telah melampaui 220 juta orang memperlihatkan bahwa ruang digital Indonesia merupakan salah satu ekosistem informasi terbesar di Asia Tenggara. Di sisi lain, tingginya penggunaan media sosial, khususnya oleh generasi muda, meningkatkan peluang penyebaran propaganda ekstrem melalui mekanisme

algoritmik yang sulit dikendalikan. Dalam konteks tersebut, ancaman keamanan tidak lagi bersifat fisik semata, tetapi juga bersifat kognitif (cognitive security), yaitu upaya memengaruhi cara berpikir, persepsi, dan sistem nilai masyarakat melalui manipulasi informasi digital.

Sebagai lembaga yang memiliki mandat utama dalam pencegahan terorisme, BNPT telah mengembangkan berbagai strategi kontra-radikalisasi dan deradikalisasi berbasis media digital. Namun, sebagian besar strategi tersebut masih didominasi pendekatan komunikasi publik dan kontra-narasi, sementara perkembangan AI generatif, deepfake, synthetic media, bot networks, serta perubahan algoritma media sosial menciptakan tantangan baru yang belum sepenuhnya terakomodasi dalam desain kebijakan yang ada.

Berbagai penelitian sebelumnya telah mengevaluasi efektivitas kontra-narasi (Schmid, 2013), deradikalisasi (Sumpter, 2017), serta faktor-faktor psikososial radikalisasi digital (Wolfowicz et al., 2022). Akan tetapi, penelitian-penelitian tersebut lebih banyak menitikberatkan pada efektivitas program atau karakteristik individu. Masih sangat terbatas penelitian yang mengintegrasikan perspektif Strategic Management, Security Studies, dan Digital Governance untuk memetakan kapasitas organisasi dalam menghadapi ancaman radikalisasi digital yang terus berevolusi.

Oleh karena itu, penelitian ini memosisikan analisis SWOT bukan sekadar sebagai alat formulasi strategi organisasi, tetapi sebagai kerangka analitis yang menghubungkan dinamika lingkungan strategis digital, kapasitas kelembagaan BNPT, perkembangan teknologi AI, algoritma media sosial, serta ancaman keamanan non-tradisional. Dengan pendekatan tersebut, penelitian ini tidak hanya memberikan rekomendasi kebijakan bagi BNPT, tetapi juga memperluas diskursus mengenai tata kelola keamanan digital (digital security governance) dalam menghadapi transformasi radikalisasi pada era kecerdasan buatan.

Kontribusi teoretis penelitian ini terletak pada pengintegrasian perspektif Security Studies, teori radikalisasi, komunikasi digital, dan manajemen strategis ke dalam kerangka SWOT untuk menjelaskan bagaimana organisasi keamanan negara dapat meningkatkan kapasitas adaptifnya terhadap ancaman radikalisasi berbasis platform digital. Sementara itu, kontribusi praktis penelitian ini diharapkan dapat menjadi dasar penyusunan strategi deradikalisasi digital yang lebih adaptif, kolaboratif, berbasis bukti (evidence-based policy), serta responsif terhadap dinamika teknologi komunikasi kontemporer.

Konstruk Teoritis Penelitian

Penelitian ini dibangun atas asumsi bahwa radikalisasi digital merupakan fenomena multidimensional yang tidak dapat dijelaskan hanya melalui satu perspektif teoritis. Perubahan karakter ancaman dari ruang fisik menuju ruang digital telah menggeser paradigma keamanan dari pendekatan konvensional menuju keamanan non-tradisional (non-traditional security), sehingga diperlukan kerangka teoritis yang mampu menjelaskan hubungan antara perkembangan teknologi digital, dinamika radikalisasi, kapasitas organisasi, dan strategi penanggulangannya secara terpadu. Oleh karena itu, penelitian ini mengintegrasikan empat perspektif teoritis, yaitu *Non-Traditional Security Theory, Online Radicalization Theory, Strategic Communication Theory, dan Strategic Management Framework (SWOT)* sebagai dasar konseptual dalam merumuskan strategi penguatan deradikalisasi digital BNPT.

Landasan pertama berasal dari *Non-Traditional Security Theory* yang dikembangkan oleh Barry Buzan, Ole Wæver, dan Jaap de Wilde (1998). Perspektif ini menjelaskan bahwa ancaman keamanan kontemporer tidak lagi didominasi oleh agresi militer antarnegara, melainkan berkembang menjadi

ancaman lintas sektor seperti keamanan siber, ekstremisme, terorisme, disinformasi, migrasi, perubahan iklim, dan kejahatan transnasional. Dalam kerangka tersebut, media sosial dipandang sebagai ruang strategis yang dapat memengaruhi stabilitas politik, kohesi sosial, serta keamanan nasional. Radikalisasi digital menjadi ancaman keamanan karena mampu memengaruhi persepsi publik, membentuk identitas kolektif, dan menciptakan legitimasi terhadap penggunaan kekerasan tanpa harus melalui kontak fisik antaranggota kelompok.

Lebih lanjut, perspektif *Securitization Theory dari Copenhagen School* memberikan penjelasan bahwa suatu isu berubah menjadi isu keamanan ketika aktor yang memiliki otoritas mendefinisikannya sebagai ancaman eksistensial yang memerlukan respons luar biasa (extraordinary measures). Dalam konteks penelitian ini, penyebaran propaganda ekstrem melalui media sosial dipandang sebagai ancaman terhadap keamanan nasional karena berpotensi meningkatkan proses radikalisasi, memperluas jaringan ekstremisme, dan melemahkan ketahanan sosial masyarakat. Dengan demikian, strategi deradikalisasi BNPT merupakan bentuk respons keamanan negara terhadap proses sekuritisasi ancaman digital yang berkembang secara dinamis.

Perspektif kedua adalah *Online Radicalization Theory*, yang menjelaskan mekanisme transformasi individu menuju penerimaan terhadap ideologi ekstrem melalui interaksi digital. Conway (2017) mendefinisikan radikalisasi daring sebagai proses ketika internet dan media sosial menjadi medium utama dalam penyebaran propaganda, perekrutan anggota, penguatan identitas kelompok, serta mobilisasi tindakan ekstrem. Neumann (2013) menambahkan bahwa ruang digital telah menghilangkan berbagai hambatan geografis, sehingga individu dapat mengalami proses radikalisasi secara mandiri (self-radicalization) melalui konsumsi konten daring tanpa keterlibatan langsung organisasi ekstrem.

Penelitian ini juga mengadopsi Staircase to Terrorism Model yang dikembangkan Moghaddam (2005). Model tersebut menjelaskan bahwa radikalisasi berlangsung secara bertahap, dimulai dari persepsi ketidakadilan, berkembang menjadi frustrasi, identifikasi kelompok, legitimasi kekerasan, hingga akhirnya menerima tindakan terorisme sebagai pilihan yang sah. Dalam lingkungan digital, tahapan tersebut dapat berlangsung lebih cepat karena pengguna terus-menerus terpapar informasi yang diperkuat oleh algoritma media sosial.

