



Hedayah

Countering Extremism  
& Violent Extremism



# MEMAHAMI DAN MENCEGAH EKSTREMISME & EKSTREMISME KEKERASAN DARING DI ASIA TENGGARA

## LAPORAN NEGARA INDONESIA



# Memahami dan Mencegah Ekstremisme & Ekstremisme Kekerasan Daring di Asia Tenggara

## LAPORAN NEGARA INDONESIA

Farangiz Atamuradova, Galen Lamphere-Englund & Emma Allen



Hedayah  
Countering Extremism  
& Violent Extremism



# Daftar Isi

<b>Ringkasan Eksekutif</b> .....	<b>4</b>
<b>1. Pendahuluan</b> .....	<b>6</b>
<b>2. Metodologi</b> .....	<b>8</b>
Tujuan & Pertanyaan Penelitian .....	9
Pendekatan & Metodologi Penelitian .....	9
Analisis Data .....	11
<b>3. Temuan Utama</b> .....	<b>12</b>
3.1. Lanskap Informasi Daring .....	13
3.1.1. Lanskap Informasi Daring dan Eksploitasi Ekstremis .....	13
3.1.2. Narasi Ekstremis, Ekstremis Kekerasan, dan Teroris Daring yang Prevalen .....	14
3.2. Ancaman yang Muncul di Dunia Maya .....	18
3.2.1. Penggunaan Platform Dominan dan Pergeseran yang Berlawanan .....	18
3.2.2. Teknologi Baru yang Sudah Digunakan: Permainan & AI .....	26
3.2.3. Teknologi yang Kurang Digunakan: Web Gelap, VR/XR, Drone, Senjata Api 3D, dan Lainnya .....	31
3.3. Tanggapan: Masa Lalu dan Masa Depan .....	32
3.3.1. Tanggapan yang Ada .....	32
3.3.2. Tantangan, Kebutuhan, dan Pelajaran Utama .....	37
<b>4. Rekomendasi</b> .....	<b>42</b>
<b>Referensi</b> .....	<b>48</b>
<b>Lampiran A: Ringkasan Sesi Paparan Negara Indonesia</b> .....	<b>54</b>

Pandangan yang diungkapkan dalam Laporan ini adalah pendapat dan karya penulis, dan tidak mencerminkan pendapat atau pandangan Hedayah atau organisasi atau individu yang berpartisipasi.

© Hedayah, 2025. Semua hak cipta dilindungi undang-undang.

## TENTANG HEDAYAH

Hedayah didirikan sebagai tanggapan atas keinginan yang semakin besar dari komunitas internasional dan anggota *Global Counter-Terrorism Forum (GCTF)* - yang kini mewakili 31 negara dan Uni Eropa - untuk membentuk wadah *'think and do'* multilateral yang independen dan bertujuan untuk melawan ekstremisme dan ekstremisme kekerasan. Sejak didirikan, Hedayah telah berkembang menjadi organisasi internasional yang penuh semangat, penuh dorongan, dan menyatukan jaringan luas yang terdiri dari para ahli dan praktisi yang tak tertandingi untuk melawan dan mencegah ekstremisme dan ekstremisme kekerasan dengan kekerasan. Dua belas anggota GCTF adalah perwakilan dari Dewan Pengarah kami yang beragam, yang memberikan pengawasan strategis. Sebagai Pusat Keunggulan Internasional untuk Melawan Ekstremisme dan Ekstremisme Kekerasan, kami berkomitmen pada inovasi, netralitas, integritas, keragaman, dan keunggulan teknis dengan memberikan penelitian terobosan, metodologi inovatif, dan program. Pendekatan kami adalah untuk memberikan dampak nyata dan berkelanjutan kepada pemerintah, masyarakat sipil, dan orang-orang yang terkena dampak ekstremisme dan ekstremisme kekerasan melalui kepemilikan dan kolaborasi lokal.



Hedayah

Countering Extremism  
& Violent Extremism

## UCAPAN TERIMA KASIH

Hedayah menyampaikan penghargaan dan terima kasih yang sebesar-besarnya kepada para ahli, praktisi, dan mitra yang terlibat dalam penelitian ini, serta Badan Nasional Penanggulangan Terorisme (BNPT) atas kerja sama dan dukungannya dalam proyek ini.

Hedayah juga berterima kasih kepada Departemen Luar Negeri dan Perdagangan Australia (DFAT) yang telah mendanai penelitian ini sebagai bagian dari program Hedayah yang lebih luas mengenai *Pemahaman dan Pencegahan Ekstremisme dan Ekstremisme Kekerasan Daring di Asia Tenggara*.

Akhirnya, kami mengucapkan terima kasih kepada para peninjau dan kontributor lainnya untuk Laporan ini, termasuk Anna Sherburn (Hedayah), Orissa Sofyan, dan Charlotte Gerdes.



## Referensi yang Disarankan:

Farangiz Atamuradova, Galen Lamphere-Englund & Emma Allen. (2025) *Memahami dan Mencegah Ekstremisme & Ekstremisme Kekerasan Daring di Asia Tenggara - Laporan Negara Indonesia*. Hedayah, Pusat Keunggulan Internasional untuk Melawan Ekstremisme dan Ekstremisme Kekerasan, Uni Emirat Arab (UEA).

Dunia saat ini telah menyaksikan perkembangan pesat dalam teknologi dan peningkatan keterhubungan dan keterlibatan secara daring. Meskipun hal ini telah mendorong pertumbuhan ekonomi global dan memungkinkan koneksi, pembelajaran, dan inovasi baru, aksesibilitas, keterlibatan, dan jangkauan ini juga dieksploitasi oleh pihak-pihak yang berniat jahat. Sebagai salah satu komunitas daring terbesar dan teraktif di dunia, Indonesia mendapatkan keuntungan secara sosial dan ekonomi, dan menghadapi tantangan seperti meningkatnya paparan terhadap konten daring yang berbahaya.

Untuk mendukung kegiatan penanggulangan ekstremisme daring di masa depan di Indonesia, penelitian kualitatif ini berupaya mengidentifikasi praktik-praktik dan model-model penanggulangan yang sudah ada, serta tren dan tantangan yang ada saat ini dan yang akan muncul. Penelitian yang dilakukan mencakup tinjauan sekunder terhadap literatur terkini tentang lanskap media dan informasi daring, eksploitasi oleh organisasi teroris dan ekstremisme, dan upaya-upaya penanggulangan yang terdokumentasi, serta penelitian primer yang dilakukan dengan para praktisi garda terdepan dalam upaya penanggulangan ekstremisme daring dan ekstremisme dengan kekerasan serta pemangku kepentingan utama lainnya yang relevan.

Laporan ini menguraikan berbagai temuan utama di tiga bidang utama. Pertama, laporan ini mempertimbangkan **lanskap informasi daring** di Indonesia, membahas tren di ruang daring, narasi yang digunakan oleh kelompok ekstremis, ekstremis dengan kekerasan, dan teroris, serta dampak dari misinformasi dan disinformasi. Kedua, laporan ini membahas **ancaman-ancaman yang muncul di dunia maya** dan dimensi lokalnya di Indonesia, mulai dari penggunaan berbagai platform hingga teknologi baru yang sedang berkembang dan bidang-bidang isu khusus (yang masih relevan) yang perlu mendapat perhatian lebih. Terakhir, Laporan ini menguraikan **tanggapan yang ada dalam melawan ekstremisme dan ekstremisme kekerasan di dunia maya**, mulai dari upaya komunikasi strategis hingga pendidikan, penelitian dan koordinasi, serta mendiskusikan tantangan, kebutuhan, dan pembelajaran utama.

Laporan ini diakhiri dengan rekomendasi kontekstual yang dapat ditindaklanjuti untuk upaya-upaya masa depan dalam penanggulangan ekstremisme daring di Indonesia, untuk mendukung upaya-upaya yang sedang berlangsung di bidang ini dan membantu menyesuaikan dan menargetkan pendekatan baru. Rekomendasi **tersebut meliputi:**

- ◆ Terus mengembangkan kapasitas lokal untuk menciptakan narasi positif dan alternatif dalam menanggapi upaya multi-saluran dan platform khusus yang digunakan oleh teroris
- ◆ Memperkuat kapasitas teknis untuk penelitian dan pemantauan narasi
- ◆ Bekerja sama dengan sektor swasta dan perusahaan teknologi untuk memanfaatkan potensi AI dalam upaya melawan ekstremisme
- ◆ Membangun mekanisme koordinasi dan kolaborasi yang sudah ada untuk menciptakan dan/atau memperkuat jaringan berbagi informasi formal dan informal
- ◆ Berfokus pada pendekatan yang disesuaikan dan berkelanjutan untuk intervensi media dan literasi informasi
- ◆ Memanfaatkan keberhasilan dalam upaya agenda Perempuan, Perdamaian dan Keamanan (WPS) dan menerapkan lensa gender yang menggabungkan faktor-faktor identitas lainnya untuk memperkuat pemahaman tentang dinamika radikalisme gender

Rekomendasi ini tidak lengkap, tetapi berusaha untuk membangun upaya dan kekuatan positif yang ada dalam konteks Indonesia untuk terus meningkatkan kemampuan praktisi kontra-ekstremisme daring dalam merespons eksploitasi ruang daring oleh teroris dan ekstremis.







# **1. PENDAHULUAN**



## 1. Pendahuluan

Era digital saat ini telah menyaksikan perkembangan pesat dalam bidang teknologi, menghubungkan orang-orang secara lokal, regional, dan global. Meskipun hal ini memberikan banyak peluang positif untuk komunikasi dan akses ke informasi, aksesibilitasnya juga dieksploitasi oleh aktor jahat untuk mendukung operasi mereka di ruang daring. Kelompok-kelompok ekstremis, ekstremis dengan kekerasan, dan teroris telah memanfaatkan tren dan alat daring baru untuk perekrutan dan radikalisi, perencanaan dan komunikasi, penggalangan dana, dan penyebaran propaganda. Para aktor ini menyesuaikan taktik dan metode mereka untuk mengeksploitasi dinamika platform dan amplifikasi algoritmik sambil semakin mengandalkan ruang terenkripsi atau semi-tertutup untuk menghindari deteksi.

Dengan sekitar 212 juta pengguna internet pada awal tahun 2025 (Kemp, 2025), Indonesia termasuk salah satu negara yang memiliki komunitas daring paling aktif dan besar di dunia. Meskipun pertumbuhan digital ini menawarkan peluang sosial dan ekonomi yang signifikan, pertumbuhan ini juga menghadirkan tantangan - terutama, meningkatnya paparan terhadap konten daring yang berbahaya seperti propaganda ekstremis dan aktivitas daring lainnya. Kaum muda tetap rentan terhadap narasi dan pendekatan radikal yang beradaptasi dengan cepat terhadap teknologi dan platform baru. Karena para aktor ekstremis terus mengembangkan strategi digital mereka, memahami lingkungan informasi di Indonesia sangat penting untuk mengembangkan respons yang tepat sasaran dan berkelanjutan.

Laporan Negara ini menyajikan temuan-temuan dari penelitian lapangan tentang lanskap media dan informasi di Indonesia, dengan fokus pada strategi para aktor ekstremis daring, tantangan yang dihadapi oleh para praktisi di garis depan, dan pelajaran yang dapat dipetik dari respons yang dilakukan saat ini. Laporan ini juga menawarkan rekomendasi praktis dan sesuai konteks bagi para praktisi dan pembuat kebijakan yang bekerja untuk mengidentifikasi dan mengganggu aktivitas ekstremis daring. Alih-alih mengusulkan satu solusi untuk semua, laporan ini menekankan pendekatan yang diinformasikan secara lokal berdasarkan wawasan dari mereka yang terlibat dalam kontra-ekstremisme di berbagai sektor. Lebih lanjut, laporan ini menilai bagaimana jaringan ekstremis di Indonesia menggunakan ruang digital daring, dan mengembangkan strategi multi-platform untuk memaksimalkan visibilitas dan keamanan operasional - memberikan pemahaman mendalam tentang bagaimana platform publik seperti TikTok, Instagram, dan X (sebelumnya disebut Twitter) digunakan untuk menyebarkan narasi dan memengaruhi wacana arus utama, sementara aplikasi pengiriman pesan dengan fungsi enkripsi seperti Telegram dan WhatsApp berfungsi sebagai pusat perekrutan, koordinasi, dan perencanaan. Laporan ini juga meneliti tren yang muncul dalam penggunaan ruang digital oleh para ekstremis, seperti pendanaan kegiatan mereka dengan menggunakan mata uang digital.

Terakhir, laporan ini mengeksplorasi respons yang ada terhadap ancaman-ancaman ini melalui langkah-langkah legislatif, peraturan platform, kerja sama antarlembaga, dan program pencegahan - Mulai dari undang-undang kontra terorisme Indonesia yang mengkriminalisasi propaganda terorisme dan perekrutan secara daring, Rencana Aksi Nasional untuk Mencegah dan Menangani Ekstremisme Kekerasan (RAN P/CVE) yang memfasilitasi respons pemerintah, masyarakat sipil, dan sektor swasta, hingga upaya regional seperti peran kepemimpinan Indonesia dalam Rencana Aksi ASEAN untuk Mencegah dan Menangani Meningkatnya Radikalisi dan Ekstremisme Kekerasan (2018-2025). Masyarakat sipil memainkan peran penting dalam meningkatkan kesadaran, mempromosikan literasi digital, dan memperkuat narasi positif-khususnya ketika upaya-upaya tersebut melibatkan kaum muda, perempuan, dan komunitas minoritas. Laporan ini berupaya memberikan contoh praktis dari praktik-praktik menjanjikan yang sudah ada, sekaligus mengidentifikasi bidang-bidang yang membutuhkan dukungan dan inovasi lebih lanjut untuk membangun masyarakat digital yang lebih tangguh dan terinformasi, serta mencegah para ekstremis mengeksploitasi ruang daring.



## 2. METODOLOGI

## 2. Metodologi

Untuk mendukung kegiatan penanggulangan ekstremisme daring di masa depan di Indonesia, penelitian ini berupaya mengidentifikasi praktik-praktik baik yang sudah ada serta tren dan tantangan yang sedang dan akan mengemuka. Bagian ini merinci metodologi yang digunakan untuk penelitian kualitatif tentang kebutuhan, tantangan, dan pembelajaran yang diidentifikasi oleh para praktisi garda depan penanggulangan ekstremisme dan kekerasan daring serta pemangku kepentingan utama lainnya yang relevan.

### Tujuan & Pertanyaan Penelitian

Tujuan utama dari laporan negara ini adalah untuk menghasilkan penelitian berbasis bukti tentang lanskap informasi dan media dalam konteks yang diteliti, bagaimana kelompok-kelompok ekstremis bertindak dalam lanskap tersebut, dan apa saja kebutuhan yang diidentifikasi untuk menanggapi tantangan ekstremisme daring. Pertanyaan penelitian utama untuk proyek ini diuraikan di bawah ini. Selain itu, pertanyaan-pertanyaan yang lebih rinci dikembangkan dan diuraikan secara tematis untuk membantu para peneliti mencakup semua tema yang diperlukan untuk menilai situasi secara menyeluruh di negara tersebut.

- ◆ **Pelajaran, tantangan, tanggapan, dan kebutuhan** apa yang diidentifikasi oleh aktor garda depan yang bekerja untuk mencegah dan melawan ekstremisme dan ekstremisme daring?
- ◆ Bagaimana **lanskap media dan informasi yang ada saat ini** berkontribusi terhadap penyebaran konten berbahaya melalui platform daring?
- ◆ **Tren baru apa yang muncul** terkait ekosistem daring yang diidentifikasi oleh para pelaku garda depan, dan dianggap paling penting untuk diatasi?

### Pendekatan & Metodologi Penelitian

Hedayah melakukan dua kegiatan penelitian khusus di Indonesia untuk menilai lanskap media dan informasi, dengan fokus pada keterampilan literasi media dan informasi (MIL) serta keterlibatan ekstremis di platform digital di negara-negara yang dipilih. Kedua kegiatan tersebut bertujuan untuk menjelaskan kebutuhan dan tantangan yang diidentifikasi oleh para praktisi garda depan. Metodologi penelitian ini mencakup penelitian kualitatif primer termasuk wawancara semi-terstruktur dan diskusi kelompok terfokus dengan para pemangku kepentingan utama, termasuk kementerian dan aktor masyarakat sipil yang terlibat dengan kaum muda dan dengan upaya-upaya penanggulangan ekstremisme dan kekerasan atau MIL, dan penelitian sekunder yang menilai literatur yang ada tentang topik tersebut. Pendekatan inklusif diterapkan dalam keseluruhan penelitian ini, dengan tujuan untuk mendapatkan representasi yang beragam dari perspektif dan pengalaman berbagai kelompok, termasuk gender, usia, agama, dan kelompok minoritas, dalam batasan ukuran sampel yang direncanakan dan jadwal waktu yang tersedia. Secara ringkas, penelitian ini mencakup kegiatan-kegiatan berikut:

- ◆ **Tinjauan komprehensif terhadap literatur yang ada** yang mencakup topik ekstremisme daring di Malaysia dalam lima tahun terakhir untuk membantu mengidentifikasi data yang tersedia, kesenjangan yang ada dalam literatur, dan memvalidasi temuan-temuan dari temuan primer
- ◆ **Dua diskusi kelompok terarah (FGD)** dengan para pemangku kepentingan utama seperti perwakilan kementerian dan organisasi masyarakat sipil di Jakarta dan Bandung, Indonesia, untuk mendapatkan wawasan tentang persepsi dan sikap yang berkaitan dengan pertanyaan penelitian dan memvalidasi temuan dari tinjauan literatur
- ◆ **23 wawancara informan kunci (KII)** dengan para ahli terpilih untuk mendapatkan perspektif dan wawasan tambahan yang mendalam terkait dengan pertanyaan penelitian dan memvalidasi temuan-temuan dari tinjauan literatur serta diskusi kelompok terarah.





Alat-alat penelitian ini dikembangkan tidak hanya untuk menjawab pertanyaan-pertanyaan penelitian utama, tetapi juga untuk menerapkan perspektif gender dan hak asasi manusia, serta mempertimbangkan sudut pandang berbagai pemangku kepentingan dan bidang-bidang isu yang relevan dengan ekstremisme daring.

## Analisis Data

Analisis data untuk penelitian ini terdiri dari pengkodean kualitatif terhadap hasil penelitian primer. Dengan menggunakan pendekatan pengkodean tematik, data primer yang dikumpulkan melalui KII dan FGD dikodekan menggunakan perangkat lunak analisis kualitatif, Dedoose, oleh tim pengode dari tim peneliti (Hedayah dan konsultan). Pengkodean dilakukan dengan menggunakan pendekatan deduktif, dari buku pedoman yang dikembangkan oleh tim peneliti berdasarkan pertanyaan-pertanyaan penelitian dan juga meliputi identifikasi:

- ◆ Pertimbangan untuk kelompok pemangku kepentingan dan/atau sektor yang berbeda
- ◆ Bidang-bidang isu yang relevan dengan pertanyaan penelitian yang telah diuraikan sebelumnya dalam laporan ini (seperti kondisi pada saat ini, tren yang muncul, dll.)
- ◆ Isu-isu lintas sektor seperti masalah gender dan inklusi atau dampaknya

Selain itu, pendapat ahli eksternal juga diminta untuk memvalidasi temuan, termasuk tinjauan dan validasi oleh pemangku kepentingan pemerintah dan masyarakat sipil.





### **3. TEMUAN UTAMA**

### 3. Temuan Utama

Temuan-temuan dari penelitian ini disajikan sebagai berikut, Berdasarkan metodologi penelitian yang telah dijelaskan sebelumnya, dengan membagi penelitian ini ke dalam tiga komponen. Yang pertama mempertimbangkan lanskap media dan informasi yang ada di Indonesia dan bagaimana hal itu dimanfaatkan oleh para ekstremis. Bagian kedua fokus pada ancaman yang muncul di ruang daring, mengeksplorasi tren dan perkembangan yang paling menonjol. Bagian terakhir mengkaji tanggapan yang ada dari aktor pemerintah dan non-pemerintah, serta tantangan dan kebutuhan yang diidentifikasi untuk pekerjaan di masa depan di bidang ini.

#### 3.1. Lanskap Informasi Daring

Bagian pertama dari laporan ini membahas pertanyaan berikut:

**Bagaimana lanskap media dan informasi yang ada saat ini berkontribusi terhadap penyebaran konten berbahaya melalui platform daring?**

Bagian dari laporan ini menyelidiki lanskap daring saat ini di Indonesia berdasarkan wawasan para ahli lokal serta literatur yang ada untuk lebih memahami bagaimana organisasi-organisasi ekstremis mengeksploitasi ruang-ruang digital sebagai sarana komunikasi dan koordinasi mereka.