Proses tersebut diperjelas oleh konsep algorithmic amplification, echo chamber, dan filter bubble yang menjelaskan bagaimana algoritma platform digital meningkatkan intensitas paparan terhadap konten yang sejalan dengan preferensi pengguna. Semakin tinggi frekuensi paparan terhadap narasi ekstrem, semakin besar kemungkinan terbentuknya confirmation bias, polarisasi sosial, dan normalisasi terhadap ideologi kekerasan. Dengan demikian, teknologi digital tidak hanya berfungsi sebagai media komunikasi, tetapi juga menjadi faktor struktural yang mempercepat proses radikalisasi.

Perspektif ketiga adalah *Strategic Communication Theory*. Teori ini menjelaskan bahwa keberhasilan kontra-radikalisasi tidak hanya bergantung pada penyampaian informasi, tetapi juga pada kemampuan membangun makna, kredibilitas, kepercayaan, dan keterlibatan publik. Dalam konteks media sosial, perang melawan ekstremisme pada hakikatnya merupakan kompetisi narasi (battle of narratives). Kelompok ekstrem berupaya membangun legitimasi ideologinya melalui propaganda yang emosional, personal, dan persuasif, sedangkan pemerintah harus mampu menghadirkan kontra-narasi yang kredibel, adaptif, dan sesuai dengan karakteristik audiens digital. Oleh karena itu, efektivitas deradikalisasi sangat dipengaruhi oleh kualitas komunikasi strategis, kolaborasi multipemangku kepentingan, literasi digital masyarakat, serta kemampuan memanfaatkan teknologi digital secara adaptif.

Perspektif keempat berasal dari Strategic Management, khususnya pendekatan SWOT yang dikembangkan oleh Humphrey (1960-an). Berbeda dengan tiga teori sebelumnya yang menjelaskan fenomena radikalisasi, SWOT digunakan sebagai kerangka analisis strategis untuk mengevaluasi kesiapan organisasi dalam merespons perubahan lingkungan. SWOT memungkinkan identifikasi kekuatan (strengths) dan kelemahan (weaknesses) internal organisasi, sekaligus peluang (opportunities) dan ancaman (threats) yang berasal dari lingkungan eksternal. Dalam penelitian ini, perkembangan Artificial Intelligence, algoritma media sosial, dinamika komunikasi digital, kolaborasi lintas sektor, regulasi pemerintah, serta evolusi strategi propaganda kelompok ekstrem diposisikan sebagai faktor lingkungan strategis yang memengaruhi efektivitas kebijakan deradikalisasi BNPT.

Integrasi keempat perspektif tersebut menghasilkan suatu konstruk teoritis yang menjelaskan bahwa transformasi teknologi digital mengubah karakter ancaman keamanan menjadi lebih kompleks melalui proses radikalisasi daring yang diperkuat oleh algoritma media sosial. Ancaman tersebut menuntut organisasi keamanan negara untuk membangun kapasitas adaptif melalui komunikasi strategis, inovasi digital, penguatan kolaborasi, dan formulasi strategi organisasi yang responsif terhadap perubahan lingkungan. Dengan demikian, efektivitas deradikalisasi digital tidak hanya ditentukan oleh kualitas kontra-narasi yang dibangun, tetapi juga oleh kemampuan organisasi dalam membaca perubahan lingkungan strategis, mengoptimalkan sumber daya internal, serta memanfaatkan peluang teknologi untuk memperkuat ketahanan masyarakat terhadap propaganda ekstrem.

Berdasarkan konstruk teoritis tersebut, penelitian ini memandang bahwa strategi penguatan deradikalisasi digital merupakan hasil interaksi dinamis antara ancaman keamanan digital, mekanisme radikalisasi daring, kapasitas komunikasi strategis BNPT, dan kemampuan organisasi dalam merumuskan strategi adaptif melalui analisis SWOT. Konstruk ini menjadi landasan konseptual untuk mengidentifikasi faktor internal dan eksternal BNPT sekaligus merumuskan strategi deradikalisasi yang lebih efektif, kolaboratif, dan adaptif terhadap perkembangan teknologi digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan desain studi literatur sistematis (*systematic literature study*) yang dipadukan dengan analisis dokumen (*document analysis*). Pendekatan ini dipilih karena memungkinkan peneliti memperoleh pemahaman yang komprehensif mengenai dinamika radikalisasi digital, strategi deradikalisasi berbasis media sosial, serta kapasitas kelembagaan Badan Nasional Penanggulangan Terorisme (BNPT) dalam menghadapi perkembangan teknologi komunikasi digital. Pendekatan kualitatif dinilai sesuai untuk mengeksplorasi fenomena yang kompleks, kontekstual, dan multidimensional, terutama ketika penelitian bertujuan mengidentifikasi faktor-faktor strategis sebagai dasar perumusan kebijakan (Creswell & Poth, 2018; Bowen, 2009).

Sumber Data

Penelitian memanfaatkan data sekunder yang diperoleh dari berbagai sumber yang memiliki kredibilitas akademik dan institusional. Penggunaan berbagai jenis dokumen dimaksudkan untuk menghasilkan pemahaman yang lebih komprehensif melalui triangulasi sumber. Sumber data meliputi:

1. Laporan resmi BNPT yang berkaitan dengan program kontra-radikalisasi, deradikalisasi, dan pencegahan ekstremisme berbasis kekerasan;

2. Dokumen kebijakan dan regulasi pemerintah yang mengatur penanggulangan terorisme, keamanan siber, serta transformasi digital;
3. Artikel ilmiah yang dipublikasikan pada jurnal nasional terakreditasi dan jurnal internasional bereputasi yang membahas radikalisasi daring, komunikasi strategis, keamanan digital, serta deradikalisasi;
4. Publikasi organisasi internasional, seperti Perserikatan Bangsa-Bangsa (United Nations), United Nations Office of Counter-Terrorism (UNOCT), United Nations Office on Drugs and Crime (UNODC), Global Counterterrorism Forum (GCTF), dan lembaga internasional lain yang relevan;
5. Konten digital pada media sosial resmi BNPT yang digunakan sebagai representasi implementasi komunikasi publik dan kontra-narasi digital.

Strategi Penelusuran Literatur

Proses identifikasi literatur dilakukan secara sistematis menggunakan beberapa pangkalan data ilmiah internasional, antara lain *Scopus, Web of Science, ScienceDirect, SpringerLink, Taylor & Francis Online, Wiley Online Library, serta Google Scholar* sebagai sumber pelengkap. Penelusuran dilakukan menggunakan kombinasi kata kunci, antara lain online radicalization, digital radicalization, counter-radicalization, deradicalization, violent extremism, social media, artificial intelligence, digital security, strategic communication, counter-terrorism, BNPT, dan SWOT analysis.

Untuk menjaga relevansi kajian, penelitian memprioritaskan publikasi yang diterbitkan dalam kurun waktu 2015–2025, dengan tetap memasukkan literatur klasik yang menjadi landasan konseptual, seperti karya Buzan, Wæver, Castells, Hoffman, Weimann, Conway, dan Moghaddam.