##### 3.1.1. Lanskap Informasi Daring dan Eksploitasi Ekstremis

Meskipun platform dan aplikasi baru dapat meningkatkan keterhubungan dan akses terhadap informasi, platform dan aplikasi ini juga menjadi alat bagi pelaku kejahatan untuk menjangkau dan melibatkan 212 juta pengguna internet di Indonesia. Pada praktiknya, para ekstremis di Indonesia terus meradikalisasi individu secara luring melalui metode yang lebih tradisional seperti dakwah dan kelompok belajar privat, serta menggunakan radikalisme daring atau digital untuk menyebarkan propaganda dan mengarahkan individu ke kelompok daring dan luring yang tertutup (Rahman et al., 2021). Kelompok teroris internasional seperti ISIS semakin mengadaptasi taktik mereka untuk menargetkan individu di Indonesia dengan menerjemahkan materi ke dalam bahasa lokal dalam praktik yang dikenal sebagai “e-jihad” atau jihad daring (ibid). Laporan terbaru dari UNICRI “menemukan contoh pengguna Telegram berbahasa Indonesia yang mengekspresikan pandangan neo-Nazi, termasuk dalam diskusi tentang Mein Kampf dan manifesto yang dibuat oleh penyerang Christchurch” (Bradley, 2025, hlm.77). Meskipun ada bukti yang lebih terbatas tentang aktivitas kanan jauh atau kanan radikal di ruang offline, penting untuk mempertimbangkan dan memantau tren ini dengan cermat. Para ahli Indonesia yang diwawancarai menggarisbawahi bahwa, berdasarkan studi yang dilakukan dengan para narapidana yang dipenjarakan atas tuduhan ekstremis, ekosistem daring adalah salah satu sumber utama radikalisme (IND25). Faktanya, penangkapan terkait terorisme terbaru di Indonesia dilakukan secara daring (Newton, 2025). Hal ini termasuk penangkapan seorang laki-laki berusia 19 tahun di Jawa Timur pada Juli 2024 yang dilaporkan teradikalisasi melalui media sosial dan berencana untuk megebom dua gereja di wilayahnya (Anuar, 2024). Hal ini semakin menyoroti tantangan penting ‘luring dalam perpotongan antara radikalisme daring dan perekrutan serta radikalisme luring di penjara.

Meskipun ada kemajuan yang terlihat tentang bagaimana platform-platform daring meningkatkan peraturan mereka tentang moderasi konten dan pendekatan lain yang relevan untuk mengatasi masalah ini, situasinya masih membutuhkan perhatian berkelanjutan karena pelaku kejahatan, seperti ekstremis, dengan cepat mengidentifikasi celah dalam pendekatan tersebut dan mengadaptasi konten mereka untuk menghindari deteksi dan penghapusan melalui penggunaan “konten di luar batas” (Saltman & Hunt, 2023). Selain itu, dengan meningkatnya jumlah konten yang diposting secara daring setiap hari, kebutuhan moderasi juga meningkat. Meskipun tidak hanya terjadi di Indonesia, para narasumber yang diwawancarai menunjukkan peningkatan intoleransi, ujaran kebencian, dan hoaks di ranah daring sebagai tantangan yang terus berlanjut (IND18). Hal-hal tersebut ada di dalam dan di luar narasi ekstremis dan taktik daring; namun, semua itu dapat dimanfaatkan oleh para ekstremis untuk meradikalisasi, merekrut, dan memobilisasi kelompok-kelompok tertentu atau memicu perpecahan di antara masyarakat (ibid).

Masalah ini semakin disorot dalam hal paparan khalayak daring terhadap konten berbahaya, dan kurangnya kemampuan untuk mengidentifikasi informasi yang salah atau berbahaya (IND19). Pada saat Internet menjadi sumber informasi utama bagi banyak orang, dan dengan meningkatnya prevalensi pelaku kekerasan yang lebih muda, terdapat peningkatan kekhawatiran bahwa anak muda paling rentan menjadi mangsa narasi ekstremis dan disinformasi saat mencari jawaban atas pertanyaan mereka (IND9). Dengan banyaknya interaksi mereka yang terjadi secara daring dan dengan moderator konten cenderung reaktif, kelompok ekstremis dapat memanfaatkan hal ini sebagai peluang untuk merekrut pengikut baru di kalangan anak muda (Ware, 2023). Tren lain yang patut diperhatikan dan perlu diteliti lebih lanjut adalah hubungan antara dinamika keluarga dan radikalisasi anak muda di platform daring, sebagaimana ditekankan oleh para ahli bahwa pencarian rasa identitas seringkali menjadi faktor pendorong utama radikalisasi anak muda (IND19). Terakhir, dibandingkan dengan penggunaan internet sebelumnya oleh kelompok ekstremis, perempuan tidak lagi dipandang sebagai aktor pasif yang memainkan peran pendukung dan secara aktif menjadi target di ruang daring oleh para ekstremis (IND17). Laporan RUSI di Indonesia menggarisbawahi bahwa “melalui media sosial, perempuan sekarang dapat memainkan peran yang lebih aktif sebagai propagandis, perekrut, penyandang dana, dan bahkan pelaku bom bunuh diri” (Nuraniyah, 2019, hlm. 2).

Ekosistem daring juga berperan dalam mengubah identitas dan interaksi sosial individu, memberikan kesempatan kepada individu untuk membentuk dan membangun identitas yang berbeda secara daring dan bertindak secara berbeda dari diri mereka secara offline - menjalani “kehidupan ganda”. Seperti di tempat lain di dunia, seorang narasumber menggarisbawahi bahwa indeks kesopanan luring orang Indonesia saat ini lebih tinggi daripada indeks kesopanan daring (IND22). Meskipun banyak yang menyambut dan menerima di ruang luring, bukti terbaru menunjukkan bahwa ada tren yang berbeda di ruang daring (Dawitri & Amara, 2023). Meskipun ruang daring dapat memperkuat ketidaksopanan, sebuah survei baru-baru ini menunjukkan bahwa intoleransi secara luring juga menjadi perhatian (LSI, 2023). Dalam laporan tersebut, sejumlah besar responden menyatakan ketidaknyamanan atau penolakan terhadap kelompok minoritas tertentu, menyoroti bahwa intoleransi tidak terbatas pada ranah digital saja (ibid). Perbedaan antara perilaku daring dan offline seseorang dapat mempersulit untuk mendeteksi perubahan, atau mengidentifikasi tanda-tanda awal radikalisasi secara offline. Hal ini dapat dimanfaatkan oleh para perekrut dan ekstremis daring untuk meradikalisasi individu dan mempersiapkan mereka hingga mereka siap untuk melakukan serangan luring (IND19; Ware, 2023).

### 3.1.2. Narasi Ekstremis, Ekstremis Kekerasan, dan Teroris Daring yang Prevalen

Narasi dan propaganda ekstremis memainkan peran penting sebagai taktik yang digunakan oleh para pelaku untuk menyebarkan pesan mereka secara daring dan menghasut kekerasan, kebencian, dan perpecahan di antara masyarakat. Dengan memanfaatkan platform digital, para ekstremis mengembangkan dan memperkuat pesan mereka untuk memberikan alternatif bagi para pengikutnya terhadap keluhan yang ada. Orang-orang yang diwawancarai melihat para ekstremis sangat canggih dalam memanipulasi informasi secara daring, mengembangkan dan menyebarkan narasi daring dengan cara yang paling strategis untuk menjangkau audiens target mereka (IND23). Meskipun narasi ekstremis terlihat menurun karena pekerjaan yang dilakukan oleh pemerintah dan perusahaan teknologi, keberadaan mereka di dunia maya tetap ada (IND24), oleh karena itu, penting untuk memahami dan mengeksplorasi narasi yang ada di Indonesia agar dapat mengatasinya secara efektif dan membangun komunitas yang lebih tangguh. Ekstremis sering menggunakan isu-isu lokal, regional, atau internasional, menambahkan elemen ideologi mereka, dan memanfaatkan informasi yang salah atau tidak benar untuk memperkuat pesan mereka kepada audiens target mereka.

#### Narasi Lokal

Meskipun narasi ekstremis global lebih menonjol dan hadir dalam wacana daring, narasi lokal sering kali memainkan peran yang lebih besar, yang secara unik disesuaikan dengan konteks negara. Para ekstremis memanfaatkan keluhan lokal, interpretasi agama, dan peristiwa nasional untuk mengembangkan pesan-pesan lokal mereka, menjadikannya kuat dan menarik bagi penduduk Indonesia. Para praktisi lokal melaporkan adanya peningkatan narasi ekstremis yang spesifik untuk wilayah tertentu, yang sering kali berfokus pada isu-isu lokal dan identifikasi (IND21, IND13, IND10, IND1).

Salah satu jenis narasi yang paling umum ditemukan di Indonesia adalah anti-statisme, yang berkisar pada iklim politik dan pemilu. Melalui narasi semacam itu, kelompok-kelompok ekstremis menggambarkan pemerintah yang terpilih sebagai “secara inheren tidak sah dan tidak adil,” dan menyebut mereka sebagai “Muslim yang murtad” (Program Harmoni 2023, hlm. 9). Dengan demikian, narasi politik sering kali memanfaatkan “mentalitas kita vs mereka,” yang berusaha menyebabkan perpecahan dalam masyarakat dan menyerukan pemerintahan yang

lebih ekstremis (IND21). Kelompok-kelompok ekstremis juga mengeksploitasi ketegangan politik di sekitar waktu pemilihan kepala daerah untuk memecah belah masyarakat dan memproduksi “narasi politik identitas dan politik sektarian untuk tidak memilih tokoh-tokoh politik atau kandidat pemerintah daerah yang berbeda agama, berbeda kelompok dengan mereka” (IND1). Mereka meningkatkan keluaran narasi tentang “topik-topik sensitif seperti agama dan ideologi, seperti retorika anti-Kristen atau pro-Islam” untuk meningkatkan mobilisasi politik selama pemilihan umum (IND10). Selain itu, organisasi ekstremis lokal memanfaatkan propaganda dan narasi ISIS yang sudah ada, membingkai ulang dan menerjemahkannya ke dalam bahasa dan konteks lokal, “menyasar isu-isu termasuk pemilu 2019 dan pemilu 2024 di Indonesia (Mok & Satria, 2024). Sebagai contoh, sebuah faksi Jemaah Ansharut Daulah (JAD) di provinsi Riau mendesak para pengikutnya melalui media sosial untuk melakukan kekacauan pada pemilu 2024 (ibid).

Para ekstremis di Indonesia juga terlihat menyesuaikan narasi dan pesan mereka untuk menghindari deteksi dan pelabelan sebagai organisasi ekstremis, ekstremis kekerasan, atau teroris, serta memperluas daya tarik dan mendapatkan lebih banyak popularitas di kalangan masyarakat. Hal ini sering kali dilakukan dengan membajak narasi lokal yang populer dan arus utama sambil mempertahankan ideologi ekstrem dan mempromosikan intoleransi terhadap anggota kelompok luar, seperti kelompok minoritas dan individu dengan latar belakang agama yang berbeda (IND24). Seperti yang digarisbawahi oleh salah satu narasumber, “narasi ekstremis telah melunak dalam nada tetapi masih mendorong pandangan agama yang ekstrem. Mereka menormalkan keseragaman ini, yang menentang keragaman” (IND16). Hal ini didukung oleh narasumber lain dan disoroti sebagai ancaman terhadap keberagaman, inklusi, dan toleransi yang ada di masyarakat Indonesia. Karena konten agama tersebar luas di ekosistem daring, kelompok ekstremis sering memanfaatkan dan mendistorsi konten tersebut untuk mempromosikan narasi mereka dan merekrut anggota baru di bawah bendera pendidikan agama (IND15).

Para ekstremis juga terlihat sering menyematkan pesan mereka secara halus dalam konten yang menarik. Para praktisi melaporkan adanya peningkatan pengagungan terhadap para terpidana terorisme dan pemimpin militan melalui TikTok. Menurut salah satu narasumber, “beberapa narasi berbasis AI di TikTok secara signifikan mengagungkan kelompok-kelompok mantan dan terpidana terorisme di Bali” (IND1). Misalnya, baik deepfake maupun konten asli yang merayakan tokoh-tokoh seperti Ali Imron (pelaku bom Bali yang telah meminta maaf secara terbuka atas tindakannya) tersebar luas. Beberapa narasi yang beredar di TikTok dilaporkan telah memengaruhi persepsi sebagian penonton terhadap tokoh seperti Ali Imron, dengan menonjolkan penyesalannya yang dianggap positif, sehingga menciptakan persepsi yang lebih positif terhadapnya (IND1, IND25). Pada saat yang sama, para pemimpin ekstremis yang telah meninggal dari Bom Bali (misalnya Dr. Azhari bin Husin dan Noordin M. Top) dijadikan mitos untuk generasi baru yang lebih muda melalui soundbite yang viral dan referensi budaya pop di platform tersebut (IND11). Seorang narasumber yang diwawancarai mencatat sebuah video TikTok yang menggunakan slogan dan ikonografi dari anime Jepang, “seni adalah ledakan” (“art is explosion”), untuk mengagungkan “pencapaian signifikan” teroris, yang mengindikasikan bagaimana para kreator ekstremis menyisipkan tema-tema militan ke dalam bahasa budaya yang akrab dengan anak muda (IND1). Pengemasan ulang pahlawan ekstremis dalam elemen-elemen konten populer yang sudah ada merupakan tren yang mengkhawatirkan yang dapat membuat ideologi ekstremis menjadi lebih mudah diterima oleh anak muda Indonesia.

Terakhir, kelompok-kelompok ekstremis mengalihkan narasi mereka ke topik-topik yang tidak terkait dengan agama, seperti kesejahteraan pribadi, lingkungan, dan topik-topik lain yang mungkin beresonansi dengan audiens perkotaan, terus “menanam benih ekstremisme, tetapi tanpa menggunakan narasi kekerasan” (IND24). Perlu dicatat bahwa meskipun cabang utama Jamaah Islamiyah (JI), kelompok ekstremis terbesar di Indonesia, mengumumkan rencananya untuk membubarkan diri pada musim panas 2024, ada kekhawatiran besar bahwa anggotanya akan terus beroperasi dengan nama yang berbeda tetapi menyebarkan ideologi yang sama (Hwang & Frank, 2024), sementara yang lain dapat bergabung ke kelompok serupa yang mendukung pandangan ideologis mereka (IND25). Perubahan-perubahan dalam struktur internal organisasi seperti itu membutuhkan investigasi lanjutan tentang bagaimana kelompok-kelompok tersebut mengubah taktik dan narasi daring mereka untuk memastikan kehadiran dan penyebaran ideologi mereka dalam konteks lokal.

Perlu dicatat bahwa meskipun narasi-narasi ini mungkin resonan dengan sebagian audiens online, mereka tidak mencerminkan sentimen publik yang lebih luas di Indonesia. Secara umum, masyarakat Indonesia menolak segala bentuk terorisme dan kekerasan, serta mendukung perdamaian, persatuan, dan pluralisme di dalam negeri. Tren-tren di atas penting untuk dipertimbangkan dalam mengembangkan respons yang tepat terhadap narasi-narasi yang ada.

## Disinformasi dan Misinformasi

Ketika kelompok ekstremis terus menyesuaikan taktik dan narasi mereka berdasarkan pergeseran lanskap politik dan sosial di Indonesia, mereka sering kali ditemukan memproduksi pesan yang sesuai dengan ideologi mereka melalui penyebaran narasi yang sengaja dibuat salah, atau disinformasi dan misinformasi. Platform media sosial dan aplikasi perpesanan telah memudahkan para ekstremis untuk membagikan dan menyebarkan narasi mereka dengan cepat dan global, “menggunakan taktik misinformasi dan disinformasi untuk memperkuat dampaknya” (Monaghan & Rodriguez, 2023). Mereka sering mengeksploitasi ruang gema daring untuk menyebarkan narasi mereka dan menargetkan mereka yang memiliki pandangan yang sama dengan kelompok tersebut (ibid).

Di Indonesia, disinformasi dan misinformasi terutama disebarluaskan pada masa-masa sensitif secara politik seperti pemilihan umum dan masa-masa perubahan politik (IND25, IND5). Hal ini diamati oleh para ahli selama pemilu 2019 dan pemilihan kepada daerah (pilkada) 2024 (Program Harmoni, 2023; Mok & Satria, 2024). Pada 2019, JI meluncurkan “perang informasi” melalui beberapa platform mereka untuk mengganggu jalannya pilkada (Mok & Satria, 2024). Para ahli percaya bahwa tujuan penggunaan disinformasi dan misinformasi di sekitar waktu pemilu bukanlah untuk mempengaruhi hasil, “tetapi untuk memprovokasi konflik di masyarakat dan merusak proses pemilu menjelang pemungutan suara nasional” (Ayuningtiyas, 2024). Ekstremis sering menggunakan konten buatan pengguna yang tidak diverifikasi untuk “membuat dan menyebarkan narasi palsu,” yang menjadi lebih mudah dengan meningkatnya ketersediaan platform AI generatif untuk penggunaan sehari-hari (IND15). Ekstremis terlihat memanfaatkan algoritme untuk “memberi makan pengguna” konten yang sudah selaras dengan keyakinan mereka, berusaha mengeksploitasi rendahnya tingkat literasi digital dan ketidakmampuan untuk mendeteksi dan secara kritis menilai konten palsu yang dibagikan secara daring, “membuat mereka lebih rentan untuk mempercayai dan membagikan” informasi tersebut lebih lanjut dengan rekan-rekan mereka (ibid).

Kelompok-kelompok ekstremis juga terlihat menggunakan cara-cara yang lebih terorganisir untuk membagikan narasi dengan mendirikan outlet media yang tidak sah, yang sering disebut sebagai “ladang media” oleh para jurnalis Indonesia (IND24). Mereka menggunakan platform-platform ini untuk menyebarkan narasi palsu dan disinformasi tentang isu-isu terkini, menebarkan rasisme dan kekerasan di dalam masyarakat (ibid). Sifat tertutup dari platform tertentu berarti informasi yang salah dan ujaran kebencian dapat beredar tanpa terkendali. Konsep “pembajakan ide” untuk mendorong interpretasi dan narasi mereka sendiri bukanlah hal yang baru, dan telah digunakan oleh kelompok-kelompok lain seperti ISIS dan para simpatisannya (Yilmaz & Atamuradova, 2022). Namun, metode penyematan dalam ideologi atau konsep yang sudah ada membuat identifikasi disinformasi dan misinformasi menjadi lebih sulit. Ketika kelompok ekstremis memadukan tema nasionalis atau politik dan agama dengan taktik disinformasi, menjadi lebih rumit untuk membedakan informasi yang sah dengan narasi ekstremis, yang dimaksudkan untuk mengganggu perdamaian dan proses demokrasi.

Dampak dari narasi-narasi ini bisa menjadi sangat nyata, dan mereka dapat secara langsung memberikan dukungan kepada organisasi-organisasi ekstremis dan ekstremis dengan kekerasan. Selama tujuh tahun terakhir, Indonesia dianggap sebagai salah satu negara paling dermawan di dunia (Charities Aid Foundation, 2025), dan para ekstremis di Indonesia telah memanfaatkan mekanisme tradisional berupa permohonan sumbangan terbuka ke dalam strategi narasi mereka, yang kini telah menjadi digital. Kelompok-kelompok yang terkait dengan ekstremis sering kali menyamar sebagai organisasi amal atau kemanusiaan untuk meminta sumbangan dengan membuat narasi yang bermuatan emosional yang ditargetkan untuk masyarakat umum. Di Indonesia, “penggalangan dana terbuka sering kali dibingkai sebagai seruan untuk mendukung keluarga para mujahidin yang syahid dan dipenjara” (Nuraniyah, 2019, hlm.12). Kampanye semacam itu dapat diiklankan di media sosial dan aplikasi perpesanan, menarik hati masyarakat untuk mengumpulkan uang yang seolah-olah untuk keluarga yang membutuhkan, yang pada kenyataannya justru mendanai kegiatan ekstremis. Seorang narasumber yang diwawancarai mengkonfirmasi bahwa ia melihat narasi media sosial yang meminta sumbangan untuk membangun pesantren yang berafiliasi dengan kelompok ekstremis seperti pesantren yang terkait dengan JI (IND25). Pada saat yang sama, pengawasan masih terbatas: “Di banyak organisasi Islam, tidak ada pelaporan yang diaudit... semua orang memberikan uang dan mereka tidak tahu ke mana perginya [uang itu]. Dan beberapa di antaranya digunakan untuk mendanai kegiatan terorisme di Indonesia” (IND23). Pada dasarnya, para aktor ekstremis dapat bersembunyi di antara berbagai badan amal dan urun dana yang sah di Indonesia, terutama jika organisasi-organisasi tersebut tidak memiliki transparansi. Hal ini mengaburkan batas bagi para donatur, yang banyak di antaranya mungkin benar-benar percaya bahwa mereka memberi untuk memberikan pendidikan agama atau bantuan kemanusiaan. Untuk melawan hal ini menjadi tantangan tersendiri, karena “mungkin kontra-narasi masih bisa digunakan [untuk mencegah orang dari ekstremisme], tapi bagaimana dengan narasi pendanaan seperti ini?” (IND25). Melawan himbuan penggalangan dana ekstremis membutuhkan taktik yang berbeda dengan melawan propaganda ideologis, karena yang pertama sering kali memanfaatkan nilai-nilai sosial yang positif seperti bentuk-bentuk amal yang sudah tertanam kuat dalam identitas dan nilai-nilai kebangsaan Indonesia.