Literatur dipilih berdasarkan beberapa kriteria inklusi, yaitu: (1) membahas radikalisasi digital, deradikalisasi, komunikasi strategis, atau keamanan digital; (2) diterbitkan pada jurnal yang melalui proses peer review atau berasal dari lembaga resmi; (3) memiliki relevansi langsung dengan tujuan penelitian; dan (4) tersedia dalam bentuk teks lengkap (full text). Sebaliknya, publikasi yang bersifat opini, tidak memiliki proses penelaahan ilmiah, atau tidak berkaitan langsung dengan fokus penelitian tidak diikutsertakan dalam analisis.

Teknik Analisis Data

Analisis data dilakukan melalui analisis isi kualitatif (qualitative content analysis) yang dipadukan dengan analisis SWOT sebagai kerangka formulasi strategi. Analisis isi digunakan untuk mengidentifikasi tema-tema utama, pola hubungan, serta faktor-faktor yang memengaruhi efektivitas deradikalisasi digital BNPT. Selanjutnya, hasil identifikasi tersebut diklasifikasikan ke dalam empat dimensi SWOT, yaitu *Strength*s (kekuatan), *Weakness*es (kelemahan), Opportunities (peluang), dan Threats (ancaman).

Proses analisis dilakukan melalui beberapa tahapan yang saling berurutan. Pertama, seluruh dokumen dikumpulkan, diseleksi, dan dikategorikan berdasarkan relevansinya terhadap fokus penelitian. Kedua, dilakukan proses coding terhadap informasi yang berkaitan dengan kapasitas organisasi BNPT, perkembangan teknologi digital, karakteristik media sosial, kebijakan pemerintah, pola radikalisasi daring, serta tantangan implementasi deradikalisasi.

Ketiga, hasil coding dianalisis secara tematik untuk mengidentifikasi faktor-faktor internal (kekuatan dan kelemahan) maupun faktor-faktor eksternal (peluang dan ancaman). Keempat, faktor-faktor strategis tersebut dipetakan ke dalam Matriks SWOT sehingga menghasilkan empat alternatif strategi,

yaitu:
1. Strategi SO (*Strength–Opportunity*), yaitu strategi yang memanfaatkan kekuatan organisasi untuk mengoptimalkan peluang eksternal;
2. Strategi WO (Weakness–Opportunity), yaitu strategi yang memanfaatkan peluang guna mengatasi kelemahan internal;
3. Strategi ST (Strength–Threat), yaitu strategi yang menggunakan kekuatan organisasi untuk menghadapi ancaman eksternal; dan
4. Strategi WT (Weakness–Threat), yaitu strategi defensif yang bertujuan meminimalkan kelemahan organisasi sekaligus mengurangi dampak ancaman yang dihadapi.

Tahap terakhir adalah interpretasi hasil analisis untuk merumuskan rekomendasi kebijakan yang adaptif terhadap perkembangan teknologi digital, pemanfaatan Artificial Intelligence, dinamika algoritma media sosial, serta perubahan pola komunikasi masyarakat dalam konteks pencegahan radikalisasi daring.

Keabsahan Data

Untuk meningkatkan trustworthiness penelitian, dilakukan triangulasi sumber dengan membandingkan informasi yang diperoleh dari dokumen pemerintah, publikasi akademik, laporan organisasi internasional, dan dokumen resmi BNPT. Selain itu, interpretasi hasil dilakukan secara iteratif dengan membandingkan berbagai perspektif teoritis dalam studi keamanan, radikalisasi, komunikasi strategis, dan manajemen strategis sehingga menghasilkan temuan yang lebih kredibel, konsisten, dan dapat dipertanggungjawabkan secara ilmiah.

HASIL DAN PEMBAHASAN

Identifikasi Faktor Strategis Internal dan Eksternal

Analisis SWOT dalam penelitian ini digunakan untuk mengidentifikasi kondisi strategis yang memengaruhi efektivitas pelaksanaan deradikalisasi digital oleh Badan Nasional Penanggulangan Terorisme (BNPT). Identifikasi dilakukan melalui analisis berbagai dokumen kebijakan, laporan kelembagaan, publikasi ilmiah, serta literatur mengenai radikalisasi digital dan komunikasi strategis. Hasil analisis menunjukkan bahwa efektivitas program deradikalisasi melalui media sosial dipengaruhi oleh kombinasi faktor internal organisasi dan dinamika lingkungan eksternal yang terus berkembang seiring dengan transformasi teknologi digital.

Faktor Internal

Faktor internal mencerminkan kapasitas organisasi yang secara langsung memengaruhi kemampuan BNPT dalam merancang dan mengimplementasikan strategi deradikalisasi berbasis media sosial. Analisis menunjukkan bahwa BNPT memiliki sejumlah kekuatan strategis yang menjadi modal utama dalam menghadapi ancaman radikalisasi digital.

Kekuatan pertama terletak pada legitimasi hukum yang kuat. Sebagai lembaga yang dibentuk berdasarkan kerangka hukum nasional untuk melaksanakan pencegahan dan penanggulangan terorisme, BNPT memiliki kewenangan institusional yang jelas dalam mengoordinasikan berbagai program kontra-radikalisasi dan deradikalisasi. Legitimasi tersebut memberikan dasar yang kuat bagi pengembangan kebijakan, koordinasi lintas kementerian dan lembaga, serta kolaborasi dengan pemerintah daerah, aparat

penegak hukum, lembaga pendidikan, organisasi masyarakat sipil, dan sektor swasta.

Kekuatan kedua adalah dukungan pemerintah yang relatif konsisten terhadap agenda pencegahan ekstremisme berbasis kekerasan. Dukungan tersebut tercermin dalam penyediaan regulasi, penguatan kelembagaan, alokasi sumber daya, serta integrasi isu pencegahan terorisme ke dalam berbagai kebijakan nasional. Kondisi ini memberikan peluang bagi BNPT untuk mengembangkan strategi deradikalisasi yang lebih terintegrasi dengan kebijakan transformasi digital nasional.

Selanjutnya, jejaring kerja sama nasional dan internasional menjadi aset strategis yang memperkuat kapasitas organisasi. BNPT telah membangun kolaborasi dengan berbagai kementerian, perguruan tinggi, organisasi masyarakat sipil, perusahaan teknologi, media massa, dan organisasi internasional. Kolaborasi tersebut memungkinkan pertukaran pengetahuan, pengembangan kapasitas, serta adopsi praktik-praktik terbaik (best practices) dalam penanggulangan radikalisasi digital.

Kekuatan lain yang bersifat unik adalah akses terhadap mantan narapidana terorisme dan penyintas proses deradikalisasi. Kelompok ini memiliki pengalaman empiris yang autentik mengenai proses rekrutmen, indoktrinasi, hingga pelepasan dari jaringan ekstrem. Dalam perspektif komunikasi strategis, pengalaman tersebut memiliki tingkat kredibilitas (source credibility) yang tinggi sehingga berpotensi menghasilkan kontra-narasi yang lebih persuasif dibandingkan pesan yang disampaikan secara formal oleh institusi pemerintah.