01101110  
00100000  
0001  
01110 00100000  
00001  
0101 01101111

## Konflik Global sebagai Narasi

Peristiwa yang terjadi baru-baru ini di Timur Tengah telah dimanfaatkan oleh organisasi ekstremis dan kekerasan secara global untuk merekrut pengikut baru (Fahmy, 2024). Tren ini juga terlihat di Indonesia, di mana kelompok-kelompok ekstremis memanfaatkan konflik regional untuk membangun solidaritas, menjustifikasi kekerasan dan respons radikal, merekrut pengikut dan simpatisan baru, serta menggalang dana (IND23, IND21). Seperti yang disoroti oleh salah satu narasumber, konflik global yang berakar pada identitas seperti itu “memicu reaksi keras di kalangan pengguna Indonesia, yang melihatnya sebagai ketidakadilan terhadap komunitas Muslim, sehingga memperkuat pengagungan agama dan solidaritas “ (IND15) - seorang ahli lebih lanjut menyoroti bahwa konflik global ini “ditafsirkan melalui kacamata lokal untuk beresonansi dengan audiens domestik”, sebuah proses yang disebut sebagai “glocalization”. (IND19). Kelompok-kelompok ekstremis membagikan informasi secara daring tentang bagaimana pendukung lokal dapat terlibat (IND21, IND23). Sementara masyarakat Indonesia pada umumnya menunjukkan keprihatinan dan solidaritas yang tulus (Arshad, 2024), para aktor ekstremis mengeksploitasi sentimen ini untuk kepentingan dan agenda mereka sendiri, mengaburkan batas antara dukungan kemanusiaan dan mobilisasi ideologis. Selain solidaritas, termasuk ajakan untuk melakukan kekerasan, kelompok ekstremis lokal juga mengeksploitasi situasi global untuk merongrong dan “menjelek-jelekkan” pemerintah dan “memperkuat legitimasi ideologi ISIS” (Hasbi dkk., 2023). Dengan mempersenjatai narasi emosional di sekitar konflik dan peristiwa global yang ada, para aktor ekstremis dapat membangun jembatan yang kuat antara konflik yang jauh dan proses radikalisasi lokal.

## 3.2. Ancaman yang Mengemuka di Dunia Maya

Konektivitas internet di Indonesia berkembang dengan cepat. Dengan lebih dari 212 juta pengguna daring, rata-rata orang Indonesia melakukan scrolling, streaming, atau bermain selama lebih dari 7 jam sehari, empat setengah jam di antaranya dihabiskan di ponsel mereka (Kepios & We Are Social, 2025). Dalam lingkungan yang sangat terhubung tersebut, para aktor ekstremis merekayasa ulang pedoman mereka, memadukan oportunisme platform (misalnya, TikTok untuk viralitas dan Telegram untuk kerahasiaan) dengan tipu muslihat algoritmik, upaya penggalangan dana yang gesit, dan penggunaan teknologi seperti propaganda AI generatif dan game daring. Para pelaku garis depan yang diwawancarai untuk penelitian ini, mulai dari praktisi pencegahan masyarakat sipil hingga penyelidik pendanaan terorisme di Jakarta, menggambarkan lawan yang bersifat improvisasi dan bukan monolitik, “selalu selangkah lebih maju” dari tindakan pencegahan konvensional (IND25). Kesaksian mereka, yang ditriangulasi dengan penelitian akademis dan penelitian sektor abu-abu, berupaya menjawab pertanyaan inti dari bab ini:

**Tren baru apa yang muncul terkait ekosistem daring yang diidentifikasi oleh para pelaku garda depan dan dianggap paling penting untuk diatasi?**

Bagian ini menyatakan bahwa ekosistem ekstremis daring di Indonesia tidak lagi terpaku pada satu ideologi atau platform, tetapi merupakan lingkungan taktik dan prosedur yang berubah-ubah dan terus berkembang seiring dengan perkembangan ekonomi digital yang lebih luas (Nuraniyah, 2019; Program Harmoni, 2023). Bab berikut ini memetakan ekosistem tersebut ke dalam tiga bagian: penggunaan dan pergeseran platform yang dominan, teknologi baru yang telah digunakan, dan teknologi terdepan yang belum digunakan dalam skala besar.

### 3.2.1. Penggunaan Platform Dominan dan Pergeseran yang Berlawanan

#### Taktik dan Penggunaan Platform Saat Ini

Para praktisi garis depan yang diwawancarai secara konsisten menyoroti pergeseran ke arah media sosial yang berbasis visual dan algoritme - terutama TikTok dan Instagram - sebagai saluran utama penyebaran konten ekstremis di Indonesia. TikTok, khususnya, telah melonjak sebagai sebuah platform, menjangkau demografi yang luas di seluruh kelas sosial (Kepios & We Are Social, 2025). Salah satu narasumber menyatakan bahwa “TikTok di Indonesia saat ini merupakan platform yang paling banyak diakses oleh anak muda... isu-isu yang diangkat di TikTok akan menjadi sumber pertama yang kemudian menjadi trending topic” (IND1). Popularitasnya di kalangan anak muda membuatnya menjadi tempat yang tepat untuk menyebarkan narasi ekstremis dan materi rekrutmen. Para peneliti menggemakan pengamatan ini, melihat platform ini sebagai “alat baru untuk menyebarkan ekstremisme ideologis yang berpotensi menimbulkan kekerasan dan merekrut anggota baru” (Suseno Sarwono, 2024). Algoritme “For You Page” aplikasi ini dapat dengan cepat menyalurkan konten ke target audiens, terlepas dari upaya kepercayaan dan

keamanan platform untuk mengurangi eksploitasi oleh para ekstremis dan ekstremis kekerasan. Propaganda ISIS, misalnya, secara efektif memanfaatkan algoritme TikTok untuk mendapatkan visibilitas yang cepat “yang dirancang untuk menyelaraskan dengan perilaku pengguna, [memfasilitasi] penargetan konten ISIS secara efektif kepada audiens yang dituju,” dengan video-video yang “dengan cepat mendapatkan pengakuan luas” di antara pengguna yang mungkin tidak akan menemukannya, yang mencerminkan upaya kelompok tersebut untuk memanfaatkan platform secara global (MEMRI, 2025; Suseno Sarwono, 2024).

Tata kelola dan desain TikTok menciptakan tantangan yang unik. Para praktisi garis depan mengamati bahwa konten TikTok “kurang terkontrol dan menyebar dengan sangat cepat,” sering kali melebihi upaya moderasi (IND24). Mereka mengutip kasus-kasus pelecehan dan intoleransi daring di TikTok yang menggambarkan masalah yang lebih luas: kelompok minoritas dan bahkan tokoh masyarakat arus utama bisa menjadi target trolling dan hasutan ekstremis. Sebagai contoh, seorang jurnalis terkemuka, Najwa Shihab, menghadapi serangan misoginis dan rasis di TikTok yang diperkuat oleh kawanan akun yang terkoordinasi setelah mengkritik para pemimpin politik (IND24). Insiden-insiden semacam itu menggarisbawahi bagaimana viralitas TikTok dapat digunakan tidak hanya untuk mendorong ide-ide ekstremis militan, tetapi juga untuk menyebarkan kebencian dan intimidasi, yang berkontribusi pada ekosistem intoleransi yang menjadi tempat tumbuh subur bagi para ekstremis. Kekerasan misoginis seperti itu juga telah terbukti mengurangi ketahanan terhadap ekstremisme kekerasan dalam konteks Indonesia (Lamphere-Englund et al., 2022). Singkatnya, tren platform menunjukkan bahwa TikTok sangat penting untuk komunikasi ekstremis dan ekstremis kekerasan dalam konteks Indonesia. Basis pengguna yang sebagian besar berusia muda (sering kali dari kelompok berpenghasilan rendah), serta ketidakpuasan mereka terhadap pihak berwenang, merupakan hal yang ingin dieksploitasi oleh para aktor ekstremis (IND24). Seperti yang dikatakan oleh salah satu narasumber, “kelompok ekstremis mungkin melihat platform seperti TikTok sebagai peluang untuk memperluas pengaruh dan jangkauan mereka, menargetkan pengguna yang mungkin lebih rentan terhadap pesan mereka” (IND17).

Instagram juga memainkan peran, meskipun para ahli menilai Instagram digunakan dengan cara yang lebih terkurasi. Sebuah studi baru-baru ini dari proyek multi-tahun Harmoni P/CVE di Indonesia menemukan bahwa “Facebook dan, semakin banyak, Instagram ... digunakan untuk mendorong pesan ke audiens yang lebih luas, sering kali dalam format yang lebih halus yang dirancang untuk menghindari kebijakan moderasi platform” (Program Harmoni, 2023, hlm.6). Para aktor ekstremis memperlakukan Instagram sebagai saluran untuk penjangkauan yang luas dengan konten ringan yang dilemahkan untuk menghindari penghapusan konten dan mengandalkan platform lain untuk ajakan bertindak secara langsung. Orang-orang yang diwawancarai mencatat bahwa Instagram (bersama dengan properti Meta lainnya termasuk Facebook) telah menjadi responsif dalam menghapus konten ekstremis yang bersifat terang-terangan, sehingga para pelaku beradaptasi dengan mengurangi kekerasan eksplisit atau sektarianisme di platform-platform tersebut. Namun, jangkauan Instagram yang luas di kalangan anak muda Indonesia (84,6% pengguna internet berusia di atas 16 tahun menggunakan platform ini setiap bulan) dan para influencer membuatnya tidak dapat diabaikan (Kepios & We Are Social, 2025). Kelompok-kelompok ekstremis mengelola akun dan mengedarkan meme atau pesan-pesan berkode di sana untuk membentuk persepsi, tetapi hanya mengungkapkan tujuan ideologis mereka secara penuh di saluran yang kurang diatur.

Meskipun TikTok dan Instagram menjadi alat penyebaran yang paling banyak dibicarakan, para aktor garis depan menekankan bahwa aplikasi pesan terenkripsi dan forum-forum privat tetap menjadi infrastruktur penting bagi jaringan ekstremis, dan lebih lanjut, dapat menjadi ruang-ruang kunci untuk penguatan ideologi, jaringan, dan perekrutan. Telegram, khususnya, merupakan platform pilihan bagi para aktor ekstremis Indonesia karena fitur keamanannya (enkripsi opsional) dan fungsi membangun komunitas. Penelitian menemukan bahwa para ekstremis memilih platform daring berdasarkan empat kriteria utama: “keramahan pengguna, bebas biaya, keamanan dan privasi, dan inisiatif kepemimpinan” (Nuraniyah, 2019, hlm.137). Berdasarkan ukuran-ukuran ini, Telegram adalah pilihan yang jelas. Telegram diadopsi lebih awal oleh elemen-elemen pro-Daesh sekitar tahun 2014 karena enkripsi ujung ke ujungnya yang masih baru dan kemampuannya untuk meng-host obrolan grup yang besar. Tidak seperti WhatsApp pada saat peluncurannya, Telegram “dipandang lebih dapat dipercaya dan independen dari pemerintah” (Nuraniyah, 2017, hlm.170). Reputasi jangka panjang ini, dikombinasikan dengan layanan cuma-cuma dan mudah digunakan, membuat Telegram menjadi basis yang relatif dapat diandalkan oleh para pendukung ISIS di Indonesia hingga pertengahan 2010-an (Program Harmoni, 2023). Bahkan setelah Telegram berada di bawah tekanan - pemerintah Indonesia memblokir sementara versi web Telegram pada tahun 2017 untuk memaksakan moderasi yang lebih ketat dan tindakan INTERPOL yang terkoordinasi secara global selama pandemi menggeser kelompok-kelompok ISIS keluar dari platform tersebut - komunitas-komunitas ekstremis terbukti tahan banting dan memilih untuk tetap menggunakan platform tersebut. Salah satu narasumber menyebutkan bahwa sebuah tutorial pembuatan bom di Telegram - bagian dari jaringan Terrorgram yang lebih luas - tetap daring selama empat

tahun, menggambarkan bagaimana video atau file instruksional dapat beredar di luar jangkauan pihak berwenang. Saat ini, banyak yang menggunakan “langkah-langkah keamanan ekstra seperti nomor telepon virtual anonim ... VPN atau perangkat lain untuk menyembunyikan lokasi dan alamat IP” dalam hubungannya dengan Telegram daripada bermigrasi ke aplikasi yang kurang dikenal dan berisiko kehilangan pengikut (Nuraniyah, 2019, hlm. 142). Menurut salah satu narasumber, “saat ini, [para ekstremis] kebanyakan menggunakan Telegram. [Telegram memiliki keamanan yang lebih privat... membuat kami agak sulit untuk mengikuti atau memantau mereka” (IND1).

WhatsApp adalah platform penting lainnya, mengingat keberadaannya di hampir semua tempat di Indonesia: lebih dari 92% pengguna internet menggunakan platform ini (Kepios & We Are Social, 2025). Platform ini sering digunakan untuk memelihara sel yang lebih kecil atau jaringan yang intim. Praktisi lapangan menggambarkan jalur yang umum terjadi di mana konten publik di platform terbuka berfungsi sebagai umpan, dan kemudian simpatisan disalurkan ke dalam grup WhatsApp atau Telegram yang tertutup untuk indoktrinasi yang lebih dalam. Seperti yang dijelaskan oleh salah satu narasumber, setelah kontak daring awal, “seseorang akan ... mendekatkan mereka ke kelompok-kelompok kecil melalui grup WhatsApp, grup Telegram, di mana Anda bisa mengintensifkan hal-hal tersebut” (IND22). Dalam obrolan grup pribadi ini, narasi ekstremis dapat didorong secara lebih langsung - mulai dari pelatihan ideologis hingga perencanaan operasional - tanpa campur tangan pihak luar. Fitur-fitur baru di WhatsApp juga masuk dalam radar sebagai risiko yang muncul: misalnya, pengenalan WhatsApp Channels (umpan siaran satu-ke-banyak), yang dapat memungkinkan siaran propaganda klandestin ke audiens yang lebih besar (IND2).

Facebook tetap menjadi bagian dari ekosistem ekstremis, meskipun perannya telah berevolusi. Hasil wawancara menunjukkan bahwa Facebook lebih jarang digunakan untuk mengirim pesan langsung kepada ekstremis dan lebih banyak digunakan untuk berjejaring dan berkumpul. Algoritma rekomendasi teman di Facebook dapat secara tidak sengaja membantu para ekstremis menemukan satu sama lain. Khususnya, ketika sebuah grup Telegram pro-Daesh khusus perempuan di Indonesia dibubarkan (setelah administratornya ditangkap di Hong Kong), “para anggotanya mencari satu sama lain di Facebook dan segera mengadakan reuni daring. Fitur ‘saran teman’ dan ‘halaman terkait’ Facebook dapat berguna dalam hal ini” (Nuraniyah, 2019, hlm.10). Para aktor ekstremis memanfaatkan algoritme rekomendasi ini untuk menghubungkan kembali dan membangun kembali komunitas setelah pelarangan. Mereka berhati-hati di Facebook karena moderasi yang lebih ketat dan lebih efektif: “pengiriman pesan di Facebook lebih berhati-hati daripada di Telegram, mungkin untuk menghindari kebijakan moderasi konten yang lebih ketat” (Program Harmoni, 2023, hlm.8). Mereka dapat mempertahankan profil dan halaman Facebook untuk menandakan kehadiran mereka, merekrut simpatisan, atau membagikan konten ideologis yang telah disterilkan, kemudian mengarahkan pengikut ke ruang yang kurang diatur atau lebih terenkripsi untuk bergerak ke arah perekrutan dan radikalisasi eksplisit. Dari perspektif kontra-ekstremisme, properti Meta seperti Facebook dan Instagram relatif responsif dalam menghapus konten teroris (IND19). Namun, hal ini menciptakan pergeseran yang berlawanan, karena para ekstremis hanya bekerja untuk mengeksploitasi fitur-fitur jaringan platform tersebut sambil menghosting materi teroris atau ekstremis yang terang-terangan di tempat lain.

X (sebelumnya dikenal sebagai Twitter) adalah platform lain yang disebutkan oleh para aktor garis depan, terutama karena digunakan oleh faksi-faksi tertentu seperti kelompok-kelompok pendukung kekhalifahan. Para aktivis “kekhalifahan” di Indonesia menggunakan X untuk memperkuat pesan mereka melalui kampanye terkoordinasi yang diuraikan di bawah ini. Taktik semacam itu menggambarkan bagaimana para aktor ekstremis memanipulasi algoritma platform arus utama untuk meningkatkan visibilitas mereka. Perlu dicatat bahwa pendekatan moderasi X telah menjadi sangat longgar, dan narasumber dari Indonesia yang diwawancarai mengeluhkan bahwa permintaan penghapusan konten terorisme sering kali tidak dipenuhi di X, mirip dengan Telegram (IND2). Akibatnya, X terus menjadi rumah bagi sebagian wacana ekstremis dan kekerasan ekstremis, termasuk dukungan terhadap jihadis atau retorika ekstremis yang kejam, meskipun biasanya diutarakan dengan cara-cara yang menghindari hasutan langsung untuk melakukan kekerasan.

Terakhir, YouTube dan situs berbagi media lainnya memainkan peran pendukung. Meskipun tidak disorot sebanyak jejaring sosial oleh para narasumber, YouTube biasanya digunakan untuk membagikan konten ekstremis dalam bentuk yang lebih panjang (ceramah, dokumenter, tutorial) baik secara terbuka maupun melalui video yang tidak terdaftar. Beberapa pembicara ekstremis mengelola saluran YouTube dengan bahasa sandi untuk menghindari pelarangan, dan para militan diketahui mencari materi pelatihan di YouTube. Streaming langsung YouTube – dan juga Twitch, DLive, dan situs-situs lainnya - telah dieksploitasi secara global (misalnya, streaming “game” langsung yang digunakan untuk menyebarkan pandangan ekstremis atau menampilkan serangan teroris) dan para pelaku di Indonesia mungkin akan mengikutinya (Wiegold dkk., 2024). Namun, peningkatan moderasi di platform-platform besar umumnya telah mendorong konten yang paling mengerikan dari situs-situs arus utama dan masuk ke dalam forum-forum yang lebih sulit dijangkau.



## Peran Enkripsi End-to-End dan Grup Tertutup

Tren penting yang diidentifikasi oleh para pelaku garis depan adalah migrasi kegiatan ekstremis dari forum terbuka ke saluran terenkripsi end-to-end (E2EE) yang tertutup, yang mencerminkan tren global. Seiring meningkatnya tekanan terhadap platform publik, kelompok-kelompok ekstremis Indonesia “biasanya menggunakan platform terbuka, tetapi sekarang ... menggunakan platform tertutup dan platform komunikasi empat mata seperti Telegram dan WhatsApp” (IND1). Platform terenkripsi ini memberikan privasi dan kerahasiaan yang secara dramatis mempersulit upaya untuk memantau konten ekstremis. Dari sudut pandang praktisi, “dulu mereka [ekstremis] menggunakan platform terbuka seperti Facebook, Instagram, YouTube, X... tapi sekarang mereka menggunakan... Telegram dan WhatsApp... untuk menginternalisasi ideologi dan narasi ekstremis di kalangan mereka” (ibid). Platform pesan terenkripsi digunakan sebagai “ruang aman untuk penguatan ideologi, jaringan, dan perekrutan” (IND19). Pergeseran ke ruang terenkripsi ini berarti lebih banyak proses radikalisis yang terjadi di luar pandangan, dalam obrolan grup yang hanya diundang atau saluran rahasia.

Terdapat dua implikasi E2EE. Pertama, enkripsi yang berhasil diimplementasikan akan melindungi komunikasi dari penegakan hukum atau pengamatan pihak ketiga, sehingga memungkinkan para ekstremis dan pelaku kekerasan untuk membagikan konten, manual, atau rencana kekerasan tanpa perlu khawatir akan adanya penyadapan. Seperti yang telah disebutkan, enkripsi Telegram yang kuat, ketika diaktifkan, bersama dengan grup yang dikontrol pengguna telah menjadikannya tempat utama untuk segala sesuatu mulai dari penyebaran propaganda hingga perencanaan. Salah satu narasumber menceritakan bagaimana pelaku serangan di Malang yang berusia 19 tahun (2024) ketika remaja “bergabung dengan grup Telegram dan teradikalisis ... Dia menjadi pelaku tunggal ... [tanpa] hubungan formal dengan kelompok teroris mana pun” (IND6). Dalam kasus ini, pelaku dilaporkan terpengaruh sepenuhnya melalui interaksi daring di saluran terenkripsi. Orang yang diwawancarai menyoroti bahwa “kelompok teror tidak memiliki kerangka kerja. Yang harus mereka lakukan adalah menyediakan narasi dan melihat siapa yang percaya... mereka menyediakan banyak narasi kemarahan... Sementara itu, organisasi masyarakat sipil kita tidak memiliki kapasitas yang matang... untuk menangani masalah seperti itu” (ibid). Sketsa ini menyoroti bagaimana platform E2EE memberdayakan jaringan ekstremis amorf untuk merekrut dan mengindoktrinasi individu dari jarak jauh, sementara masyarakat sipil dan pemerintah kesulitan untuk mendeteksi interaksi ini, apalagi melawannya secara langsung.