Selain itu, pengalaman panjang BNPT dalam melaksanakan program deradikalisasi menjadi modal institusional yang penting. Pengalaman tersebut menghasilkan akumulasi pengetahuan mengenai karakteristik kelompok sasaran, pola penyebaran ideologi ekstrem, pendekatan rehabilitasi, serta mekanisme kolaborasi dengan berbagai pemangku kepentingan. Modal kelembagaan ini menjadi fondasi bagi pengembangan strategi yang lebih adaptif terhadap perubahan lingkungan digital.

Meskipun demikian, analisis juga mengidentifikasi sejumlah kelemahan internal yang berpotensi mengurangi efektivitas strategi deradikalisasi digital. Kelemahan pertama berkaitan dengan karakter komunikasi digital yang masih cenderung formal dan birokratis. Pola komunikasi seperti ini kurang sesuai dengan karakteristik media sosial yang mengedepankan interaktivitas, kreativitas, personalisasi, dan kedekatan emosional dengan audiens. Akibatnya, pesan kontra-radikalisasi sering kali kurang mampu bersaing dengan konten ekstrem yang dirancang secara lebih menarik, emosional, dan mudah dibagikan.

Kelemahan kedua adalah keterbatasan sumber daya manusia yang memiliki kompetensi pada bidang komunikasi digital kreatif, analisis media sosial, kecerdasan buatan, dan pemasaran digital. Transformasi ekosistem komunikasi menuntut organisasi keamanan untuk tidak hanya memiliki keahlian substantif mengenai terorisme, tetapi juga kemampuan memanfaatkan teknologi digital secara inovatif. Kesenjangan kompetensi ini berpotensi menghambat kemampuan organisasi dalam menghasilkan konten yang relevan dengan karakteristik pengguna media sosial.

Selanjutnya, penelitian menemukan bahwa personalisasi konten digital masih relatif rendah. Sebagian besar pesan kontra-radikalisasi disampaikan secara umum tanpa mempertimbangkan segmentasi audiens berdasarkan usia, latar belakang sosial, preferensi platform, maupun karakteristik perilaku digital. Padahal, berbagai penelitian menunjukkan bahwa efektivitas komunikasi digital sangat dipengaruhi oleh kemampuan menyesuaikan pesan dengan karakteristik kelompok sasaran.

Kelemahan berikutnya berkaitan dengan sistem evaluasi program yang masih lebih berorientasi pada indikator keluaran (output) dibandingkan perubahan perilaku (outcome) maupun dampak jangka panjang (impact). Pengukuran keberhasilan yang hanya didasarkan pada jumlah kegiatan, jumlah peserta,

atau jumlah konten yang diproduksi belum mampu menggambarkan efektivitas program dalam meningkatkan resiliensi masyarakat terhadap propaganda ekstrem.

Selain itu, penelitian juga mengidentifikasi pemanfaatan teknologi Artificial Intelligence yang masih terbatas. Padahal, perkembangan AI menawarkan berbagai peluang untuk melakukan analisis sentimen, deteksi dini narasi ekstrem, pemetaan jejaring digital, segmentasi audiens, hingga optimalisasi distribusi kontra-narasi secara lebih presisi. Keterbatasan pemanfaatan teknologi tersebut menyebabkan kemampuan organisasi dalam merespons dinamika propaganda digital belum sepenuhnya optimal.

Faktor Eksternal

Selain faktor internal, efektivitas deradikalisasi digital juga dipengaruhi oleh perubahan lingkungan eksternal yang menghadirkan peluang sekaligus ancaman bagi organisasi.

Dari sisi peluang, tingginya penetrasi internet dan media sosial di Indonesia menciptakan ruang komunikasi yang sangat luas bagi penyebaran pesan-pesan kontra-radikalisasi. Besarnya jumlah pengguna internet memungkinkan BNPT menjangkau kelompok sasaran secara lebih cepat, efisien, dan berkelanjutan dibandingkan pendekatan konvensional.

Peluang berikutnya berasal dari dukungan berbagai platform digital global yang dalam beberapa tahun terakhir semakin aktif mengembangkan kebijakan moderasi konten, penghapusan materi ekstremisme, serta kerja sama dengan pemerintah dan organisasi internasional dalam upaya pencegahan penyebaran propaganda terorisme. Kolaborasi semacam ini membuka kesempatan bagi BNPT untuk memperkuat efektivitas strategi komunikasi digital melalui mekanisme berbagi informasi dan pengembangan kapasitas.

Penelitian juga menemukan bahwa pertumbuhan komunitas kreatif digital merupakan peluang strategis yang belum dimanfaatkan secara optimal. Komunitas kreator konten, influencer, animator, ilustrator, maupun pengembang media digital memiliki kemampuan menghasilkan pesan yang lebih menarik, komunikatif, dan sesuai dengan karakteristik generasi muda. Pelibatan aktor-aktor kreatif tersebut dapat memperkuat efektivitas kontra-narasi melalui pendekatan yang lebih partisipatif.

Selain itu, meningkatnya literasi digital masyarakat memberikan peluang bagi penguatan ketahanan sosial terhadap penyebaran propaganda ekstrem. Berbagai program literasi digital yang dilaksanakan pemerintah, lembaga pendidikan, organisasi masyarakat sipil, dan sektor swasta berpotensi meningkatkan kemampuan masyarakat dalam melakukan verifikasi informasi, mengenali manipulasi digital, serta menolak narasi ekstrem yang beredar di media sosial.

Peluang strategis lainnya berasal dari perkembangan teknologi Artificial Intelligence. Teknologi ini memungkinkan analisis data dalam skala besar, identifikasi pola penyebaran propaganda, deteksi dini terhadap konten ekstrem, hingga optimalisasi penyusunan kontra-narasi berbasis karakteristik audiens. Apabila dimanfaatkan secara tepat, AI dapat meningkatkan efektivitas, efisiensi, dan ketepatan sasaran program deradikalisasi digital.

Di sisi lain, lingkungan eksternal juga menghadirkan berbagai ancaman yang semakin kompleks. Ancaman pertama adalah semakin luasnya penggunaan platform komunikasi terenkripsi yang menyulitkan proses deteksi, pemantauan, dan intervensi terhadap aktivitas kelompok ekstrem. Migrasi komunikasi dari platform terbuka menuju aplikasi dengan sistem enkripsi tinggi menyebabkan penyebaran propaganda dan proses rekrutmen menjadi lebih tertutup.

Ancaman berikutnya berasal dari fenomena echo chamber dan filter bubble yang dihasilkan oleh

algoritma media sosial. Mekanisme ini menyebabkan pengguna terus-menerus menerima informasi yang memperkuat keyakinan yang telah dimiliki sehingga mempercepat polarisasi sosial dan meningkatkan risiko radikalisasi.