Kedua, kelompok tertutup yang terenkripsi menumbuhkan komunitas dan dapat memfasilitasi pembangunan peran baru dalam gerakan ekstremis. Menariknya, penelitian dan wawancara menunjukkan adanya peningkatan keterlibatan perempuan dalam lingkaran ekstremis di Indonesia yang sebagian disebabkan oleh ruang daring yang bersifat privat ini. “Platform yang lebih privat seperti Telegram atau WhatsApp benar-benar memungkinkan perempuan untuk terlibat lebih jauh dalam ekstremisme kekerasan,” kata seorang ahli, seraya menambahkan bahwa partisipasi perempuan dalam kegiatan dan komplotan ekstremis “telah meningkat sejak tahun 2020” (IND1). Obrolan grup terenkripsi memberikan tingkat anonimitas dan kebebasan dari pengawasan sosial, yang memungkinkan perempuan - yang mungkin menghadapi hambatan sosial yang lebih besar dalam berpartisipasi dalam lingkaran yang lebih militan secara terbuka - untuk terlibat dalam jaringan ekstremis di belakang layar:

*“Platform yang lebih privat ini adalah platform yang nyaman bagi perempuan, karena mereka bebas mengekspresikan diri di ruang yang lebih privat dan tidak dapat diawasi oleh orang-orang yang menganggap mereka berbahaya atau memiliki kecenderungan intoleransi” (IND1).*

Dengan kata lain, forum E2EE dapat membantu memfasilitasi radikalisis perempuan dan memfasilitasi koordinasi mereka dengan cara yang kurang umum dilakukan ketika jaringan dilakukan di depan umum.

Bagi pihak berwenang, efek “walled garden” dari aplikasi terenkripsi adalah masalah utama. Kecuali jika ada penyusup atau anggota grup yang berbagi informasi, layanan keamanan memiliki visibilitas yang terbatas. Permintaan pemerintah untuk penghapusan konten atau data pengguna sering kali gagal pada platform yang berfokus pada privasi. Laporan informal dari orang yang diwawancarai mencatat bahwa kepatuhan Telegram terhadap permintaan penghapusan konten berada di bawah 50% - “hanya konten yang mengandung pornografi dan perjudian yang dihapus; untuk terorisme agak sulit di Telegram” (IND2). Ini berarti saluran propaganda dan koordinasi ekstremis dapat bertahan selama bertahun-tahun, seperti yang ditunjukkan oleh bertahannya setidaknya tiga fase Terrorgram dan jaringan terkait di platform tersebut (Barbarossa, 2024). Kesenjangan seperti itu menggarisbawahi bagaimana E2EE, meskipun melindungi kebebasan sipil untuk publik, dieksploitasi oleh para ekstremis untuk menghindari pengawasan dan penghapusan konten.

Selain itu, obrolan grup yang terenkripsi atau privat cenderung mengintensifkan eco-chamber atau ruang gema. Di dalam lingkaran ekstremis tertutup di WhatsApp dan Telegram, pesan-pesan tidak dapat ditentang dan dapat



menjadi lebih ekstrem dari waktu ke waktu: “Begitu Anda berada di sana [dalam grup obrolan pribadi], sangat sulit untuk benar-benar meneliti, ... memoderasi atau mengawasi situasi semacam itu ... [sehingga] sangat sulit untuk dipantau dan dikontrol” (IND22). Diskusi dalam kelompok-kelompok yang terisolasi ini dapat memperkuat keluhan dan meningkatkan komitmen terhadap suatu tujuan, terutama selama peristiwa-peristiwa yang memicu seperti pemilihan umum, bentrokan sektarian, atau peristiwa yang secara geografis jauh (lihat Bagian 1). Memang, saluran dan akun cadangan biasanya dibuat di seluruh Telegram dan platform serupa untuk memastikan bahwa meskipun satu saluran diekspos atau ditutup, jaringan tetap bertahan dalam bentuk lain. Ketahanan ini merupakan produk langsung dari lingkungan anonim yang terenkripsi untuk mendorong redundansi dan regenerasi yang tidak terlihat.

## Mekanisme Amplifikasi dan Celah Moderasi

Meskipun ada peningkatan moderasi konten dan pengawasan di platform utama, para aktor ekstremis dan ekstremis kekerasan terus mengadaptasi taktik amplifikasi kreatif untuk menyebarkan pesan mereka. Responden dan penelitian di garis depan menggambarkan dinamika kucing-kucingan di mana para ekstremis mengeksploitasi celah dalam kebijakan platform dan sistem algoritmik untuk memastikan konten mereka dilihat oleh khalayak sasaran.

Salah satu mekanisme utamanya adalah manipulasi algoritme dan sistem peringkat untuk memperkuat narasi ekstremis. Di Indonesia, seperti yang telah disebutkan, para ekstremis memanfaatkan fitur trending topic X sejak pertengahan tahun 2010. Seorang narasumber menceritakan bagaimana gerakan keagamaan konservatif “hijrah” dengan ahli “memanfaatkan trending topic untuk mendapatkan daya tarik yang masif, dikombinasikan dengan bahasa yang disesuaikan dengan kelompok sasaran yang berbeda,” jauh sebelum para pendukung keberagaman menyadari hal tersebut (IND24). Menurut salah satu sumber, para pelaku ini sengaja memposting secara massal pada jam-jam di luar jam sibuk dan menggunakan “tagar acak ... yang tidak bermakna” untuk mengelabui algoritme X saat membuat konten yang sedang tren (IND8). Dengan memasukkan tagar yang tidak relevan atau unik di setiap postingan, mereka memastikan setiap postingan tampak berbeda, menghindari filter konten duplikat X dan mempersulit deteksi otomatis. Strategi penandaan hashtag massal ini memungkinkan mereka membanjiri platform dengan konten dan bahkan mendorong poin-poin pembicaraan ekstremis menjadi topik yang sedang tren selama jam-jam dengan lalu lintas rendah. Praktik pembajakan atau manipulasi tagar ini adalah “praktik yang sangat umum di antara kelompok-kelompok semacam itu ... terutama jika menyangkut [X],” yang mengonfirmasi bahwa ekstremis Indonesia merupakan bagian dari pola global eksploitasi algoritmik (IND8). Hasilnya adalah slogan atau tema ekstremis sesekali muncul dalam wacana arus utama (misalnya, sebagai topik yang sedang tren atau konten yang direkomendasikan), memberikan narasi ekstremis lapisan popularitas atau legitimasi.

Strategi amplifikasi lainnya adalah dengan mengeksploitasi titik-titik lemah moderasi konten melalui bahasa sandi dan konten singkat. Untuk menghindari deteksi oleh filter otomatis atau moderator manusia, para ekstremis Indonesia sering kali menggunakan penyamaran. Sebuah penelitian mencatat bahwa banyak yang menggunakan “Internet ‘leet speak’ (mengganti huruf dengan angka dan simbol) untuk menyamarkan istilah-istilah kontroversial,” serta fitur-fitur platform baru seperti Stories yang menghilang untuk lolos dari sensor konten (Newton dkk. 2021, hlm. 9). Sebagai contoh, para pendukung ISIS di Indonesia diketahui menggunakan kode angka seperti “1515” untuk menandakan “ISIS” atau singkatan seperti “AD#15” untuk Anshar Daulah (kelompok pro-Daesh) (IPAC, 2018, hlm.12). Dengan menghindari kata-kata pemicu yang jelas, mereka mem-bypass deteksi berbasis kata kunci yang sederhana. Mereka juga memanfaatkan unggahan yang bersifat sementara dan terikat waktu (misalnya Instagram dan TikTok Stories, Status WhatsApp, dll.) yang menghilang setelah 24 jam, sehingga menyulitkan moderator atau pihak berwenang untuk menangkap konten tersebut tepat waktu. Secara teori, hal ini dapat ditinjau oleh platform setelah kejadian, tetapi dalam praktiknya, sering kali tidak, kecuali jika akun tersebut ditandai. Para praktisi mencatat melihat gambar atau video penghasut dalam umpan cerita dengan waktu terbatas, yang sering kali menghindari pemantau konten otomatis dan manusia.

Selain praktik sembunyi-sembunyi, para aktor ekstremis merencanakan ketahanan dalam menghadapi penghapusan konten. Saluran ekstremis Indonesia menunjukkan kemampuan beradaptasi yang tinggi: ketika satu akun atau saluran ditutup, saluran cadangan muncul seketika. Para analis mendokumentasikan lebih dari 100 saluran Telegram ISIS Indonesia yang telah dihapus, “meskipun sebagian besar dari mereka bangkit kembali hampir seketika” (Nuraniyah, 2019, hlm. 142). Administrator saluran menggunakan berbagai taktik bertahan hidup: mengubah nama saluran menjadi judul yang tidak berbahaya untuk menghindari perhatian, membuat beberapa saluran cermin sebagai cadangan, dan mengompres dan menyimpan konten penting dalam file PDF atau e-book yang dapat diunggah ulang atau dibagikan di tempat lain. Salah satu strategi yang umum dilakukan adalah mempertahankan saluran “feeder” khusus yang tujuan utamanya adalah mengiklankan tautan cadangan terbaru kepada para pengikut, memastikan komunitas dapat berkumpul kembali dengan waktu henti yang minimal, dengan cara yang sama seperti pengedar narkoba atau aktor pornografi di tempat lain secara daring.



Celah moderasi pada platform tertentu juga memainkan peran penting. Para praktisi garis depan menunjukkan bahwa beberapa platform secara khusus memilih untuk tidak bekerja sama atau kekurangan sumber daya untuk menghapus konten teroris dan ekstremis, sehingga para pelaku kejahatan memusatkan upaya mereka di sana. Sikap Telegram adalah contoh yang jelas, sementara X telah diidentifikasi sebagai “sangat sulit” dalam mengabulkan permintaan penghapusan di luar konten ilegal yang jelas-jelas ilegal seperti pornografi atau perjudian (IND2). Hal ini secara efektif menciptakan celah di mana propaganda ekstremis (yang mungkin tidak secara eksplisit melanggar hukum atau dapat dibingkai sebagai pidato politik/agama) tetap ada secara daring dengan alasan kebebasan berekspresi. Hasilnya adalah jaringan ekstremis Indonesia dapat secara terbuka mempertahankan kehadirannya di platform semacam itu untuk mendorong narasi ideologis atau disinformasi, karena mengetahui bahwa penegakan hukumnya terbatas dibandingkan dengan platform yang lebih ketat. Memang, salah satu narasumber yang diwawancarai membahas perbedaan antara platform-platform tersebut, mencatat tantangan-tantangan yang ada di samping contoh positif di mana salah satu platform secara proaktif memberi tahu pihak berwenang tentang ancaman yang kredibel (serangan yang direncanakan terhadap tokoh agama yang sedang berkunjung) yang berarti bahwa, dalam beberapa jam, polisi telah menangkap para tersangka, yang menunjukkan betapa efektifnya kerja sama antarplatform tersebut (IND19). Sayangnya, kerja sama semacam itu sering kali menjadi pengecualian; para ekstremis mengandalkan platform di mana moderasi sangat minim atau penegakan hukum tidak merata.

Pada intinya, para ekstremis memperlakukan konten dan saluran sebagai sesuatu yang bersifat sementara dan kemungkinan besar akan diketahui atau ditutup, dan dengan demikian mereka mengembangkan beberapa saluran yang berbeda untuk memastikan beberapa di antaranya selalu aktif meskipun ada yang dimoderasi. Sebuah laporan IPAC merangkum permainan kucing-kucingan ini: “Alih-alih merespons dengan tindakan pencegahan berteknologi tinggi, mereka hanya membuat ratusan saluran dan akun cadangan, memindahkan grup dan saluran mereka secara teratur, dan menyimpan terabyte materi propaganda di berbagai platform dan perangkat” (IPAC, 2018, hlm.1). Kegigihan berteknologi rendah ini sering kali dapat bergerak lebih cepat daripada proses penghapusan konten yang lebih birokratis.

Para ekstremis juga mengeksploitasi ruang gema dan sistem rekomendasi yang melekat pada media sosial untuk memperkuat jangkauan mereka. Seperti yang telah disebutkan, algoritme yang menyesuaikan konten dengan preferensi pengguna dapat secara tidak sengaja menciptakan lingkaran penguat bagi mereka yang terjun ke dalam konten ekstremis. Media sosial mengubah persepsi tentang realitas: jika seseorang berinteraksi dengan unggahan ekstremis atau intoleran, algoritme akan menampilkan lebih banyak hal yang sama, sehingga tampak bahwa pandangan seperti itu lebih luas daripada yang sebenarnya (IND15). “Efek ruang gema” ini berarti pengguna yang menunjukkan ketertarikan pada konten radikal akan diberi materi yang lebih ekstrem, mungkin dari berbagai platform yang saling memposting dan menautkan (misalnya, rekomendasi YouTube yang mengarah ke tautan Telegram). Di Indonesia, di mana literasi digital tidak merata, banyak anak muda yang mungkin rentan salah mengartikan kurasi algoritmik sebagai sentimen populer yang sebenarnya. Dengan demikian, bahkan tanpa sengaja memanipulasi algoritme, para ekstremis mendapatkan keuntungan dari sistem rekomendasi yang memprioritaskan keterlibatan daripada kualitas, yang sering kali mendorong konten yang sensasional atau mempolarisasi.

## Mekanisme Pembiayaan: Pergeseran yang Lambat ke Digital

Para ahli di Indonesia juga mengamati dengan seksama bagaimana kelompok-kelompok ekstremis, ekstremis dengan kekerasan, dan teroris mendanai operasi mereka dan bagaimana metode-metode ini berkembang. Saluran pendanaan tradisional masih tetap dominan, tetapi ada kecenderungan yang jelas untuk melakukan diversifikasi ke dalam mekanisme penggalangan dana digital dan daring.

Banyak kelompok ekstremis di Indonesia yang masih mengandalkan metode tradisional seperti donasi tunai, transfer bank, dan sistem transfer nilai informal (hawala). Penelitian menunjukkan bahwa aliran dana dari simpatisan luar negeri - diaspora Indonesia atau pendukung asing - masih sering bergerak melalui jalur tradisional ke Indonesia. Sebagai contoh, penelitian terbaru mencatat bahwa “aliran dana terorisme yang melibatkan diaspora dari luar negeri ke Indonesia lazim terjadi di Amerika Serikat, Malaysia, Filipina, Australia, dan Afganistan,” sementara dana dari Indonesia juga mengalir ke Malaysia, Filipina, dan sekitarnya (Ismail, 2023, hlm. 15). Transfer ini biasanya terjadi melalui sistem perbankan biasa atau layanan pengiriman uang dan jumlahnya cukup kecil untuk menghindari tanda bahaya. Sebuah studi tentang pendanaan teroris di Indonesia menyimpulkan bahwa meskipun platform daring tersedia untuk penggalangan dana, “transfer perbankan tradisional dan metode hawala masih diprioritaskan karena kecilnya jumlah dana yang dibutuhkan ... dan kebutuhan untuk menjaga ketersediaan uang tunai untuk tujuan operasional” (Wibisono et al., 2024, hlm. 141). Pada dasarnya, seringkali lebih mudah dan lebih aman bagi para ekstremis untuk memindahkan dana dalam bentuk tunai atau melalui deposito bank lokal, terutama untuk operasi dalam negeri yang tidak membutuhkan dana dalam jumlah besar. Hal ini juga menyoroti peran yang berpotensi signifikan dari komunitas diaspora dalam radikalisasi daring, perekrutan, dan upaya pendanaan, yang seharusnya menjadi faktor penting yang perlu dipertimbangkan dalam menentukan respons.

Kelompok-kelompok ekstremis seperti Jemaah Islamiyah (JI) secara historis membangun jaringan pendanaan berbasis komunitas yang luas. Seorang narasumber yang akrab dengan kelompok ini menyatakan bahwa “bagi JI, daring bukanlah saluran utama. Mereka memiliki sekolah, komunitas, [dan] yayasan. Jadi, saluran utamanya bukan daring... Tapi untuk [Daesh]... mereka melakukan [penggalangan dana] daring” (IND23). JI dilaporkan telah mengumpulkan aset yang signifikan melalui kontribusi anggota, badan amal, dan usaha bisnis. Menurut perkiraan kasar yang dibahas dalam sebuah wawancara, JI mungkin telah mengumpulkan dana sekitar satu triliun rupiah, atau sekitar 59,5 juta dolar AS pada tahun 2025, berkat kebiasaan di antara para anggotanya untuk menyumbang (zakat/infaq) secara teratur untuk tujuan tersebut (IND23). Kebiasaan penggalangan dana tradisional ini telah membuat JI tangguh secara finansial tanpa membutuhkan penggalangan dana modern. Seorang narasumber menyampaikan bahwa keberhasilan penggalangan dana JI dapat disamakan dengan “startup unicorn yang tidak dikenal” di Indonesia (IND23). Hal ini menggarisbawahi bahwa penggalangan dana tradisional masih sangat efektif untuk kelompok-kelompok yang memiliki jaringan luring yang mapan dan kelompok-kelompok ini mungkin merasa tidak perlu mengekspos diri mereka sendiri melalui penggalangan dana daring. Namun, ekosistem daring ini masih memungkinkan dan meningkatkan metode tradisional. Para ekstremis secara rutin menggunakan aplikasi terenkripsi untuk mengoordinasikan pergerakan uang dan pada akhirnya menggunakan bank konvensional atau pengiriman uang untuk menyelesaikan transaksi. Misalnya, Telegram telah digunakan untuk mengatur transfer uang tunai secara fisik:

*“Platform obrolan daring Telegram telah digunakan untuk mengoordinasikan transfer bank untuk pembelian senjata api dan perjalanan anggota kelompok MIT (Mujahidin Indonesia Timur) dalam rangka persiapan serangan pada Pilpres 2019... Transfer dana dilakukan secara tunai di kantor cabang bank dan konfirmasinya dikomunikasikan melalui Telegram” (Wibisono dkk., 2024, hlm. 146).*

Demikian pula, kerabat pejuang teroris asing Indonesia di luar negeri “telah menggunakan platform daring untuk berkomunikasi, mengoordinasikan kegiatan, dan mendanai keluarga mereka di luar negeri” (ibid). Dengan demikian, aplikasi-aplikasi tersebut menyediakan koordinasi dan kerahasiaan secara real-time untuk memfasilitasi taktik pendanaan kuno (pengiriman uang tunai secara langsung, transfer ke bank yang dilakukan dengan nama palsu, atau melalui kerabat perempuan, dan lain-lain). Bahkan ketika para aktor ekstremis memindahkan uang secara internasional, mereka sering kali lebih memilih untuk melapisi metode tradisional dengan dukungan teknologi kecil: seorang ekstremis yang ditangkap pada tahun 2017 menggunakan fungsi obrolan rahasia Telegram untuk mengatur transfer uang dari Suriah ke Indonesia melalui Western Union, menggunakan beberapa kurir untuk mengirimkan dana dengan cara yang berputar-putar untuk menghindari deteksi (Nuraniyah, 2019, hlm. 13). Hal ini menunjukkan penggabungan teknologi baru dengan taktik lama: pesan terenkripsi untuk berkoordinasi, dan juga metode pengiriman uang konvensional untuk memindahkan dana. Aktor-aktor ekstremis juga diketahui mengeksploitasi rekening bank perempuan - istri atau kerabat perempuan sering kali memiliki catatan kriminal yang bersih dan tidak terlalu menarik perhatian, sehingga membuat mereka menjadi saluran yang ideal untuk mendanai terorisme (ibid).

Para penyidik semakin khawatir dengan kemunculan mata uang kripto dan fintech lainnya dalam pendanaan teroris. Meskipun masih belum menjadi saluran utama pendanaan, ada beberapa contoh penting dan peningkatan minat terhadap metode ini. Memang, Indonesia telah mengalami insiden pendanaan terorisme yang signifikan yang melibatkan kejahatan siber dan Bitcoin. Serangan di Jakarta pada bulan Januari 2016 (yang terkait dengan ISIS) sebagian didanai melalui skema daring yang rumit. Pihak berwenang Indonesia mengungkapkan bahwa para militan “menggunakan Bitcoin sebagai sarana untuk mendanai operasi sel-sel teror yang berafiliasi dengan mereka di Indonesia,” dengan satu sel mengumpulkan “donasi dalam Bitcoin yang diatur melalui situs forum darknet, sebelum kemudian meretas situs perdagangan valas,” dan menghasilkan hampir US\$600.000 (Wibisono dkk, 2024, hlm.142). Kombinasi crowdfunding di web gelap dan pencurian siber langsung ini memberikan modal yang cukup besar untuk melakukan serangan tersebut. Kelompok lain, MIT, juga “berhasil menggelapkan dana dari perusahaan keuangan Malaysia dan mengumpulkan US\$33.000 dari operasi peretasan ini” (ibid, hlm.146). Kasus-kasus ini, meskipun sudah terjadi beberapa tahun yang lalu, menggambarkan potensi rejeki nomplok dari pembiayaan yang dimungkinkan oleh dunia maya.