Perkembangan *Artificial Intelligence* generatif, termasuk teknologi deepfake, synthetic media, dan automated bots, juga menjadi tantangan baru bagi strategi deradikalisasi. Teknologi tersebut memungkinkan kelompok ekstrem memproduksi propaganda yang semakin realistis, personal, dan sulit dibedakan dari informasi yang autentik sehingga meningkatkan kompleksitas upaya deteksi maupun penanggulangannya.

Ancaman lainnya adalah meningkatnya fenomena lone wolf terrorism, yaitu individu yang melakukan aksi teror tanpa keterikatan langsung dengan struktur organisasi formal. Pola ini umumnya dipicu oleh proses radikalisasi mandiri melalui konsumsi konten digital sehingga jauh lebih sulit diidentifikasi melalui pendekatan keamanan konvensional.

Terakhir, kecepatan penyebaran informasi di media sosial menyebabkan propaganda ekstrem dapat menyebar secara viral dalam waktu yang sangat singkat. Kondisi tersebut menuntut organisasi pemerintah untuk memiliki kemampuan merespons secara cepat, adaptif, dan berbasis data agar kontra-narasi mampu hadir sebelum propaganda ekstrem memperoleh perhatian publik yang luas.

Secara keseluruhan, hasil identifikasi faktor internal dan eksternal menunjukkan bahwa keberhasilan deradikalisasi digital tidak hanya ditentukan oleh kapasitas internal BNPT, tetapi juga oleh kemampuan organisasi dalam beradaptasi terhadap perubahan lingkungan digital yang berkembang sangat cepat. Oleh karena itu, strategi yang dirumuskan perlu mengintegrasikan penguatan kapasitas organisasi, pemanfaatan teknologi digital, kolaborasi multipemangku kepentingan, serta inovasi komunikasi strategis agar mampu meningkatkan efektivitas pencegahan radikalisasi pada era transformasi digital.

Tabel 1. Matriks Strategi SWOT Penguatan Deradikalisasi Melalui Media Sosial oleh BNPT

Strategi SO (Strengths–Opportunities)	**Strategi WO (Weaknesses–Opportunities)**
Memanfaatkan legitimasi hukum dan jejaring kelembagaan untuk memperluas kolaborasi dengan platform digital dalam kampanye perdamaian dan kontra narasi.	Meningkatkan adaptasi komunikasi digital melalui storytelling, konten visual kreatif, dan kolaborasi dengan influencer untuk menjangkau generasi muda.
Mengoptimalkan akses terhadap testimoni mantan narapidana terorisme sebagai materi kampanye deradikalisasi berbasis pengalaman nyata.	Mengembangkan kapasitas SDM kreatif digital dan sistem evaluasi berbasis dampak perilaku audiens.
Strategi ST (Strengths–Threats)	**Strategi WT (Weaknesses–Threats)**
Memperkuat koordinasi patroli siber dan kerja sama lintas lembaga untuk mendeteksi serta menanggulangi penyebaran konten radikal di ruang digital.	Mengembangkan sistem pemantauan dan deteksi dini berbasis Artificial Intelligence (AI) guna mengantisipasi propaganda radikal yang semakin adaptif.
Memanfaatkan legitimasi kelembagaan untuk memperkuat kebijakan penanganan konten ekstrem dan meningkatkan literasi keamanan	Meningkatkan program literasi digital keluarga (digital parenting) dan kemampuan komunikasi digital BNPT.

digital masyarakat.	

Sumber: Hasil Analisis Peneliti (2026)

Tabel 2. Matriks Analisis SWOT Penguatan Deradikalisasi Melalui Media Sosial oleh BNPT

Faktor Internal dan Eksternal	**Kekuatan (Strengths)**	**Kelemahan (Weaknesses)**	**Peluang (Opportunities)**	**Ancaman (Threats)**
Faktor Strategis	1. Legitimasi hukum yang kuat 2. Jejaring kerja sama kelembagaan 3. Testimoni mantan napiter	1. Komunikasi formal 2. Tim kreatif terbatas 3. Evaluasi berorientasi output	1. Penetrasi internet tinggi 2. Dukungan platform digital 3. Kesadaran masyarakat meningkat	1. Kanal terenkripsi 2. Echo chamber 3. Konten radikal berbasis AI
Strategi SO	BNPT memanfaatkan legitimasi hukum dan jejaring kelembagaan untuk membangun kolaborasi dengan platform digital global.			
Strategi WO	BNPT meningkatkan adaptasi komunikasi melalui storytelling, konten visual humanis, dan kolaborasi dengan influencer.			
Strategi ST	BNPT memperkuat patroli siber dan kerja sama lintas sektor untuk menghadapi propaganda radikal.			
Strategi WT	BNPT mengembangkan sistem pemantauan berbasis AI dan memperkuat literasi digital keluarga.			

Sumber: Data Penelitian Diolah (2026)

Formulasi Strategi Penguatan Deradikalisasi Digital

Hasil analisis SWOT menunjukkan bahwa efektivitas strategi deradikalisasi melalui media sosial tidak hanya ditentukan oleh kapasitas internal Badan Nasional Penanggulangan Terorisme (BNPT), tetapi juga oleh kemampuan organisasi dalam mengantisipasi perubahan lingkungan strategis yang dipengaruhi oleh perkembangan teknologi digital, algoritma media sosial, dan evolusi propaganda ekstrem. Oleh karena itu, strategi penguatan deradikalisasi perlu dirancang sebagai strategi yang bersifat adaptif, kolaboratif, berbasis teknologi, dan berorientasi pada pembangunan ketahanan masyarakat (societal resilience), bukan semata-mata sebagai respons terhadap ancaman yang telah terjadi.

Analisis pada kuadran Strength–Opportunity (SO) menunjukkan bahwa BNPT memiliki modal kelembagaan yang kuat berupa legitimasi hukum, dukungan pemerintah, pengalaman panjang dalam program deradikalisasi, serta jejaring kerja sama nasional dan internasional. Modal tersebut perlu dioptimalkan untuk memanfaatkan peluang yang muncul akibat tingginya penetrasi internet, meningkatnya literasi digital masyarakat, berkembangnya komunitas kreatif, serta kemajuan teknologi digital. Strategi SO diarahkan pada penguatan kolaborasi lintas sektor melalui pendekatan whole-of-government dan whole-of-society, sehingga penyebaran pesan damai tidak lagi menjadi tanggung jawab tunggal pemerintah, tetapi menjadi gerakan kolektif yang melibatkan akademisi, tokoh agama, organisasi masyarakat sipil, komunitas kreatif, media massa, perusahaan teknologi, dan platform media sosial. Pendekatan kolaboratif semacam ini memungkinkan terbentuknya ekosistem komunikasi yang lebih inklusif, kredibel, dan memiliki jangkauan yang lebih luas dalam membangun ketahanan masyarakat terhadap propaganda ekstrem.