Namun, ada juga pengecualian. Saat ini, menurut salah satu penyelidik keuangan, kasus-kasus pendanaan terorisme di Indonesia lebih cenderung menunjukkan rangkaian pencucian uang yang rumit di mana uang tersebut pada akhirnya, “pada lapisan kelima ... berakhir dengan menggunakan mata uang kripto” (IND5). Para narasumber yang diwawancarai menyoroti bahwa Bitcoin dan mata uang kripto lainnya menarik karena bersifat “universal dan ... sulit dilacak” (IND8). Seorang ahli menjelaskan bahwa para ekstremis beralih menggunakan mata uang kripto yang tidak hanya terkenal, tetapi juga mata uang kripto yang berfokus pada privasi seperti Monero dan koin serupa yang memiliki fitur privasi lebih baik yang dapat menyembunyikan pengirim, penerima, dan jumlah, sehingga lebih sulit dilacak daripada Bitcoin (ibid). Wawasan ini sejalan dengan pengamatan global: “Pasar mata uang kripto yang berkembang seperti Bitcoin [telah] memberikan tingkat anonimitas dan desentralisasi yang dapat dieksploitasi oleh para penjahat dan teroris”, dan memang ISIS, bersama dengan kelompok-kelompok sayap kanan, telah dilaporkan meminta sumbangan kripto pada platform seperti Telegram (Ismaizam, 2023, hlm. 162). Bukti saat ini menunjukkan bahwa contoh-contoh ini terbatas - satu studi mencatat bahwa “penggunaan mata uang kripto secara sistematis oleh kelompok teroris ... belum terlihat,” dan lebih banyak kasus-kasus satuan (Dion-Schwartz et al., 2020, dikutip dalam Ismaizam, 2023, hlm.162). Hal ini sejalan dengan tren global, karena analisis terbaru mengenai pendanaan teroris global memperkirakan bahwa kurang dari 7% dana terorisme disalurkan melalui mata uang kripto (Jofre et al., 2024). Namun, ketika digunakan, pelacakan mata uang kripto tetap menjadi tantangan, karena banyak bursa yang berbasis di luar negeri di luar yurisdiksi Indonesia (IND5). Perusahaan baru seperti Chainalysis dapat melacak transaksi kripto, tetapi menindaklanjuti dompet tertentu tetap menjadi tantangan yurisdiksi. Pelaku teror dapat mengeksploitasi hal ini dengan mengubah dana menjadi kripto setelah serangkaian lompatan melalui dompet elektronik atau rekening bank, sehingga mengaburkan jejak audit. Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) dapat melacak transaksi perbankan, tetapi ketika dana masuk ke dalam jaringan kripto yang terdesentralisasi, penelusuran menjadi jauh lebih sulit tanpa kerja sama internasional.

Terdapat bukti bahwa jaringan ekstremis dan teroris di Indonesia telah mulai bereksperimen dengan pembayaran digital lainnya. Para aparat mencatat adanya “gerakan yang berkembang di Indonesia untuk menggunakan barcode untuk pembayaran” dan “dorongan umum untuk beralih ke pembayaran non-tunai,” yang menimbulkan kekhawatiran bahwa “kelompok teroris/VE dapat menggunakan [pembayaran digital] untuk mendapatkan dana” (IND20). Aplikasi seperti OVO, Dana, GoPay (dari Gojek), yang menggunakan kode QR dan dompet digital, sangat populer di ekonomi daring Indonesia dan dapat disalahgunakan untuk mengumpulkan dana dengan kedok palsu. Sejauh ini, belum ada kasus terorisme besar yang menggunakan dompet elektronik yang telah dikonfirmasi, tetapi infrastrukturnya ada dan dilaporkan tidak cukup diatur untuk mencegah pendanaan terorisme.

Metode lain yang muncul juga termasuk mengeksploitasi pasar daring dan platform urun dana. Secara global, terdapat kekhawatiran bahwa teroris dapat menjual barang palsu secara daring (melalui situs e-commerce atau fitur pasar media sosial) untuk mencuci uang - pada dasarnya menerima “pembayaran” untuk produk yang tidak ada yang merupakan sumbangan, atau dengan menjual barang dagangan yang sebenarnya untuk kelompok tersebut. Narasumber yang diwawancarai menyatakan bahwa sejauh ini belum ada laporan mengenai penyalahgunaan e-commerce semacam itu di Indonesia (IND5). Meskipun demikian, kemungkinan tersebut membuat para praktisi tidak nyaman.

Ke depannya, game daring dan teknologi Web3 membuka peluang baru untuk pendanaan ilegal. Meskipun belum tercatat dalam kasus-kasus di Indonesia, para ahli memperingatkan bahwa teknologi ini dapat menawarkan lebih banyak lagi anonimitas dan metode kreatif untuk menggalang dana. Transaksi mikro dalam game daring atau dalam pengaturan metaverse dapat memungkinkan para ekstremis untuk mencuci dana atau menjalankan penggalangan dana di dalam game di bawah radar. Seperti yang dicatat oleh sebuah studi pandangan ke depan, “metaverse dapat menjadi lingkungan yang ideal untuk pencucian dan transfer dana yang dikendalikan oleh aktor teroris,” misalnya melalui penjualan seni NFT yang tidak jelas “di mana uang dalam jumlah besar dapat dipertukarkan tanpa regulasi



dan dengan risiko yang terbatas” (Hunter dkk., 2024, hlm. 106). Secara teori, seorang ekstremis dapat menjual karya seni digital unik (NFT) atau real estat virtual kepada donatur dengan jumlah yang besar, dan ini akan tampak sebagai transaksi yang sah dalam ruang yang sebagian besar tidak diatur. Metode seperti ini dapat “luput dari perhatian” dengan lebih mudah dibandingkan dengan transfer bank konvensional. Meskipun hal ini bersifat spekulatif, para pembuat kebijakan di Indonesia memperhatikan tren tersebut untuk merencanakan potensi ancaman.

### 3.2.2. Teknologi Baru yang Sudah Digunakan: Game & AI

Di luar platform media sosial dan aplikasi perpesanan, para praktisi garda depan di Indonesia meneliti bagaimana teknologi yang sedang berkembang dapat memungkinkan gelombang aktivitas ekstremis berikutnya. Ada tiga area yang menonjol dalam analisis mereka: ekosistem game daring, kecerdasan buatan, dan teknologi lain (seperti dark web dan metaverse) yang dapat dimanfaatkan oleh para ekstremis. Meskipun beberapa tren ini baru saja muncul, konsensus yang ada adalah bahwa tetap berada di depan tren ini sangat penting untuk pencegahan ekstremisme yang efektif.

#### Ekosistem Game Daring sebagai Ruang Rekrutmen dan Propaganda

Game daring diidentifikasi sebagai salah satu jalur pertumbuhan pengaruh ekstremis di Indonesia. Indonesia memiliki populasi gamer yang sangat besar dan muda, dengan sekitar 150 juta orang yang bermain game secara teratur. Munculnya e-sports dan game mobile berarti jutaan anak muda Indonesia menghabiskan waktu berjam-jam setiap hari di lingkungan virtual yang imersif dan sosial (Newzoo, 2025). Para ahli garis depan mengamati bahwa kelompok ekstremis menyadari hal ini dan telah mulai menyusup ke dalam platform dan komunitas game, yang telah diamati dan dicatat secara global (Lamphere-Englund & White, 2023; White et al., 2024). Salah satu orang yang diwawancarai memperingatkan bahwa “permainan elektronik sekarang menjadi ajang propaganda...[Dari Call of Duty, Roblox, Fortnite] ternyata ada yang menggunakannya [untuk tujuan memfitnah]” (IND25). Kekhawatirannya ada dua: para ekstremis dapat menggunakan game untuk menyisipkan konten atau narasi propaganda, dan mereka dapat menggunakan komunitas game untuk meradikalisasi dan merekrut secara langsung di dalamnya. Seperti yang diilustrasikan oleh Extremism and Gaming Research Network (2021), hal ini selaras dengan enam tipologi utama bahaya yang ditimbulkan oleh para aktor ekstremis di permukaan game: membuat video game baru dan modifikasi, mengeksploitasi lingkungan sosial game, merekrut dan berkomunikasi di dalam game, membuat konten teroris menjadi game, menggunakan game untuk propaganda, dan mendanai atau mencuci uang melalui game (Lamphere-Englund, 2024). Sebagai contoh, dalam sebuah penelitian di tujuh negara tentang ekstremisme di platform game, gamer yang disurvei di Indonesia adalah yang paling sering melaporkan melihat gambar, video, atau simbol yang mempromosikan ekstremisme di permukaan game (44%), sementara 26% melaporkan melihat upaya perekrutan, 18% terpapar dengan permintaan donasi kepada kelompok ekstremis, dan 36% melihat orang yang mendukung kekerasan terhadap kelompok sosial tertentu di platform game (White et al., 2024).

Beberapa karakteristik membuat platform game menarik bagi para aktor ekstremis. Pertama, banyak game daring (dan platform yang berpusat pada game seperti Discord) sering kali memiliki moderasi konten yang terbatas, terutama jika dibandingkan dengan media sosial arus utama. Tidak seperti Facebook, jaringan game secara historis tidak pernah menerima pengawasan terhadap konten ekstremis, meskipun hal ini akan berubah pada tahun 2025, yang mengarah pada sikap yang longgar dalam memantau percakapan yang mengandung kebencian atau terorisme. Penelitian menegaskan bahwa “banyak platform game dan platform yang berdekatan dengan game tidak melakukan banyak atau bahkan tidak ada upaya untuk memoderasi konten ekstremis”, karena mereka tidak ditekan untuk melakukannya (Lamphere-Englund & White, 2023, hlm. 20). Fungsi obrolan dalam game atau komunikasi suara dapat dipenuhi dengan bahasa beracun, yang dapat mencakup sentimen misoginis atau rasis, namun sering kali hanya kecurangan terang-terangan yang memicu pelanggaran. Para pelaku ekstremis memanfaatkan celah moderasi ini. Misalnya, obrolan suara di konsol atau dalam game pada dasarnya bersifat sementara dan tidak terpantau; mereka kurang mudah ditangkap oleh tindakan deteksi daripada postingan teks, dan begitu percakapan suara berakhir, biasanya tidak ada catatan bagi pihak berwenang untuk mengambil tindakan (Modulate, 2024). Para ekstremis Indonesia juga dapat menggunakan obrolan suara game atau lobi game pribadi untuk komunikasi rahasia.

Kedua, game memberikan kedok hiburan yang dapat menutupi perekrutan dan radikalisasi ekstremis. Orang tua atau pihak berwenang mungkin melihat seorang remaja bermain game yang populer dan tidak curiga bahwa ada sesuatu yang tidak beres, dibandingkan dengan melihat keterlibatan dalam forum yang diketahui. Dinamika ini mengkhawatirkan para aktivis di Indonesia: “ketika Gen Z bermain game... kita tidak memiliki kontrol. Karena kami pikir mereka hanya melakukan hiburan,” tetapi pada kenyataannya, ada kemungkinan mereka menjadi sasaran perekrut di dalam game (IND25). Perekrut, atau hanya gamer yang berpikiran ekstremis yang hadir dalam komunitas



yang besar, dapat secara bertahap membangun kepercayaan dengan pemain muda melalui obrolan, kemudian mengundang mereka ke saluran tertutup (grup Telegram, atau server Discord). Secara khusus, “fungsi obrolan dalam game memungkinkan akses yang cepat dan mudah ke berbagai pengguna, termasuk demografi yang lebih muda, yang dapat membantu perekrutan, propaganda, dan potensi komunikasi antar-kelompok” (Lamphere-Englund & White, 2023, hlm. 19). Penelitian yang berfokus pada Asia Tenggara juga mencatat bahwa “fitur komunikasi dalam gim ... tidak hanya berfungsi sebagai platform terselubung untuk menyebarkan ideologi ekstremis, tetapi juga sebagai tempat untuk menjangkau anak muda di Asia Tenggara untuk perekrutan” (Sulaiman & De Lang, 2024, hlm.26). Hal ini sangat relevan untuk populasi anak muda di Indonesia. Ada beberapa kasus regional yang bersifat anekdot (misalnya, dua pemuda Singapura yang teradikalisasi melalui Roblox), yang menyoroti bahwa ancaman ini tidak hanya bersifat teoritis.

Contoh spesifik dari konten ekstremis dalam game telah diamati oleh para pengamat di Indonesia. Seorang narasumber membagikan contoh mencolok dari gamifikasi propaganda: sebuah skenario yang dimodifikasi dalam game tembak-menembak populer Call of Duty atau judul game tembak-menembak orang pertama yang serupa disebarkan dengan sebuah perubahan - para pemain diberi identitas yang selaras dengan konflik di dunia nyata, dalam hal ini merujuk pada konflik di Timur Tengah. Mod atau permainan khusus ini menekankan narasi Muslim vs. musuh, yang secara efektif mengubah permainan rekreasi menjadi alat untuk memperkuat pandangan dunia ekstremis (IND25). Kemungkinan hal ini merujuk pada Knights of al-Aqsa, sebuah game shooter FPS dengan nada antisemit, yang diulas oleh live streamer game Indonesia (Lamphere-Englund & Thompson, 2024). Rekaman ini ditemukan di YouTube, dan telah dipromosikan melalui saluran Telegram, yang menunjukkan hubungan yang jelas antara jaringan ekstremis terenkripsi dan konten game. Dengan “memasukkan atribut agama tertentu ke dalam game ... mereka menekankan bahwa kita adalah teman dan mereka adalah musuh ... [gagasan] bahwa musuh-musuh itu harus dibunuh”, para propagandis menyampaikan pesan ekstremis interaktif kepada para pemain (IND25). Propaganda imersif semacam ini bisa menjadi sangat kuat - ini melibatkan pengguna secara emosional dan aktif, bukan hanya menonton video secara pasif. Hal ini juga menggambarkan bagaimana para ekstremis menggunakan kembali game populer yang sudah ada (alih-alih membuat game sendiri dari awal) untuk mengindoktrinasi para pemain secara halus.

Meski begitu, sejauh mana penetrasi ekstremis ke dalam komunitas game di Indonesia (lebih dari sekadar paparan) masih menjadi pertanyaan terbuka. Beberapa praktisi tetap berhati-hati untuk tidak membesar-besarkan fenomena ini. Seorang gamer yang diwawancarai mengatakan, “sebagai seorang gamer yang rajin bermain game... saya belum pernah melihat narasi ekstremis dalam game yang saya mainkan, terutama ekstremisme kekerasan” (IND13). Kadang-kadang ditemukan hinaan rasis dan nasionalis, sering kali muncul dari konflik antara pemain yang berbeda kebangsaan, namun perekrutan atau propaganda secara terang-terangan tidak ditemukan (ibid). Hal ini menjadi pengingat bahwa eksploitasi ekstremis dalam game tidak bersifat universal, dengan hanya 44% yang terpapar konten semacam itu di Indonesia pada jajak pendapat tahun 2024 (White et al., 2024). Penelitian terbaru mengenai identitas gamer di Indonesia menemukan bahwa meskipun ada keengganan untuk bermain dengan gamer dari latar belakang budaya atau kebangsaan yang berbeda (hanya 36% laki-laki dan 22% perempuan yang merasa nyaman), sebagian besar gamer Indonesia menunjukkan sifat-sifat yang sangat tangguh terhadap ekstremisme (Lamphere-Englund dkk, 2025).

Pendanaan melalui game adalah sudut pandang lain dari tren ini. Ekstremis berpotensi menggunakan platform game dan fitur monetisasi untuk mengumpulkan dana atau mencuci uang dan, seperti yang diilustrasikan sebelumnya, sekitar 18% gamer di Indonesia pernah melihat permintaan semacam itu di permukaan game (White et al., 2024). Literatur menyoroti beberapa metode: perdagangan mata uang dalam game atau barang langka dengan uang sungguhan (yang dapat dipindahkan dengan cara yang tidak jelas), menggunakan ekonomi hadiah game (seperti donasi selama streaming langsung) untuk menyalurkan uang, atau bahkan menjual modifikasi game yang hasilnya disalurkan ke pundi-pundi ekstremis. (Saiz, 2025) . Misalnya, “ada bukti adanya celah untuk menjual game, item dalam game, dan produk game lainnya dengan imbalan mata uang kripto atau mata uang fiat... banyak game menggunakan pertukaran mata uang virtual yang sering kali tidak sesuai dengan standar anti-pencucian uang” (Lamphere-Englund & White, 2023, hlm. 20). Contoh konkretnya adalah game populer Fortnite: game ini memiliki fitur loot box dan kartu hadiah yang telah “terlibat dalam skema pencucian uang” oleh kelompok kriminal terorganisir - kelompok ekstremis dapat membeli kartu hadiah dengan dana ilegal dan menjualnya kembali, atau menggunakan loot box untuk mengaburkan transaksi (ibid). Selain itu, platform streaming seperti Twitch telah disalahgunakan: ekstremis sayap kanan telah menghasilkan uang dengan melakukan streaming video game sambil menyebarkan pesan-pesan politik mereka, yang secara efektif mendapatkan donasi dari para pemirsa untuk propaganda (Schlegel, 2021). Kelompok ekstremis Indonesia dapat meniru teknik ini, terutama karena influencer dan streamer game Indonesia menarik banyak penonton dari kalangan anak muda.

Singkatnya, game daring mewakili ekosistem yang sedang berkembang yang sedang dijajaki oleh para aktor ekstremis. Para ahli di Indonesia melihat potensi platform game untuk menjadi seperti media sosial pada tahun 2020-an - sebuah vektor baru untuk radikalisasi dan koordinasi yang dapat terbang di bawah radar. Tantangan ini diperkuat oleh sifat interaktif dan transnasional dari game. Tren ini masih terus berkembang, dan meskipun belum sampai pada tingkat krisis, ini merupakan “peluang dan tantangan bagi generasi muda di Indonesia” (IND25) yang harus diantisipasi oleh para pembuat kebijakan dan masyarakat sipil. Langkah-langkah proaktif - seperti kesadaran untuk orang tua dan gamer, dan keterlibatan dengan industri game untuk membantu meningkatkan moderasi - harus dipertimbangkan untuk mencegah infiltrasi ekstremis mendapatkan pijakan di komunitas game Indonesia.

## Penggunaan Kecerdasan Buatan dalam Propaganda dan Perencanaan Operasional

Kecerdasan Buatan (Artificial Intelligence/AI) dengan cepat mengubah ekosistem daring, dan para aktor garis depan di Indonesia mencatat tanda-tanda saat ini dan kemungkinan eksploitasi AI di masa depan oleh kelompok-kelompok ekstremis. Dari pembuatan propaganda AI generatif hingga penargetan algoritmik dan chatbot, para ekstremis mendapatkan keuntungan dari AI, dan para praktisi memperingatkan bahwa jika para aktor pro-sosial tidak mengikutinya, para ekstremis dapat memperoleh keuntungan teknologi meskipun ada potensi manfaat yang kuat dari AI untuk pekerjaan pencegahan.