Sementara itu, hasil analisis *Weakness–Opportunity* (WO) mengindikasikan bahwa sejumlah kelemahan internal masih membatasi efektivitas komunikasi digital BNPT. Pola komunikasi yang cenderung formal, rendahnya personalisasi pesan, keterbatasan sumber daya manusia di bidang komunikasi digital kreatif, serta pemanfaatan teknologi yang belum optimal perlu ditransformasikan agar sesuai dengan karakteristik komunikasi pada era media sosial. Generasi muda sebagai kelompok pengguna media sosial terbesar memiliki preferensi terhadap konten yang singkat, visual, interaktif, autentik, dan emosional. Oleh karena itu, strategi komunikasi perlu bergeser dari pendekatan institusional yang bersifat satu arah menuju komunikasi partisipatif yang berpusat pada audiens (audience-centered communication). Transformasi tersebut mencakup pengembangan konten berbasis storytelling, video pendek, animasi, infografik, podcast, dan format digital lain yang mampu meningkatkan keterlibatan (engagement) sekaligus memperkuat internalisasi nilai-nilai moderasi, toleransi, dan perdamaian.

Lebih jauh, analisis *Strength–Threat* (ST) menunjukkan bahwa kekuatan organisasi harus dimanfaatkan secara optimal untuk menghadapi ancaman yang semakin kompleks akibat perkembangan teknologi digital. Meningkatnya penggunaan platform komunikasi terenkripsi, fenomena echo chamber, filter bubble, propaganda berbasis Artificial Intelligence, serta munculnya pola lone wolf terrorism menunjukkan bahwa strategi deradikalisasi konvensional tidak lagi memadai. BNPT perlu mengintegrasikan kapasitas intelijen digital, analisis data, dan komunikasi strategis ke dalam satu sistem deteksi dini yang mampu mengidentifikasi pola penyebaran propaganda secara lebih cepat dan akurat. Penguatan patroli siber tidak hanya diarahkan pada pemantauan konten, tetapi juga pada analisis pola interaksi, identifikasi jaringan digital, pemetaan narasi ekstrem, serta deteksi perubahan perilaku komunikasi yang berpotensi mengarah pada proses radikalisasi.

Di sisi lain, strategi *Weakness–Threat* (WT) menekankan pentingnya penguatan kapasitas internal organisasi sebagai langkah defensif dalam menghadapi perubahan lingkungan strategis yang semakin dinamis. Keterbatasan kompetensi digital, rendahnya pemanfaatan kecerdasan buatan, dan sistem evaluasi yang masih berorientasi pada indikator keluaran (output) perlu diperbaiki melalui investasi pada pengembangan sumber daya manusia, modernisasi infrastruktur digital, serta reformulasi sistem evaluasi berbasis dampak (outcome dan impact). Dalam konteks komunikasi digital yang sangat cepat berubah, organisasi keamanan tidak lagi cukup mengandalkan prosedur birokrasi yang bersifat reaktif, tetapi harus membangun kapasitas organisasi yang adaptif, inovatif, dan berbasis pembelajaran berkelanjutan (learning organization).

Temuan penelitian juga menunjukkan bahwa efektivitas kontra-radikalisasi sangat dipengaruhi oleh kemampuan membangun komunikasi strategis yang humanis. Propaganda ekstrem umumnya memanfaatkan pendekatan emosional, identitas kelompok, dan narasi ketidakadilan untuk menarik simpati masyarakat. Oleh karena itu, kontra-narasi yang disampaikan pemerintah perlu dikembangkan melalui pendekatan yang lebih persuasif dengan memanfaatkan pengalaman mantan pelaku terorisme, penyintas korban terorisme, tokoh agama, komunitas lokal, serta figur publik yang memiliki tingkat kredibilitas tinggi di ruang digital. Pendekatan storytelling berbasis pengalaman nyata dipandang lebih efektif dibandingkan penyampaian pesan normatif yang bersifat formal karena mampu membangun kedekatan emosional dan meningkatkan kepercayaan audiens terhadap pesan yang disampaikan.

Selain aspek komunikasi, penelitian ini juga menegaskan bahwa perkembangan Artificial Intelligence (AI) telah mengubah karakter ancaman sekaligus membuka peluang baru dalam pelaksanaan deradikalisasi digital. Teknologi AI tidak hanya dimanfaatkan oleh kelompok ekstrem untuk menghasilkan

propaganda yang lebih realistis melalui deepfake, synthetic media, maupun automated bots, tetapi juga dapat digunakan oleh pemerintah untuk memperkuat kapasitas deteksi dini, analisis sentimen, identifikasi tren percakapan, pemetaan jejaring digital, serta optimalisasi distribusi kontra-narasi berdasarkan karakteristik audiens. Dengan demikian, pemanfaatan AI perlu diposisikan sebagai bagian integral dari strategi keamanan digital nasional, bukan sekadar sebagai instrumen pendukung teknologi.

Secara keseluruhan, hasil analisis menunjukkan bahwa keberhasilan deradikalisasi digital tidak lagi hanya ditentukan oleh kekuatan kelembagaan BNPT ataupun efektivitas regulasi pemerintah. Keberhasilan tersebut sangat bergantung pada kemampuan organisasi dalam beradaptasi terhadap dinamika algoritma media sosial, perubahan perilaku pengguna internet, perkembangan teknologi kecerdasan buatan, serta penguatan kolaborasi multipemangku kepentingan. Dengan kata lain, strategi deradikalisasi digital harus dipahami sebagai proses adaptasi organisasi yang berlangsung secara berkelanjutan terhadap perubahan lingkungan keamanan digital yang semakin kompleks dan tidak pasti.

Implikasi Kebijakan

Berdasarkan hasil analisis strategis tersebut, penelitian ini mengusulkan beberapa implikasi kebijakan yang dapat memperkuat kapasitas nasional dalam mencegah radikalisasi berbasis media sosial.

Pertama, diperlukan pembentukan Digital Counter-Radicalization Center sebagai pusat koordinasi nasional yang mengintegrasikan fungsi pemantauan media sosial, analisis data digital, pengembangan kontra-narasi, riset perilaku digital, serta koordinasi lintas kementerian dan lembaga. Keberadaan pusat ini diharapkan mampu meningkatkan respons yang lebih cepat terhadap dinamika propaganda ekstrem di ruang siber.

Kedua, BNPT perlu memperkuat kemitraan strategis dengan perusahaan platform media sosial dan penyedia layanan digital untuk mempercepat identifikasi serta penanganan konten ekstrem, sekaligus mengembangkan mekanisme berbagi informasi (information sharing) yang tetap memperhatikan prinsip perlindungan hak asasi manusia, kebebasan berekspresi, dan tata kelola data yang akuntabel.

Ketiga, penguatan literasi digital nasional perlu diposisikan sebagai strategi pencegahan jangka panjang. Literasi digital tidak hanya diarahkan pada kemampuan menggunakan teknologi, tetapi juga pada pengembangan berpikir kritis, ketahanan terhadap disinformasi, kemampuan mengenali propaganda ekstrem, serta peningkatan kesadaran mengenai etika dan keamanan bermedia digital. Pendekatan ini berkontribusi pada pembentukan societal resilience, yaitu kemampuan masyarakat untuk menolak dan mengurangi pengaruh ideologi ekstrem secara mandiri.

Keempat, penelitian merekomendasikan pengembangan AI-Based Monitoring System yang mampu melakukan analisis sentimen, deteksi dini terhadap narasi ekstrem, identifikasi pola penyebaran propaganda, serta pemetaan jaringan komunikasi digital secara real time. Sistem ini tidak dimaksudkan sebagai instrumen pengawasan massal, melainkan sebagai perangkat analitik berbasis bukti (evidence-based intelligence) untuk mendukung pengambilan keputusan yang lebih cepat, tepat, dan proporsional.

Kelima, diperlukan reformulasi sistem evaluasi program deradikalisasi dari pendekatan yang berorientasi pada keluaran administratif menuju evaluasi berbasis perubahan perilaku, perubahan sikap, tingkat keterlibatan masyarakat, serta penguatan resiliensi sosial. Pengembangan indikator yang mengukur outcome dan impact akan memberikan gambaran yang lebih akurat mengenai efektivitas program sekaligus menjadi dasar bagi penyempurnaan kebijakan deradikalisasi digital di masa mendatang.

Dengan demikian, implikasi kebijakan yang dihasilkan penelitian ini tidak hanya berorientasi pada

peningkatan kapasitas kelembagaan BNPT, tetapi juga menawarkan kerangka tata kelola keamanan digital yang lebih adaptif, kolaboratif, dan berbasis teknologi untuk memperkuat ketahanan masyarakat Indonesia dalam menghadapi ancaman radikalisasi pada era transformasi digital.

KESIMPULAN

BNPT memiliki kekuatan strategis yang signifikan dalam melaksanakan deradikalisasi melalui media sosial. Namun, perkembangan teknologi digital menuntut transformasi pendekatan komunikasi yang lebih kreatif, kolaboratif, dan berbasis teknologi. Analisis SWOT menunjukkan bahwa strategi penguatan deradikalisasi harus diarahkan pada optimalisasi literasi digital, pemanfaatan AI, pengembangan kontra narasi visual-humanis, serta penguatan kemitraan lintas sektor.

Berdasarkan temuan penelitian, penguatan strategi deradikalisasi digital memerlukan transformasi kelembagaan yang tidak hanya berorientasi pada peningkatan kapasitas operasional, tetapi juga pada kemampuan organisasi untuk beradaptasi terhadap perubahan ekosistem digital yang berlangsung sangat cepat. Oleh karena itu, penguatan kompetensi sumber daya manusia di bidang komunikasi digital, analisis data, kecerdasan buatan (Artificial Intelligence), dan manajemen media sosial perlu menjadi prioritas strategis agar BNPT memiliki kemampuan yang memadai dalam merancang, mengimplementasikan, dan mengevaluasi program deradikalisasi yang relevan dengan karakteristik ruang digital kontemporer.

Sejalan dengan perkembangan teknologi, pembentukan pusat pemantauan siber berbasis AI (*AI-Based Cyber Monitoring Center*) menjadi kebutuhan strategis untuk mendukung sistem deteksi dini terhadap penyebaran propaganda ekstrem, memetakan pola interaksi digital, serta mengidentifikasi kecenderungan radikalisasi secara lebih cepat dan akurat. Pemanfaatan teknologi tersebut perlu didukung oleh tata kelola data yang akuntabel, transparan, serta menghormati prinsip perlindungan hak asasi manusia dan privasi sehingga efektivitas kebijakan keamanan tetap berjalan seiring dengan prinsip-prinsip demokrasi.

Pada saat yang sama, keberhasilan deradikalisasi digital tidak dapat bergantung sepenuhnya pada kapasitas pemerintah. Pendekatan yang lebih kolaboratif melalui kemitraan dengan influencer, kreator konten, komunitas kreatif, organisasi masyarakat sipil, akademisi, dan perusahaan platform digital perlu terus diperkuat untuk membangun kontra-narasi yang lebih kredibel, inklusif, dan sesuai dengan karakteristik berbagai kelompok audiens. Keterlibatan aktor-aktor non-negara tersebut akan memperluas jangkauan komunikasi sekaligus meningkatkan legitimasi pesan-pesan moderasi, toleransi, dan perdamaian di ruang digital.

Selain itu, sistem evaluasi program deradikalisasi perlu direformulasi dari pendekatan yang berorientasi pada keluaran administratif (output) menuju evaluasi berbasis perubahan perilaku (behavioral outcomes) dan dampak jangka panjang (impact). Pengembangan indikator yang mampu mengukur perubahan sikap, peningkatan resiliensi terhadap propaganda ekstrem, kualitas keterlibatan masyarakat, serta efektivitas kontra-narasi akan menghasilkan dasar yang lebih kuat bagi penyempurnaan kebijakan secara berkelanjutan. Pendekatan evaluasi berbasis bukti (*evidence-based evaluation*) juga memungkinkan organisasi melakukan penyesuaian strategi secara lebih responsif terhadap perubahan lingkungan digital.

Sebagai upaya preventif jangka panjang, program literasi digital perlu diperluas secara sistematis dengan memberikan perhatian khusus kepada kelompok-kelompok yang memiliki tingkat kerentanan lebih tinggi terhadap paparan ideologi ekstrem, terutama generasi muda, pelajar, mahasiswa, dan komunitas yang

memiliki intensitas penggunaan media sosial yang tinggi. Literasi digital tidak hanya diarahkan pada peningkatan kemampuan teknis dalam menggunakan teknologi, tetapi juga pada penguatan kemampuan berpikir kritis, verifikasi informasi, pengenalan terhadap manipulasi algoritmik, serta pembangunan ketahanan sosial terhadap berbagai bentuk propaganda digital.

Dengan demikian, penguatan deradikalisasi melalui media sosial perlu dipahami sebagai strategi keamanan yang bersifat adaptif, kolaboratif, dan berbasis teknologi. Sinergi antara peningkatan kapasitas kelembagaan, pemanfaatan kecerdasan buatan, penguatan komunikasi strategis, kemitraan multipemangku kepentingan, sistem evaluasi berbasis dampak, serta pengembangan literasi digital akan membentuk ekosistem deradikalisasi yang lebih tangguh dalam menghadapi dinamika ancaman ekstremisme pada era transformasi digital. Pendekatan yang terintegrasi tersebut diharapkan tidak hanya meningkatkan efektivitas kebijakan BNPT dalam jangka pendek, tetapi juga memperkuat resiliensi masyarakat dan ketahanan nasional terhadap perkembangan radikalisme digital di masa depan.