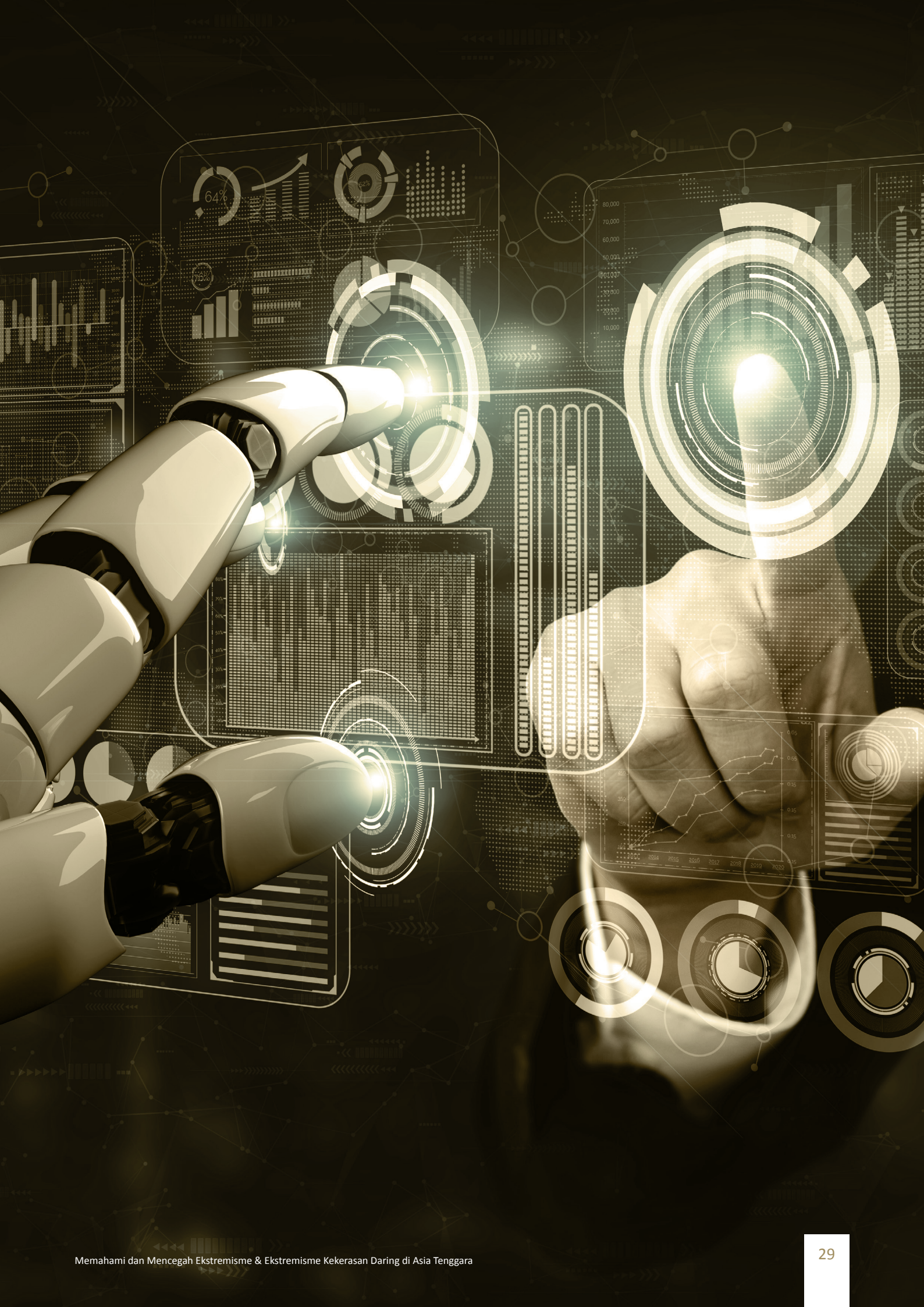
Salah satu kekhawatiran langsung adalah penggunaan AI generatif untuk menghasilkan propaganda ekstremis yang lebih persuasif dan lebih sulit dibedakan sebagai tidak otentik. Alat-alat AI generatif (untuk teks, gambar, video, dan audio) memungkinkan pengguna untuk membuat konten dengan mudah. Para peneliti mencatat bahwa para teroris sudah mengadopsi alat tersebut:

*“Kelompok teroris semakin banyak mengadopsi AI generatif untuk meningkatkan dan menyebarkan propaganda mereka, membuatnya lebih efisien dan disesuaikan dengan audiens tertentu. Hal ini termasuk membuat gambar, video, atau audio sintesis untuk mengintensifkan pesan mereka dan memengaruhi emosi” (Sulaimarl & De Lang, 2024, hlm.23).*

Para ahli di Indonesia sudah memperhatikan konten daring yang tampak mencurigakan dan berasal dari kalangan ekstremis. Seorang narasumber membagikan contoh unggahan TikTok/Instagram yang membahas filsafat dan konsep agama dengan kedalaman yang mengejutkan - unggahan-unggahan tersebut secara halus menyimpulkan bahwa “filsafat itu salah dan hanya ada satu kepercayaan yang benar,” yang selaras dengan pandangan kelompok garis keras (IND24). Orang yang diwawancarai menyatakan, “Saya yakin ini dibuat dengan menggunakan AI karena ... kelompok-kelompok ini anti-filsafat. Kajian linguistik dan agama yang disajikan ... terlihat sangat mendalam, memberikan kesan bahwa pembuatnya adalah ahli, [namun] seringkali tidak demikian. Kontennya dibuat agar terlihat mengesankan, menciptakan ilusi bahwa pembuatnya adalah seorang sarjana atau ahli” (IND24). Dengan kata lain, pembuatan teks dengan AI dapat membantu para ekstremis membuat narasi yang ditulis dengan baik dan terdengar berwibawa, yang mungkin sulit dibuat oleh para penyebarannya yang sebenarnya. Pada saat yang sama, para praktisi menunjukkan contoh-contoh konten bergaya anime yang dibuat oleh AI di kanal Telegram dan Instagram ekstremis di Indonesia dengan para VEO yang secara aktif “berusaha membuatnya menarik bagi anak muda” (IND21). Konten-konten ini, selain menstimulasi secara visual, juga dapat menampilkan teks overlay dengan ajakan untuk bertindak (ibid). Singkatnya, perangkat AI sudah digunakan di Indonesia untuk membantu pesan ekstremis agar lebih beresonansi dengan audiens yang berpendidikan atau skeptis dan membanjiri umpan sosial dengan konten berkualitas tinggi yang ditargetkan dengan baik.

AI juga terkait dengan pengembangan informasi yang salah dan pemalsuan, yang dapat memicu narasi ekstremis atau menyebabkan kekacauan sosial yang dieksploitasi oleh para ekstremis. Dengan model difusi gambar yang tertanam dalam perangkat AI, lebih mudah dari sebelumnya untuk membuat gambar atau video yang realistis dan menyuntikkannya ke media sosial. Para ahli di Indonesia dengan waspada mengamati peningkatan global dalam deepfake. Salah satu narasumber menyebutkan kemungkinan para ekstremis menggunakan AI untuk membuat pernyataan atau video palsu tentang tokoh-tokoh penting di Indonesia untuk mengikis kepercayaan. “Orang-orang penting yang moderat ... wajah mereka digunakan [dalam deepfake] ... Mereka menyampaikan ucapan [ekstremis palsu] ... meskipun kita tahu orang ini adalah orang yang baik” (IND25). Rekayasa Bom Bali melalui deepfake di TikTok di Indonesia, seperti yang telah disebutkan sebelumnya, memberikan gambaran yang jelas tentang bagaimana hal ini dapat dimanfaatkan (IND1). Dampak psikologis dari video yang dipalsukan secara meyakinkan bisa sangat signifikan. Para ekstremis sering kali selangkah lebih maju dalam mengadopsi teknologi baru: para aktor pencegahan dan penegakan hukum harus mengikutinya.







AI juga dapat membantu dalam penargetan mikro dan personalisasi pesan rekrutmen. Dengan menggunakan AI analitik, para aktor ekstremis secara teori dapat menganalisis kumpulan data yang besar (profil media sosial, metrik keterlibatan) untuk mengidentifikasi individu yang mungkin rentan terhadap radikalisasi dan kemudian menyesuaikan propaganda kepada mereka. Seperti yang dicatat oleh seorang peneliti, “AI analitik dapat digunakan untuk menganalisis data individu untuk mempersonalisasi taktik perekrutan” (Sulaimarl & De Lang, 2024, hlm. 23). Informasi yang tersedia untuk umum - misalnya, kesukaan, share (apa yang dibagikan), dan keanggotaan grup seseorang - dapat diproses oleh alat AI untuk menyimpulkan keluhan atau minat mereka (seperti yang dilakukan oleh algoritme media sosial) dan secara otomatis menghasilkan konten yang sesuai dengan sentimen tertentu: “Algoritme generasi bahasa alami yang digerakkan oleh AI (natural language generation, NLG) memiliki kemampuan untuk membuat konten berbasis teks yang persuasif ... yang beresonansi dengan individu tertentu,” secara efektif “menyesuaikan pesan mereka untuk menyelaraskan dengan keyakinan dan keluhan yang sudah ada sebelumnya dari individu tersebut” (Ismaizam, 2023, hlm. 163). Meskipun tidak ada kasus yang terkonfirmasi tentang ekstremis Indonesia yang melakukan kampanye yang sangat personal seperti itu, terlepas dari kampanye berbasis anime ini, teknologinya tersedia dan perlu diamati dengan seksama, dan dalam praktiknya, beberapa orang yang diwawancarai percaya bahwa kelompok-kelompok ekstremis telah menggunakan bentuk-bentuk penargetan berbasis AI yang lebih sederhana. Salah satunya mencatat bahwa kelompok-kelompok ini “menggunakan AI untuk memetakan konten dan audiens di media sosial” - pada dasarnya menganalisis narasi apa yang sesuai dengan demografi yang mana - dan kemudian “mengidentifikasi segmen pasar yang dapat ditargetkan oleh kelompok ekstremis ... membuat narasi yang disesuaikan untuk menarik audiens tersebut” (IND24). Hal ini menunjukkan tingkat operasi media strategis, di mana AI atau setidaknya beberapa tingkat analisis data memandu fokus propaganda (misalnya, mendorong konten anti-pemerintah kepada pengguna yang menunjukkan ketidakpercayaan kepada negara, atau narasi sektarian kepada mereka yang memiliki pandangan konservatif). Segmentasi semacam itu meningkatkan kemampuan propaganda. Akhirnya, seorang ahli menyoroti penggunaan kecerdasan buatan (AI) untuk menerjemahkan teks dari bahasa Inggris dan Arab ke dalam bahasa Indonesia, menciptakan “lapisan baru aksesibilitas dan otonomi” bagi pengikut dan perekrut (IND19). Memanfaatkan AI sebagai cara untuk menghasilkan pesan yang dipersonalisasi serta mendaur ulang pesan yang sudah ada dalam bahasa lain meningkatkan peluang bagi para pelaku ekstremis untuk memproduksi dan membagikan propaganda secara daring.

Ancaman lainnya adalah agen interaktif atau chatbot yang didukung oleh AI. Kelompok-kelompok ekstremis dan ekstremis dengan kekerasan dapat menggunakan chatbots di platform (Telegram, Terrorist Operated Websites (TOWs), atau bahkan media sosial arus utama melalui pesan langsung) untuk berinteraksi dengan orang-orang yang ingin tahu atau calon anggota baru. Bot-bot ini, yang didukung oleh model bahasa yang besar, dapat mensimulasikan percakapan manusia dan menjawab pertanyaan tentang ideologi ekstremis, yang secara efektif bertindak sebagai agen radikalisasi 24/7. Pakar keamanan memperingatkan bahwa “teroris dapat menggunakan chatbot yang didukung oleh model bahasa besar (LLM), seperti ChatGPT, untuk berinteraksi dengan calon anggota baru” (Sulaimarl & De Lang, 2024, hlm. 23). Ismaizam (2023, hlm.163) juga mencatat bahwa “chatbots AI dan asisten virtual beroperasi dengan mahir di platform media sosial, secara aktif terlibat dengan pengguna ... dengan terampil menirukan interaksi manusia, semakin mengindoktrinasi pengguna dengan ideologi ekstremis.” Model-model jailbreak tersedia dan dapat menyediakan interaksi semacam itu. Keterlibatan satu-ke-satu ini bisa sangat kuat, terutama jika perekrut manusia langka, dengan preseden yang mengkhawatirkan di domain lain (misalnya, jaringan penipuan yang menggunakan bot untuk penipuan) dan tren saat ini menunjukkan bahwa kasus penggunaan utama AI adalah untuk terapi dan pendampingan (Zao-Sanders, 2025), sementara bot pendamping yang meradikalisasi telah mendorong individu untuk melakukan kekerasan di Inggris.

Menariknya, orang-orang yang diwawancarai mencatat bahwa kelompok-kelompok moderat dan kontra-ekstremis di Indonesia mungkin belum memanfaatkan AI secara ekstensif karena keraguan etis atau filosofis. Salah satu narasumber yang diwawancarai mengamati bahwa “kelompok agama moderat ... belum menggunakan AI untuk melawan konten ekstremis karena mereka masih percaya bahwa pekerjaan mereka harus berasal dari pemikiran orisinal” (IND24). Sikap berprinsip ini, meskipun patut diacungi jempol, dapat membuat para aktor pencegahan dirugikan jika para ekstremis menggunakan AI sepenuhnya. Orang yang diwawancarai menyiratkan bahwa tanpa mengadopsi alat baru, praktisi pencegahan dan penanggulangan ekstremisme “akan selalu tertinggal dalam hal memanfaatkan teknologi,” karena para pelaku ekstremis dan teroris sering kali tidak memiliki kepedulian terhadap etika (IND24).

Kekhawatiran lain yang tampak ke depan adalah AI digunakan dalam perencanaan serangan atau serangan siber. Perangkat AI analitis dapat membantu para ekstremis melakukan pengintaian (misalnya, menganalisis citra satelit atau data Google Maps untuk memilih target atau merencanakan rute). Di dunia maya, AI dapat mengotomatiskan pembuatan email phishing atau mengidentifikasi kerentanan perangkat lunak, yang berpotensi menurunkan standar

bagi kelompok ekstremis untuk melakukan peretasan. Seperti yang dikatakan oleh salah satu sumber, “serangan siber dapat digunakan oleh teroris untuk menimbulkan kerusakan yang signifikan; AI dapat membantu membuat email phishing yang lebih meyakinkan dan penyalahgunaan lainnya” (Ismaizam, 2023, hlm.162). Meskipun belum terlihat di Indonesia, risiko tetap ada seiring dengan berkembangnya alat-alat ini.

Ada juga cara yang tidak disengaja di mana AI memengaruhi lanskap ekstremisme: melalui bagaimana masyarakat menggunakan AI untuk mendapatkan informasi. Salah satu narasumber menunjukkan bahwa anak muda semakin beralih ke chatbot AI untuk mengajukan pertanyaan yang rumit, termasuk pertanyaan agama atau ideologis. “Alat-alat AI seperti ChatGPT juga digunakan untuk mengajukan pertanyaan-pertanyaan agama... dan mereka memberikan jawaban yang cepat dan meyakinkan. Hal ini membuat informasi tersebut tampak nyata dan otoritatif” (IND24). Bahayanya ada dua: AI dapat memberikan jawaban yang, meskipun netral, tidak memiliki konteks atau nuansa yang diperlukan untuk pertanyaan-pertanyaan sensitif. Lebih buruk lagi, jika data pelatihan AI tidak mencukupi atau tidak selaras dengan pertanyaan-pertanyaan ini, AI dapat menggemakan sudut pandang yang condong ke arah ekstremis (Shah et al., 2025). Secara umum, ini bukan tentang ekstremis yang menciptakan alat AI dan lebih kepada publik yang tanpa disadari mempercayai keluaran AI yang dapat memperkuat narasi ekstremis.

AI merupakan pedang bermata dua dalam konteks ekstremisme. Para aktor garda depan di Indonesia melihat bahwa para ekstremis mulai mengeksploitasi AI untuk pembuatan dan penargetan konten, memberikan mereka kemampuan yang berpotensi besar untuk mempengaruhi dan menghindari deteksi. Sementara itu, mereka yang bekerja melawan ekstremisme berupaya mengejar ketertinggalan - menggunakan AI untuk memperkuat narasi positif dan mendeteksi konten fitnah yang dihasilkan oleh AI. Pesan utama untuk audiens kebijakan adalah bahwa AI mempercepat tantangan - mulai dari propaganda palsu hingga radikalisasi yang dipersonalisasi, tren yang digerakkan oleh AI yang muncul ini dapat secara signifikan membentuk masa depan ekstremisme jika langkah-langkah proaktif tidak diambil.

### 3.2.3. Teknologi yang Kurang Digunakan: Web Gelap, VR/XR, Drone, Senjata Api 3D, dan Lainnya

Para ahli garis depan juga mengidentifikasi berbagai tren teknologi lain yang, meskipun saat ini masih bersifat perifer, dapat segera menjadi pendorong utama ekstremisme. Ini termasuk teknologi keuangan yang berkembang (mata uang kripto dan NFT, yang sering kali difasilitasi melalui web gelap) serta platform imersif (metaverse) dan bahkan perangkat keras seperti drone dan senjata api cetak 3D. Alat dan domain ini umumnya bersifat transnasional dan anonim, itulah sebabnya mengapa para aktor teroris menganggapnya menarik.

Dark web - bagian tersembunyi dari internet yang dapat diakses melalui peramban dan alat khusus - sering kali berjalan seiring dengan kripto dalam pendanaan teroris. Di forum atau pasar web gelap, para ekstremis dapat meminta sumbangan atau memperdagangkan barang terlarang dengan tingkat anonimitas yang tinggi. Sebuah studi baru-baru ini menunjukkan bahwa “penggalangan dana dan transaksi keuangan semakin banyak dilakukan di web gelap melalui mata uang kripto digital seperti Bitcoin dan Monero. Platform ini memungkinkan organisasi teroris untuk menggalang dana melalui donasi Bitcoin, pemerasan daring, dan bahkan perdagangan manusia dan organ tubuh” (Sulaimar & De Lang, 2024, hlm. 25). Meskipun para praktisi P/CVE di Indonesia belum melaporkan adanya pasar teror web gelap di dalam negeri, mereka menyadari fenomena global ini. Faktanya, pejabat keamanan Indonesia telah mengidentifikasi transaksi pendanaan terorisme menggunakan dark web dan kripto (IND3, IND8, IND23). Ketidaktepatan relatif dark web di Asia Tenggara mungkin bersifat sementara; Kantor PBB untuk Narkoba dan Kejahatan (UNODC) memperingatkan hampir lima tahun yang lalu bahwa meskipun data tentang aktivitas dark web di wilayah ini terbatas, “kemungkinan akan berkembang dalam ruang lingkup dan skala dalam waktu dekat” (UNODC, 2020). Oleh karena itu, membangun kapasitas untuk memantau dan melawan transaksi web gelap menjadi agenda bagi pihak berwenang di Indonesia, agar para ekstremis tidak mengeksploitasi celah ini.

Konsep metaverse - dunia virtual bersama dan game yang sering diakses melalui VR/AR/XR (virtual/augmented/extended reality) - masih terus bermunculan, namun para analis telah mempertimbangkan implikasinya terhadap ekstremisme. Banyak dari potensi bahaya ini yang sudah tercakup dalam bagian game. Namun, karena pengalaman VR dapat mengaburkan batas antara simulasi dan kenyataan, mereka dapat mengintensifkan dampak konten ekstremis dan juga berguna untuk perencanaan dan pelatihan serangan. Pelatihan kebencian yang imersif seperti ini bersifat spekulatif tapi tidak mengada-ada saat teknologi ini menjadi arus utama - dan sudah ada di platform game daring lainnya (Lamphere-Englund & Thompson, 2024).

Drone dan senjata api cetak 3D juga perlu disebutkan. Drone FPV yang murah telah digunakan oleh kelompok teroris dalam konteks lain dan pasukan keamanan Indonesia telah mencatat ketertarikan terhadapnya (McDonald, 2024). Sejauh ini, teroris Asia Tenggara belum secara signifikan menggunakan drone dalam serangan. Sebuah



tinjauan mencatat bahwa teroris “sudah mulai menggunakan drone untuk tujuan pengawasan atau propaganda, tetapi belum menjadi alat utama,” dan penggunaan drone dalam serangan yang sebenarnya masih terbatas (West, 2021, hlm. 31). Penggunaan drone kemungkinan besar akan dikoordinasikan melalui sarana daring (atau fly-by-wire), dan setiap peningkatan aktivitas drone mungkin bertepatan dengan tutorial dan pengadaan daring. Seorang narasumber menyebutkan bahwa terdapat kekhawatiran yang semakin meningkat terkait anggota kelompok lokal seperti JI dan Jamaah Ansharut Syaria (JAS) yang dilatih di luar negeri dalam penggunaan drone, dan menyerukan pemantauan yang lebih ketat terhadap tren ini serta implikasinya di negara ini di masa yang akan datang (IND19). Sementara itu, senjata api cetakan 3D menjadi lebih mudah dibuat dan jauh lebih tahan lama, sehingga dapat dengan mudah menghindari pembatasan senjata api (Veilleux-Lepage dan Füredi, 2025). Setidaknya satu orang yang diwawancarai di Indonesia mencatat kekhawatiran mereka bahwa kelompok-kelompok tertentu akan segera menggunakan pencetakan 3D (IND19).

Tren lainnya adalah kemungkinan bertemunya kejahatan siber terorganisir dan ekstremisme. Para pejabat Indonesia mengamati bahwa beberapa aktor non-lokal di wilayah yang terkena dampak konflik terlibat dalam “penggalangan dana bawah tanah ... menyamar di sekolah-sekolah Islam” (IND10). Hal ini mungkin menunjukkan adanya tumpang tindih antara jaringan kriminal dan jaringan teroris, dengan maraknya penipuan daring yang menjadi pendekatan penggalangan dana yang potensial. Sebuah kasus pendanaan terorisme bersejarah di Indonesia, sebuah operasi skimming bank daring pada tahun 2011 yang menjaring militan sebesar \$700 ribu, menunjukkan konvergensi ini (Nuraniyah, 2019, hlm.6). Jika kelompok-kelompok ekstremis memanfaatkan dunia kejahatan siber di Indonesia atau di Asia Tenggara, kita bisa melihat lebih banyak lagi plot pendanaan hibrida.

### 3.3. Tanggapan: Masa Lalu dan Masa Depan

Bagian temuan akhir yang disajikan dalam laporan ini akan membahas pertanyaan penelitian berikut:

**Pelajaran, tantangan, tanggapan, dan kebutuhan apa yang diidentifikasi oleh aktor garda depan yang bekerja untuk mencegah dan melawan ekstremisme di dunia maya?**

Oleh karena itu, bagian ini secara khusus menyoroti perspektif para praktisi dan pemangku kepentingan di garis depan yang bekerja untuk mencegah dan melawan ekstremisme dan kekerasan di dunia maya, dan pelajaran yang telah mereka pelajari, tantangan yang mereka hadapi, dan kebutuhan selanjutnya yang telah mereka tentukan. Perspektif lebih lanjut dari penelitian digabungkan untuk menguji hasil dan memperluas diskusi.

#### 3.3.1. Tanggapan yang Ada

Pendekatan berbasis masyarakat di Indonesia, seperti Rencana Aksi Nasional Pencegahan dan Penanggulangan Ekstremisme Berbasis Kekerasan yang Mengarah pada Terorisme (RAN PE) yang dipimpin oleh pemerintah, dan inisiatif-inisiatif LSM seperti Komuji, PeaceGen, dan Indika Foundation, tampaknya telah mendorong kolaborasi dan inovasi yang lebih besar. Sebagai contoh, inisiatif ArtVocation dari Komuji mengintegrasikan lokakarya mendongeng, seni, dan musik untuk membangun narasi tandingan, terutama di kalangan anak muda. Contoh lainnya adalah kolaborasi PeaceGen dengan KHub, yang membimbing OMS untuk mengembangkan narasi alternatif, dengan menekankan pemikiran kritis dan empati. Tantangan yang umum terjadi adalah kesenjangan sumber daya dan pelatihan, termasuk di bidang komunikasi strategis daring, meskipun kampanye kontra-narasi di Indonesia dianggap tepat sasaran dan menarik (termasuk yang dikategorikan dalam Strategi Komunikasi Strategis RAN PE).