DAFTAR PUSTAKA

Adikara, A. P. B., Zuhdi, M. L., & Purwanto, W. H. (2021). Analisis metode penggalangan intelijen dalam penerapan program deradikalisasi oleh BNPT. SOCIA: Jurnal Ilmu-Ilmu Sosial, 18(1), 61–71. https://doi.org/10.21831/socia.v18i1.41913

Akram, M., & Nasar, A. (2023). Systematic review of radicalization through social media. Ege Academic Review, 23(2), 215–228. https://doi.org/10.21121/eab.1166627

Aly, A., Macdonald, S., Jarvis, L., & Chen, T. M. (2017). Introduction to the special issue: Terrorist online propaganda and radicalization. Studies in Conflict & Terrorism, 40(1), 1–9. https://doi.org/10.1080/1057610X.2016.1157400

Amin, R., Wijanarko, D. S., Putri, A. H., Chandra, J. K., Novega, L., & Ambarrini, D. N. (2024). Membangun budaya hukum masyarakat dalam menggunakan media sosial. Abdi Bhara.

Ayu, A. M., Shabirah, S., & Putri, A. A. (2025). Penggunaan media sosial Instagram sebagai sarana promosi program deradikalisasi oleh BNPT di Indonesia. Jurnal Netnografi Komunikasi, 4(2). https://doi.org/10.59408/jnk.v4i2.120

Baaken, T., Korn, J., Ruf, M., & Walkenhorst, D. (2020). Dissecting de-radicalisation: Challenges for theory and practice in Germany. International Journal of Conflict and Violence, 14, 1–8. https://doi.org/10.4119/ijcv-3808

Bouttier, V., Leclercq, S., Jardri, R., & Deneve, S. (2023). A normative approach to radicalization in social networks. arXiv. https://arxiv.org/abs/2309.00513

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40.

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

Cannizzaro, S. (2016). Internet memes as internet signs: A semiotic view of digital culture. Sign Systems Studies, 44(4), 562–586. https://doi.org/10.12697/SSS.2016.44.4.05

Castells, M. (2010). The rise of the network society (2nd ed.). Wiley-Blackwell.

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. Studies in Conflict & Terrorism, 40(1), 77–98.

https://doi.org/10.1080/1057610X.2016.1157408
Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). Sage.
Doosje, B., Moghaddam, F. M., Kruglanski, A. W., de Wolf, A., Mann, L., & Feddes, A. R. (2016). Terrorism, radicalisation and de-radicalisation. Current Opinion in Psychology, 11, 79–84. https://doi.org/10.1016/j.copsyc.2016.06.008
Effendi, R., Sukmayadi, V., Triyanto, & Unde, A. A. (2022). Social media as a medium for preventing radicalization: A case study of an Indonesian youth community's counter-radicalization initiatives on Instagram. Plaridel, 19(2), 1–27.
Ferrara, E. (2017). Contagion dynamics of extremist propaganda in social networks. arXiv. https://arxiv.org/abs/1701.08170
Gill, A. S., Mustafa, G., & Rizwan, M. (2020). De-radicalisation in Pakistan: Implication of Swat Model. Journal of the Research Society of Pakistan, 57(1), 401–415.
Hoffman, B. (2006). Inside terrorism (2nd ed.). Columbia University Press.
Holt, T. J., Freilich, J. D., & Chermak, S. M. (2020). Internet-based radicalization as enculturation to violent deviant subcultures. Deviant Behavior, 41(7), 855–869. https://doi.org/10.1080/01639625.2019.1589426
McGuffie, K., & Newhouse, A. (2020). The radicalization risks of GPT-3 and advanced neural language models. arXiv. https://arxiv.org/abs/2009.06807
Minardi. (2021). Dynamics of deradicalization: Knowing the compromise of two state institutions. Governabilitas, 2(1), 1–15. https://doi.org/10.47431/governabilitas.v2i1.108
Moghaddam, F. M. (2005). The staircase to terrorism: A psychological exploration. American Psychologist, 60(2), 161–169.
Mutrofin, & Kharis, A. (2020). Deradikalisasi kaum remaja dalam membendung radikalisme media sosial. Jurnal Sosiologi Agama, 14(2), 241–260. https://doi.org/10.14421/jsa.2020.142-08
Neumann, P. R. (2013). The trouble with radicalization. International Affairs, 89(4), 873–893. https://doi.org/10.1111/1468-2346.12049
Nugrahajati, S. D., & Suparno, B. A. (2023). Program deradikalisasi dalam perspektif komunikasi politik. Jurnal Ilmu Komunikasi, 21(3), 245–259. https://doi.org/10.31315/jik.v21i3.11440
Puspita, R. (2019). Kontra-radikalisasi pada media sosial dalam perspektif komunikasi. Jurnal Komunikasi Universitas Garut.
Putra, I. E., & Sukabdi, Z. A. (2014). Religious terror activities in Indonesia. Journal of Pacific Rim Psychology, 8(2), 83–95.
Safri, H. M., Utomo, S. L., & Hakim, L. (2025). Terorisme di era digital: Kajian teoritis perkembangan upaya penanggulangan hukum sejak era Orde Baru hingga memasuki era digital. Jurnal Hukum Pelita.
Schmid, A. P. (2013). Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review. ICCT.
Sumpter, C. (2017). Countering violent extremism in Indonesia: Priorities, practice and the role of civil society. Journal for Deradicalization, 11, 112–147.
Sumpter, C. (2017). Terrorism and social media in Indonesia: Radicalisation and counter-narratives. Journal of Policing, Intelligence and Counter Terrorism, 12(1), 30–44.

https://doi.org/10.1080/18335330.2017.1413096

Syamsurrijal, M., Nurmandi, A., Jubba, H., Hidayati, M., & Hariyanto, B. (2024). De-radicalization through social media: Social media literacy in countering terrorism in Indonesia. Wawasan: Jurnal Ilmiah Agama dan Sosial Budaya, 9(1), 1–15. https://doi.org/10.15575/jw.v9i1.16788

Ula, M. (2019). Kajian literatur penerapan social media network dan information security intelligent untuk mengidentifikasi potensi radikalisasi online. Sisfo: Jurnal Ilmiah Sistem Informasi, 3(2), 121–132. https://doi.org/10.29103/sisfo.v3i2.6336

Ulyana, Y. A., Ladiqi, S., Salleh, M. A., & Riyansyah, A. (2023). Assessing the effectiveness of the National Counter Terrorism Agency (BNPT) in Indonesia. International Journal of Advances in Social Sciences and Humanities, 2(2), 38–48. https://doi.org/10.56225/ijassh.v2i2.121

Weimann, G. (2016). Terrorism in cyberspace: The next generation. Columbia University Press.

Wibisono, A. A., Kumendong, R., & Maulana, I. (2025). Indonesia's handling of terrorists' cyber activities: How repressive measures still fall short. Journal of Policing, Intelligence and Counter Terrorism. https://doi.org/10.1177/23477970241298764

Winter, C. (2019). Online extremism: Research trends in internet activism, radicalization, and counter-strategies. International Review of Sociology, 29(2), 1–17.

Wolfowicz, M., Hasisi, B., & Weisburd, D. (2022). What are the effects of different elements of media on radicalization outcomes? A systematic review. Campbell Systematic Reviews, 18(2). https://doi.org/10.1002/cl2.1244

BNPT. (2024). Annual report 2024. Badan Nasional Penanggulangan Terorisme.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). National digital literacy report 2024. Kementerian Komunikasi dan Informatika Republik Indonesia.