Meskipun anak muda Indonesia sering dianggap sebagai kelompok yang paling rentan terhadap radikalisasi, peran mereka sangat penting dalam strategi CEVE. Program-program yang bertujuan memberdayakan kaum muda untuk menciptakan dan menyebarkan kontra-narasi telah menunjukkan hasil yang menjanjikan, tetapi seringkali masih berskala kecil. Meskipun ada berbagai program MIL yang aktif di Indonesia, program-program tersebut melayani berbagai aktor (tidak hanya kaum muda) dan tidak selalu terintegrasi ke dalam sistem pendidikan, serta tidak cukup besar untuk menjangkau segmen populasi yang signifikan ini.

Moderasi konten menghadapi berbagai tantangan - keragaman bahasa dan budaya menciptakan rintangan yang signifikan bagi platform teknologi dalam memoderasi konten ekstremis melalui pendekatan pembelajaran mesin, dan para ekstremis dapat mengeksploitasi nuansa bahasa, bahasa yang dienkripsi, dan referensi budaya yang sering kali disalahpahami atau terlewatkan oleh perangkat moderasi global. Upaya untuk mengatasi tantangan-tantangan ini memiliki sumber daya yang terbatas dan tidak memiliki pendekatan sistematis untuk memasukkan keahlian lokal ke

dalam kerangka kerja moderasi konten, meskipun banyak aktor juga menyoroti kerja sama dan keterlibatan positif untuk tujuan-tujuan ini antara pemerintah dan sektor teknologi. Demikian pula, banyak pemangku kepentingan yang diwawancarai menekankan kemajuan konstruktif dalam koordinasi dan kolaborasi antara pemerintah, masyarakat sipil, dan platform teknologi, sembari mencatat bahwa tantangan dalam hal ini masih ada. Seperti di banyak konteks lainnya, keterbatasan sumber daya dan pendanaan yang tidak konsisten juga membatasi skala dan dampak inisiatif.

### Pendekatan atau Kerangka Kerja Perundang-undangan, Kebijakan & Hukum

Fokus utama diskusi dalam hal kerangka hukum dan kebijakan untuk merespons dalam melawan ekstremisme dan ekstremisme kekerasan di dunia maya adalah RAN PE Indonesia. Seperti yang dicatat dalam sebuah artikel baru-baru ini, “pemerintah mengeluarkan peraturan presiden pada tahun 2021 untuk memberlakukan Rencana Aksi Nasional Pencegahan dan Penanggulangan Ekstremisme Berbasis Kekerasan yang Mengarah pada Terorisme (RAN PE), setelah advokasi dan perencanaan dari Badan Nasional Penanggulangan Terorisme (BNPT) dan para mitranya. Di antara serangkaian proses dan niat, rencana tersebut berupaya untuk meningkatkan koordinasi di antara para pemangku kepentingan dan mendorong kepemilikan strategi pencegahan di tingkat daerah. [Meskipun masih ada tantangan yang dihadapi, pemerintah Indonesia sedang membangun infrastruktur P/CVE yang sangat menjanjikan yang dapat menghasilkan manfaat jangka panjang, jika antusiasme dan sumber daya dimobilisasi dan dipertahankan di tahun-tahun mendatang” (Sumpter, 2024, hlm. 10).

RAN PE secara konsisten ditekankan sebagai pendorong utama koordinasi dan keterlibatan dengan para pelaku di tingkat lokal (IND24), dengan salah satu narasumber yang diwawancarai mencatat bahwa RAN PE telah “membuka pintu untuk kolaborasi yang berarti” (IND17). Kelompok kerja tematik dianggap telah meningkatkan fokus program dan memberikan kerangka kerja bagi para pelaku utama di tingkat lokal dan OMS untuk menyelaraskan dan memfokuskan upaya mereka (IND24). Kelompok kerja tematik juga telah memfasilitasi kolaborasi dengan berbagai pihak, dan mengurangi keengganan untuk berkolaborasi di antara beberapa aktor (IND24). Salah satu OMS yang diwawancarai menyatakan bahwa RAN PE telah memfasilitasi keterlibatan yang lebih baik dengan kementerian, yang pada gilirannya memungkinkan mereka untuk mengintegrasikan perspektif gender dengan lebih baik dalam program mereka melalui keterlibatan dengan kementerian terkait. Juga disoroti bahwa RAN PE telah membangun pengakuan yang lebih besar terhadap pekerjaan OMS dan mengangkat isu upaya penanggulangan ekstremisme dan ekstremisme kekerasan di kalangan mereka dan aktor lokal terkait lainnya (IND17). Seorang narasumber mengatakan:

*“RAN PE secara signifikan meningkatkan pendekatan kami dalam memoderasi ekstremisme daring dengan mempromosikan kolaborasi di antara berbagai pemangku kepentingan yang dapat menangani ekstremisme daring dan offline dengan cara yang terkoordinasi. Aktor tradisional [...] fokus pada penegakan hukum dan pemantauan daring, tetapi RAN PE mengajak kementerian, pemerintah daerah, dan organisasi masyarakat sipil untuk bekerja sama. Kolaborasi ini memungkinkan kami untuk mengatasi ekstremisme daring dengan strategi yang lebih bersifat preventif dan berbasis masyarakat” (IND12).*

RAN PE dianggap telah memperkuat pendekatan di seluruh area isu yang dibahas dalam Laporan ini, termasuk melawan narasi ekstremis di dunia maya, meningkatkan moderasi konten, dan mempromosikan MIL (IND12).

Kerangka hukum juga sangat penting bagi upaya moderasi konten (lihat 3.1.2. Moderasi Konten di bawah). Indonesia memiliki undang-undang yang memberikan pemerintah kemampuan untuk menghapus atau memblokir akses ke platform atau Penyedia Layanan Internet (ISP) yang memfasilitasi peredaran propaganda ekstremisme, serta memungkinkan penuntutan terhadap ujaran daring dan pelanggaran siber lainnya, mewajibkan penghapusan konten dan pelarangan pengguna, serta mewajibkan platform daring untuk mengikuti peraturan yang telah digariskan dan mendaftarkan diri ke Kementerian Komunikasi dan Informatika (Wibisono dkk, 2024). Bersama-sama, UU No. 5/2018 tentang Pemberantasan Tindak Pidana Terorisme dan UU No. 19/2016 tentang Informasi dan Transaksi Digital menjadi dasar hukum penindakan konten ekstremis kekerasan di internet” (Wibisono et al., 2024, hal. 149 & 150f). Peraturan perundang-undangan lain yang relevan meliputi Peraturan Presiden Nomor 77 Tahun 2019 tentang Pencegahan Terorisme dan Perlindungan Penyidik, Jaksa Penuntut Umum, Hakim, dan Petugas Pemasyarakatan, serta Keputusan Menteri Komunikasi dan Informatika Nomor 172 Tahun 2024, yang memberikan pedoman mengenai denda terkait konten yang dibuat oleh pengguna (User Generated Content atau UGC).<sup>1</sup>

1 Harap diperhatikan bahwa penelitian ini tidak melakukan pemetaan komprehensif terhadap peraturan perundang-undangan yang relevan, dan kerangka hukum yang tercantum di sini tidak dimaksudkan untuk menjadi daftar lengkap semua peraturan perundang-undangan yang berlaku, melainkan kerangka hukum utama yang diidentifikasi melalui literatur dan peserta penelitian.

## Moderasi Konten, Kebijakan & Penegakan Hukum

Acuan yang umum digunakan oleh para pemangku kepentingan pemerintah, khususnya, adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ITE ini memungkinkan Kementerian Komunikasi dan Informatika untuk memblokir informasi yang melanggar secara langsung di dunia maya (Paterson, 2019, hlm.225). Narasumber yang diwawancarai mengatakan bahwa Kementerian Komunikasi dan Informatika melakukan penghapusan akun secara aktif berdasarkan informasi yang dibagikan oleh berbagai departemen yang mengidentifikasi materi yang melanggar. Badan Intelijen Negara (BIN) juga melakukan pengawasan/intelijen secara daring dan luring (IND23). Laporan mengidentifikasi bahwa dari tahun 2017 hingga 2022, 27.443 situs web diblokir di Indonesia karena ‘menyebarkan radikalisme’ atau pelanggaran terkait (Wibisono et al., 2024, hlm. 152), yang menunjukkan adanya mekanisme identifikasi dan moderasi konten yang relatif kuat. Peningkatan kewenangan di bawah undang-undang anti-terorisme tahun 2018 juga tercatat telah meningkatkan volume penangkapan terkait (bersamaan dengan peningkatan jumlah staf dan anggaran) (Jones, 2022, h.163). Mekanisme hukum yang efektif untuk memungkinkan moderasi dan penghapusan konten berbahaya adalah kuncinya, meskipun beberapa penelitian telah menyuarakan keprihatinan terkait penerapan undang-undang ini secara luas - para aktor pemerintah juga mengakui dalam wawancara bahwa kebebasan berpendapat dan berekspresi adalah lensa penting bagi upaya penghapusan konten, serta menekankan perlunya melestarikan ujaran-ujaran yang ‘tidak nyaman’ yang mungkin tidak disukai atau disetujui oleh sebagian pihak, tetapi tidak melanggar UU ITE (IND8). Para narasumber yang diwawancarai menggambarkan kerangka kerja yang relatif jelas untuk keterlibatan para pihak yang terlibat dalam upaya moderasi konten ini, yang melibatkan pihak-pihak seperti Badan Siber dan Sandi Negara (BSSN) dan BNPT di tingkat nasional, dan kerja sama dengan mitra regional dan lokal seperti Kementerian Komunikasi dan Informatika (IND8). Beberapa orang yang diwawancarai juga mencatat bahwa kemampuan teknis para aktor seperti Kementerian Komunikasi dan Informatika untuk mengidentifikasi dan menghapus konten berbahaya telah meningkat (IND10).

Praktisi dan pemangku kepentingan yang diwawancarai juga menekankan perlunya mempertimbangkan, dan mengatasi, ‘jalur’ konten yang dapat masuk ke dunia maya. Secara khusus, keterlibatan Kementerian Agama dengan para penyuluh agama yang dapat menyampaikan pesan agama yang positif dan sah, baik secara offline maupun daring (IND9) dan mengurangi kebutuhan akan moderasi konten (IND9).

## Komunikasi Strategis - Melawan Narasi Ekstremis dan Kekerasan Ekstremis

### Komunikasi Strategis Pemerintah

Di bawah RAN PE terbaru, BNPT ditugaskan untuk “meningkatkan peran berbagai tokoh masyarakat, media massa, dan pemberi pengaruh di media sosial dalam menyampaikan pesan-pesan pencegahan ekstremisme kekerasan [...] mengoordinasikan strategi kontra-narasi baik melalui media daring maupun luring” (Wibisono dkk., 2024, hlm. 148). Hal ini diperkuat oleh dokumen Peta Jalan Komunikasi Strategis RAN PE (KOMSTRA PE), yang diselaraskan dengan strategi komunikasi regional dan global yang sudah ada, seperti salah satunya adalah program Preventing Violent Extremism (PVE) melalui Komunikasi Strategis dari UNOCT dan Rencana Aksi ASEAN untuk Mencegah dan Melawan Bangkitnya Radikalisasi dan Ekstremisme Kekerasan (2018). Dalam hal ini, BNPT memiliki upaya komunikasi strategis yang sedang berlangsung dan bekerja untuk menyampaikan narasi tandingan dan memantau narasi yang muncul dan lazim baik secara offline maupun daring untuk merespons secara efektif, yang mencakup taktik seperti ‘membanjiri’ media dengan konten yang positif dan moderat melalui media Islam moderat (IND8, IND25). Selain upaya kontra narasi darangnya sendiri, BNPT telah membuat inisiatif seperti Duta Damai Dunia Maya, sebuah komunitas sukarelawan yang menciptakan “konten positif dan damai sehingga perkembangan konten negatif dan radikalisme dapat dikurangi” (Abdullah & Alfatra, 2019, hlm. 159). Beberapa praktisi garis depan menyebutkan peran penting ‘Duta Damai Dunia Maya’ BNPT sebagai penyampai pesan utama baik secara daring maupun luring untuk upaya kontra-propaganda (IND25), yang menyatukan para kreator konten daring anak muda yang mendapatkan pelatihan dan dukungan untuk membuat konten narasi tandingan daring dan luring mereka sendiri atau konten narasi positif, serta mengajarkan kreator lain untuk melakukannya (Tio & Kruber, 2022).

Wawancara juga menyoroti berbagai upaya pemerintah terkait untuk meningkatkan keamanan daring dan mengatasi misinformasi, melalui berbagai upaya seperti seri video pendek tentang perjudian daring, pinjaman predator, hoaks, dan penipuan (IND5). Kementerian Komunikasi dan Informatika (sebelumnya dikenal sebagai Kominfo, sekarang Komdigi) dalam satu dekade terakhir telah melakukan upaya aktif untuk meningkatkan literasi digital, seperti pengarahannya tentang hoaks yang baru-baru ini diposting secara daring (Paterson, 2019).

## Upaya Komunikasi Strategis yang Dipimpin oleh Non-Pemerintah dan Masyarakat Sipil

Diakui secara luas bahwa organisasi masyarakat sipil (OMS), yang sering kali memiliki hubungan yang erat dengan masyarakat yang mereka layani, memiliki posisi yang sangat baik untuk melakukan komunikasi strategis yang efektif karena pengetahuan mereka tentang khalayak sasaran dan kepercayaan khalayak tersebut. OMS di Indonesia secara aktif melakukan berbagai jenis upaya komunikasi strategis, beberapa di antaranya secara khusus ditargetkan untuk mencegah dan melawan ekstremisme dan ekstremisme kekerasan, dan yang lainnya memiliki potensi dampak positif di bidang pembangunan perdamaian, toleransi, dan keberagaman, atau pemikiran kritis, misalnya. OMS yang diwawancarai untuk Laporan ini menyoroti beberapa upaya yang mereka advokasi dan terbukti efektif. Upaya-upaya tersebut termasuk mengembangkan berbagai ‘merek’ atau saluran yang ditargetkan untuk berbagai jenis konten (misalnya, saluran yang menjangkau audiens Islam milenial; saluran lain yang lebih umum tentang toleransi dan keragaman; satu saluran khusus untuk siswa) dan menyoroti bahwa hal tersebut telah meningkatkan keterlibatan dan efektivitas (IND6). OMS Mubadalah menyoroti strategi utama seperti menggunakan narasi alternatif (daripada ‘melawan’), menekankan rasa saling menghormati dengan menggunakan pendekatan yang sesuai dengan audiens mereka, dan memberikan interpretasi yang inklusif dan positif terhadap ajaran agama (IND14).

Aktor-aktor lain mengelola situs web dengan narasi tandingan untuk mempromosikan Islam moderat (Wibisono et al, 2024; Suryana, 2018); misalnya, Nahdlatul Ulama (NU), organisasi Islam independen terbesar di Indonesia, meluncurkan kampanye anti-ekstremisme global ‘untuk menyebarkan pesan tentang Islam yang toleran (Islam toleran) untuk mengekang radikalisme, ekstremisme, dan terorisme’ (Varagur, 2015), dan untuk melakukan hal tersebut, NU telah merangkul media dan komunikasi strategis, dengan inisiatif utama seperti film dokumenter Rahmat Islam Nusantara (2015) dan inisiatif ‘prajurit siber’ (Schmidt, 2021, hlm.237), serta melatih para relawan untuk membuat dan menyebarkan narasi tandingan dan alternatif di media sosial (Schmidt, 2018). Ada situs web serupa lainnya yang bertujuan untuk melawan ekstremisme dan mempromosikan Islam moderat, sering kali dengan ‘menyanggah’ ideologi atau interpretasi ekstremis dengan pengetahuan agama, memproduksi konten oleh mantan ekstremis, atau menciptakan narasi alternatif (Rahman et al., 2023, hlm. 275). Yang lain berusaha menciptakan platform untuk konten positif, seperti Mikrofon.id, sebuah platform yang terdiri dari jurnalis, seniman, dan praktisi budaya yang bekerja untuk membangun kapasitas dan mendukung outlet media komunitas lainnya untuk menangani isu-isu sensitif melalui seni dan karya kreatif (IND24).

Aktor masyarakat sipil dan non-pemerintah lainnya berupaya memberdayakan pembuat konten untuk mengembangkan narasi tandingan atau alternatif, seperti perusahaan sosial Peace Generation Indonesia (PeaceGen) yang memimpin Creator Academy yang didukung oleh Google Project Inspire, atau inisiatif ‘Creators for Change’ yang dirancang oleh YouTube dan UNDP yang memberikan dana bantuan kecil di Indonesia dan negara-negara Asia Tenggara lainnya (Tio & Kruber, 2022). Garis besar dari upaya-upaya ini adalah pelibatan dan penguatan masyarakat yang terdampak, terpinggirkan dan/atau masyarakat lokal, dan berbagai OMS menekankan hal ini - misalnya, INFID menyoroti pengalaman positifnya dalam melibatkan anak muda dalam pembuatan konten (IND21).

## **Pendidikan, Membangun Toleransi, dan Mengembangkan Literasi Media & Informasi (MIL)**

Secara positif, dalam hal upaya toleransi dan kesetaraan gender, penelitian dari tahun 2023 menunjukkan adanya penurunan intoleransi di Indonesia (Halida et al., 2023). OMS telah menyoroti keberhasilan dalam memperkenalkan perspektif gender dalam ruang agama melalui media sosial, dengan mendukung panutan positif seperti ulama perempuan (IND17) dan Ulama Perempuan (seperti KUPI, Kongres Ulama Perempuan Indonesia). Mereka mencatat adanya peningkatan jumlah platform yang menawarkan konten Islam yang lebih beragam, inklusif, dan peka terhadap gender (IND11, IND14). Berdasarkan hal ini, berbagai upaya Literasi Media dan Informasi (MIL), serta upaya untuk meningkatkan toleransi telah dilakukan di seluruh Indonesia, yang menargetkan berbagai audiens. Sebagai contoh, Kementerian Pendidikan dan Kebudayaan mengelola ‘Merdeka Mengajar’, sebuah platform pembelajaran daring bagi para guru di mana konten tentang keberagaman dan toleransi dapat disebarkan dan menjangkau ratusan ribu pengguna, memberikan penyebaran daring yang mendukung upaya luring (IND3).

Gerakan nasional seperti Siberkreasi, Mafindo, dan AIS Nusantara di Indonesia bertujuan untuk mengajarkan MIL kepada masyarakat luas untuk memerangi disinformasi, terutama melalui kegiatan luring (Ummah & Al Fajri, 2020). Program seperti CekFakta, sebuah “proyek pengecekan dan verifikasi fakta yang diluncurkan oleh dua puluh dua perusahaan media dengan tujuan melatih jurnalis untuk memerangi misinformasi dan disinformasi” (Liu, 2018), juga telah menjawab tantangan ini, dalam hal ini merupakan hasil kolaborasi antara Google News, Asosiasi Media Siber Indonesia (AMCI), Masyarakat Anti Fitnah Indonesia (Mafindo), Aliansi Jurnalis Independen (AJI), dan Internews (Paterson, 2019, hlm. 224). Facebook (sekarang Meta) sebelumnya juga telah mendukung upaya serupa melalui OMS lokal (Tio & Kruber, 2022). Ruangobrol mengembangkan narasi alternatif dan dilaporkan

sedang menguji coba pendekatan ‘pengalihan’, di mana mereka yang mencari istilah-istilah terkait ekstremisme dapat dialihkan ke Ruangobrol atau ke sumber tepercaya yang memandu pengguna untuk mendapatkan informasi yang berimbang (IND12). Sementara wawancara dengan praktisi dan pemangku kepentingan utama yang dilakukan untuk penelitian ini menyoroti berbagai pendekatan inovatif, mereka juga menekankan perlunya dukungan teknis dan peningkatan kapasitas bagi OMS, praktisi media, dan aktor pemerintah, yang sebelumnya telah didukung atau dilakukan oleh organisasi seperti AJI dan BNPT, tetapi masih relatif terbatas dalam skala dan jangkauan dan idealnya dapat mencakup khalayak yang lebih luas, seperti tokoh masyarakat, pendidik, dan pembuat kebijakan (IND10).

Berbagai macam OMS tercatat memiliki, atau menjadi bagian dari, berbagai intervensi MIL, yang menggabungkan elemen-elemen mulai dari keamanan digital hingga kebebasan beragama dan keadilan gender (IND24). MIL umumnya merupakan komponen dari program atau inisiatif yang lebih luas - misalnya, pekerjaan Komuji dengan pemuda dan seniman di Bandung, meskipun tidak berfokus secara khusus pada MIL, mendorong kaum muda untuk “berpikir kritis tentang informasi yang mereka terima, memprosesnya dengan perspektif inklusif, dan meresponsnya secara kreatif” (IND24). Organisasi-organisasi lain berkolaborasi dengan media digital dan media alternatif untuk mempromosikan literasi media (IND14); atau mempromosikan inklusi atau kebebasan beragama (IND24). Menanggapi lanskap digital yang baru, organisasi di Indonesia - seperti Bersinergi - bekerja untuk menawarkan pelatihan tentang ‘literasi AI’ yang memiliki komponen MIL yang kuat, dan organisasi lain memiliki upaya ‘debunking’ yang mengidentifikasi informasi yang salah dan berusaha memperkuat literasi digital, seperti Mafindo atau SafeNet (IND15, IND10), dan Koalisi Cek Fakta, yang didukung oleh Google Initiative (IND11). Bukti terbaru juga menunjukkan potensi gamifikasi - sebuah taktik yang sudah digunakan oleh berbagai aktor, termasuk kelompok ekstremis - sebagai alat untuk komunikasi dan pembelajaran (Mohd Nor, 2023). Moonshot dan IREX menciptakan permainan literasi media Gali Fakta, yang disesuaikan dengan konteks Indonesia, dan menemukan bahwa para peserta “menunjukkan skeptisisme yang jauh lebih besar terhadap berita utama yang salah dan menyatakan berkurangnya kemungkinan untuk menyebarkannya” setelah terlibat dalam permainan tersebut (Facciani dkk., 2024, hlm. 1).

Singkatnya, upaya untuk meningkatkan MIL sering kali berjalan seiring dengan upaya inklusi yang lebih luas dan menasar berbagai macam khalayak di Indonesia, mulai dari pelaku media hingga anak muda dan komunitas lokal.

## Memahami Dampak

Memahami dampak dalam upaya penanggulangan dan pencegahan daring dapat menjadi tantangan dalam berbagai cara. Namun, para narasumber yang diwawancarai menyoroti model-model yang kuat untuk memahami dampaknya. Ini termasuk:

- **Pengembalian Sosial atas Investasi** - “cara sistematis untuk memasukkan nilai-nilai sosial, lingkungan, ekonomi, dan nilai-nilai lainnya ke dalam proses pengambilan keputusan” (BetterEvaluation, n.d.)
- **Memprioritaskan pemantauan dan evaluasi yang berfokus pada hasil** - berfokus pada tingkat ‘hasil’ dalam pemantauan dan evaluasi, yaitu perubahan konkret dalam pengetahuan, keterampilan, sikap atau perilaku yang dapat kita amati sebagai hasil dari program
- **Memanfaatkan metrik Media Sosial** - mempertimbangkan metrik utama seperti jangkauan, kesukaan, keterlibatan, dan juga memverifikasinya dengan penelitian tambahan untuk menyelidiki pemahaman dan dampak di antara para audiens dan Net Promoter Scores (NPS) - “alat survei yang cepat dan efektif untuk mengevaluasi pelatihan, lokakarya, layanan, komunikasi, atau kegiatan lain dari sebuah organisasi” (CIVICUS, n.d.)

Meskipun daftar ini tidak lengkap, daftar ini merupakan indikasi kuat adanya upaya positif dan terpadu untuk memahami dampak dari melawan dan mencegah ekstremisme dan ekstremisme kekerasan di dunia maya.

## Mekanisme Koordinasi & Pembagian Informasi Lintas Sektor

Wawancara secara konsisten menekankan nilai yang sangat besar dari kerja sama, koordinasi, kolaborasi, dan mekanisme berbagi informasi, baik lintas sektoral maupun di dalam pemerintahan. Seiring dengan bertambahnya jumlah OMS yang terlibat dalam upaya kontra ekstremisme dan ekstremisme kekerasan (IND1), kebutuhan ini hanya akan meningkat.



Berbagai inisiatif disoroti karena kontribusi positif mereka terhadap koordinasi, kolaborasi, dan kerja sama meskipun masih ada kebutuhan. ‘Pusat pengetahuan komunitas’ yang didukung oleh AIPJ dan dipimpin oleh PeaceGen serta platform seperti I-KHub dan WGWC sering disebutkan oleh para narasumber. Keterlibatan positif dengan media sosial dan perusahaan teknologi, yang memfasilitasi moderasi konten, juga disoroti oleh para narasumber yang berbicara tentang keterlibatan Meta dan Google secara positif (IND2) dan mencatat portal penegakan hukum yang memungkinkan permintaan data yang lebih mudah (IND5). Demikian pula, penelitian menyoroti kantor permanen Meta di Indonesia, penyertaan Google di Indonesia sebagai ‘pemberi sinyal tepercaya’ pertamanya, dan saluran komunikasi yang telah dibangun antara X (sebelumnya Twitter) dan Telegram dengan pemerintah Indonesia (IPAC, 2018, hlm. 5). Penelitian dari Royal United Services Institute (RUSI) mencatat bahwa

*“Indonesia lebih maju [...] dalam hal membina hubungan dengan platform teknologi, yang telah menghasilkan beberapa keberhasilan dalam membendung aliran propaganda ekstremis secara daring [sementara tekanan pada platform membantu pemerintah Indonesia mencapai tujuan keamanan. [Intervensi Indonesia terhadap Telegram juga membantu mengguncang sektor teknologi dari kelambanannya. Ini merupakan peringatan bagi platform besar lainnya seperti Facebook, yang telah dikritik oleh pemerintah Indonesia karena bersikeras untuk mematuhi standar komunitasnya sendiri daripada hukum nasional” (Nuraniyah, 2019, hlm.14).*

Meskipun hanya ada sedikit platform media sosial yang dimiliki atau berbasis di dalam negeri, meskipun platform e-commerce Gojek yang masif merupakan kisah sukses lokal, beberapa di antaranya dicirikan sangat kooperatif (IND2). Masyarakat sipil yang diwawancarai juga menandai kegunaan pendekatan seperti ‘mitra ahli’ TikTok yang telah terverifikasi (termasuk organisasi riset lokal seperti Wahid Foundation) yang dapat diminta untuk memberikan rekomendasi, masukan, dan konteks yang berkaitan dengan konten ekstremisme (IND1) untuk memperkuat dan mengontekstualisasikan pendekatan moderasi konten.

### 3.3.2. Tantangan, Kebutuhan, dan Pelajaran Utama

Sejauh ini, Bagian ini telah menguraikan tanggapan yang ada dan berfokus pada upaya, intervensi, dan pendekatan yang disorot oleh literatur dan penelitian primer sebagai efektif atau berguna dalam konteks Indonesia. Namun demikian, Laporan ini juga berupaya mengidentifikasi tantangan, kebutuhan, dan pembelajaran, untuk mempertimbangkan di mana dukungan, sumber daya, dan solusi yang diperlukan menurut pandangan para ahli dan praktisi garis depan yang relevan. Banyak pihak yang diwawancarai, terlepas dari peran dan organisasi mereka, menyoroti perlunya peningkatan kapasitas untuk menanggapi tantangan yang terus berkembang dan memastikan bahwa tanggapan yang diberikan dapat sesuai dengan skala tantangan, di seluruh area isu yang ada.

#### Mengidentifikasi dan Mengatasi Tantangan Kerja Sama, Koordinasi & Kolaborasi

Seperti yang telah disebutkan sebelumnya, para narasumber yang diwawancarai secara konsisten menekankan pentingnya kerja sama, koordinasi, kolaborasi, dan mekanisme berbagi informasi, baik lintas sektoral maupun di dalam pemerintahan. Banyak yang melihat berbagai perkembangan positif dan upaya yang sudah ada dalam hal ini (lihat 3.1.5. di atas), tetapi kebutuhan akan upaya lebih lanjut dan penekanan yang berkelanjutan juga sering dicatat. Sebagai contoh, membangun kolaborasi yang lebih baik antara LSM, OMS dan pemerintah, keterlibatan di tingkat lokal, pendekatan dari bawah ke atas, dan pendekatan kolaboratif yang seimbang dengan kepemimpinan yang kuat telah diterima dengan baik.

Namun, sejumlah tantangan juga diidentifikasi oleh para narasumber dan literatur. Misalnya, meskipun banyak yang memuji RAN PE karena telah membuat kemajuan positif, beberapa aktor merasa bahwa mereka belum melihat dampak besar terhadap moderasi daring (IND13) atau bahwa masih terlalu dini untuk melihat dampak yang lebih luas dari RAN PE (IND24). Tantangan yang dicatat termasuk tidak efektifnya implementasi tujuan RAN PE secara efektif di tingkat lokal - banyak aktor akar rumput, menurut narasumber, masih menganggap terorisme dan ekstremisme sebagai masalah ‘pemerintah pusat’. Akibatnya, para aktor lokal mungkin merasa tidak siap untuk melakukan intervensi ketika masalah ini muncul di tingkat lokal. Efektivitas RAN PE dapat ditingkatkan dengan melanjutkan kepekaan, pelibatan, dan peningkatan kapasitas di tingkat lokal (IND12). Pihak-pihak lain sepakat bahwa meskipun RAN PE telah menjadi kekuatan positif, masih ada kebutuhan untuk menerjemahkan dampaknya ke tingkat lokal, dan masih ada tantangan dalam hal koordinasi, pendanaan, dan pelibatan pemangku kepentingan (IND10).



## Tantangan & Peluang Komunikasi Strategis Utama: Menjangkau Audiens Kunci, Melibatkan Offline

Meskipun ada berbagai pendekatan komunikasi strategis yang sukses dan canggih yang disoroti oleh para narasumber yang berpartisipasi dalam penelitian ini (dan literatur tentang topik ini), berbagai tantangan tetap ada. Konteksnya terus berkembang, dan upaya komunikasi strategis juga harus bergulat dengan perubahan lanskap ekstremisme dan ekstremisme kekerasan - seperti tren narasi berbahaya atau kekerasan yang bergeser ke ruang yang lebih tidak umum, seperti yang dilaporkan dalam konteks Indonesia dan tren umum dalam konteks lain juga, dengan banyak penyampai pesan ekstremis yang berpindah dari forum publik seperti Facebook ke grup WhatsApp pribadi atau ruang tertutup dan terenkripsi lainnya (IND24).

Upaya komunikasi strategis juga memiliki risiko - misalnya, satu kampanye daring pada tahun 2019 menemukan jangkauan dan daya tarik perhatian yang sangat tinggi, tetapi evaluasi tidak dapat mengonfirmasi efek signifikan terhadap sikap dan bahkan mencatat bahwa mungkin ada efek bumerang (Bodine-Baron et al., 2020). Ini bukan tantangan yang tidak biasa dan merupakan area yang perlu diwaspadai - meskipun upaya komunikasi strategis seperti narasi tandingan atau alternatif dapat menjadi alat yang berguna dalam upaya pencegahan dan penanggulangan ekstremisme dan ekstremisme kekerasan yang lebih luas, investasi yang berlebihan pada pendekatan ini dapat berisiko karena bukti mengenai dampaknya masih beragam (lihat misalnya de Carvalho, 2023; Tio & Kruber, 2022; Alava dkk., 2017). Demikian pula, penelitian telah mengindikasikan bahwa hubungan antara narasi ekstremis dan kekerasan ekstremis dengan radikalisme dan rekrutmen semakin kompleks (lihat misalnya: Newton et al., 2021; Nuraniyah, 2019). Lebih lanjut, penelitian telah menimbulkan pertanyaan tentang efektivitas lembaga media daring Muslim moderat dalam menangani konten ekstremis digital, karena beberapa alasan, antara lain keterbatasan dana dan tantangan budaya (Suryana, 2023), dan mencatat bahwa OMS dalam beberapa kasus telah menjadi pembuat narasi tandingan yang sangat efektif, namun mereka juga sering kali melewatkan khalayak yang lebih muda yang rentan terhadap radikalisme dan tidak selalu mahir dalam memilih platform atau mengevaluasi dampaknya (Ismail, 2024). Banyak dari risiko dan tantangan ini dapat diatasi dengan penyesuaian dan kontekstualisasi yang cermat dan memanfaatkan berbagai pendekatan yang saling melengkapi, tetapi penting untuk dipertimbangkan.

## Hambatan dalam Literasi Media & Informasi

Para narasumber juga mencatat bahwa meskipun ada beberapa inisiatif yang baik, upaya-upaya yang dilakukan oleh MIL sebagian besar tidak cukup komprehensif untuk menyamai skala penyebaran konten di media sosial (IND15). Hal ini sangat relevan dengan penelitian yang mencatat kurangnya literasi digital dan tingkat kerentanan yang tinggi terhadap misinformasi dalam konteks Indonesia (Yani, 2021; Paterson, 2019; Facciani et al., 2024). Dengan berbagai bentuk misinformasi yang meningkat di dunia maya, mulai dari yang berkaitan dengan politik hingga kesehatan dan keuangan (McRae et al., 2022; Mujani & Kuipers, 2020; Nasir & Nurmansyah, 2020), hal ini menjadi perhatian utama. Penelitian terbaru juga menyoroti terbatasnya kemampuan mahasiswa di Indonesia dalam membedakan berita palsu dan faktual (Syam & Nurrahmi, 2020) dan meluasnya praktik membagikan konten tanpa membacanya (McDonnell & MacKinnon, 2020). Penelitian juga menunjukkan adanya ketegangan antara menciptakan keterlibatan langsung secara tatap muka, tetapi secara umum mengurangi jangkauan, dengan melakukan keterlibatan secara luring (Ummah & Al Fajri, 2020), yang menyoroti pentingnya pendekatan luring dan daring yang saling melengkapi untuk membangun kapasitas MIL.

## Gender, Inklusi, & Toleransi

Meskipun isu-isu gender, inklusi, dan toleransi merupakan isu lintas sektor yang penting dalam pencegahan dan penanggulangan ekstremisme online, dan karenanya dibahas secara menyeluruh di berbagai bagian laporan ini, penting juga untuk secara khusus menyoroti peran mereka dalam respons yang ada serta respons potensial. Banyak pihak yang diwawancarai, terutama yang berafiliasi dengan OMS yang menangani masalah ini, menekankan perlunya upaya berkelanjutan untuk tidak hanya membuat upaya pencegahan dan penanggulangan ekstremisme dan ekstremisme kekerasan menjadi lebih inklusif, tetapi juga memastikan bahwa dimensi gender ekstremisme dan ekstremisme kekerasan dilibatkan secara efektif. Seperti yang telah lama ditegaskan dalam berbagai literatur (Johnston et al., 2020), dan juga ditegaskan oleh para narasumber yang diwawancarai, ekstremisme dan ekstremisme kekerasan adalah fenomena gender. Kelompok ekstremis dan ekstremis kekerasan menggunakan peran dan norma gender dalam radikalisme, perekrutan, dan operasi mereka. Mereka mahir dalam membuat narasi yang ditargetkan untuk laki-laki dan perempuan yang melibatkan pengalaman gender mereka. Upaya pencegahan dan penanggulangan ekstremisme dan ekstremisme kekerasan harus melakukan hal yang sama, tidak hanya agar inklusif, tetapi juga efektif. Seperti yang telah disebutkan sebelumnya, penelitian dari tahun 2023 menunjukkan sedikit penurunan intoleransi di Indonesia, tetapi juga mencatat adanya marjinalisasi dan stigma yang sedang



berlangsung terhadap beberapa kelompok sosial, dan hak-hak perempuan yang masih “tidak populer” di kalangan masyarakat yang disurvei (Halida dkk., 2023). Penelitian yang mempertimbangkan hubungan antara gender dan ekstremisme kekerasan di kawasan ini, termasuk Indonesia, menunjukkan relevansi kekhawatiran ini, dengan menemukan “korelasi positif dan signifikan” antara dukungan terhadap ekstremisme kekerasan dan dukungan terhadap kekerasan terhadap perempuan (Johnston et al., 2020). OMS yang diwawancarai dalam penelitian ini menekankan sejumlah kebutuhan utama, termasuk kebutuhan akan pelaporan yang aman terhadap kelompok minoritas yang rentan (IND24); mengarusutamakan gender dalam program dan kebijakan pencegahan (IND14); dan menciptakan pesan yang kontekstual dan tidak konfrontatif untuk mengenalkan isu-isu terkait gender (misalnya, dengan menggunakan istilah kesalingan (yang diterjemahkan secara beragam sebagai ‘timbang-balik’, atau ‘timbang balik’), bukan ‘kesetaraan gender’) (IND14).

Literatur menyoroti bahwa kebutuhan akan upaya-upaya ini sangat mendesak. Para ekstremis menggunakan propaganda dan pesan daring untuk mendukung pandangan misoginis dan permusuhan terhadap perempuan (Phelan et al., 2022) dan secara eksplisit menjangkau perempuan berdasarkan motivasi mereka yang berbeda (Johnston et al., 2020). Norma gender masih tetap kaku dan tidak setara dalam konteks Indonesia (ibid). Kelompok-kelompok ekstremis dan ekstremis dengan kekerasan terus secara aktif melibatkan dan menggunakan perempuan yang direkrut untuk menghindari pengawasan (Nuraniyah, 2019) dan memberikan berbagai bentuk dukungan. Media sosial telah memungkinkan perempuan untuk mengakses ruang-ruang yang mungkin hanya dapat diakses oleh laki-laki jika dilakukan secara offline, baik karena anonimitas (Curtis, 2020) atau kurangnya pembatasan fisik terhadap pergerakan atau ruang, yang dimanfaatkan oleh kelompok-kelompok seperti ISIS untuk melibatkan perempuan sebagai pendukung (Johnston et al., 2020) dan kombatan aktif (Nuraniyah, 2017).

Mengingat hal ini, kebutuhan akan lensa gender menjadi sangat jelas. Namun, penelitian terbaru menunjukkan bahwa diperlukan upaya lebih lanjut - sebuah survei terhadap para ahli lokal, regional, dan nasional di Asia Tenggara (terutama Indonesia, Thailand, dan Filipina) menunjukkan hal tersebut:

*“Hanya 26% peserta yang setuju bahwa kebijakan P/CVE yang ada saat ini secara memadai menangani keyakinan misoginis dan permusuhan yang dianut terhadap perempuan oleh kelompok ekstremis kekerasan. Faktanya, 50% dari responden tidak setuju bahwa kebijakan yang ada saat ini secara memadai menangani keyakinan misoginis dan permusuhan terhadap perempuan, dan 48% yang tidak setuju berasal dari Indonesia” (Phelan et al., 2022, hal. 42).*

Lebih lanjut dikatakan bahwa “kebijakan yang lebih responsif gender dapat mengatasi dimensi spesifik gender dari meningkatnya radikalisme daring dan dampaknya terhadap rekrutmen offline laki-laki dan perempuan terhadap ekstremisme kekerasan” (ibid, hlm.9). Hal ini menyoroti bahwa meskipun ada kemajuan positif, upaya yang berkelanjutan masih diperlukan. Selain itu, literatur mencatat bahwa upaya berkelanjutan untuk mengatasi ketidakseimbangan dalam pasukan keamanan dapat menjadi bagian dari solusi (Curtis, 2020). Kepolisian Indonesia telah melakukan upaya positif dan terpadu untuk meningkatkan perekrutan perempuan, tetapi jumlah keseluruhan perempuan di kepolisian masih rendah (Jones, 2022).

## Kesenjangan Moderasi Konten & Tantangan Koordinasi

Para narasumber yang diwawancarai memberikan perhatian pada pentingnya koordinasi antara aktor penegak hukum tradisional seperti Densus 88 dan BNPT dengan lembaga-lembaga yang memiliki kemampuan teknis di bidang komunikasi seperti Kementerian Komunikasi dan Informatika, atau BSSN (Badan Siber dan Sandi Negara) (IND12). Mereka juga menandai beberapa masalah koordinasi dalam proses berbagi informasi tentang pelaku atau pembawa pesan potensial VE secara daring: misalnya, informasi rahasia sering kali menjadi rintangan untuk berbagi informasi (IND23). Juga ditandai bahwa penghapusan konten masih dapat menghadapi tantangan identifikasi (misalnya, ketika konten akademis yang membahas ekstremisme diklasifikasikan sebagai konten ekstremis) (IND12). Penelitian telah menyoroti bahwa upaya koordinasi antarlembaga dalam merespons konten ekstremis, ekstremis dengan kekerasan, dan teroris masih bisa diperkuat, dengan mencatat contoh-contoh keterbatasan koordinasi seperti kurangnya koordinasi antara proses penetapan teroris (yang dihasilkan oleh sistem peradilan pidana) dengan tata kelola konten daring dan platform digital yang mengakibatkan platform digital kurang terdorong untuk memoderasi atau melaporkan konten tersebut (Wibisono dkk, 2024). Penelitian juga mendorong Indonesia untuk mempertimbangkan efektivitas keseluruhan upaya moderasi di tingkat platform, bukan hanya fokus pada metrik tingkat kepatuhan (IPAC, 2018). Para narasumber yang diwawancarai mencatat tantangan yang lebih luas dari konten berbahaya di internet, dengan menyatakan bahwa - seperti di banyak konteks lainnya - mereka yang bekerja



untuk memoderasi konten di internet sering kali menganggap ekstremisme dan ekstremisme kekerasan hanya sebagai salah satu dari sekian banyak sudut pandang, dan juga mengelola upaya yang lebih luas untuk memoderasi bentuk-bentuk konten berbahaya lainnya (IND20), yang bisa memecah fokus dan membuat upaya-upaya untuk memoderasi secara khusus konten ekstremis, ekstremis kekerasan, atau teroris di internet menjadi semakin sulit.

Tantangan untuk menyeimbangkan hak asasi manusia dengan upaya kontra-ekstremisme juga diangkat - literatur telah memperingatkan bahwa kerangka kerja hukum yang berguna untuk memoderasi konten ekstremis, ekstremis dengan kekerasan, atau teroris secara daring dapat digunakan secara berlebihan dan berakibat pada berkurangnya kebebasan berbicara atau berekspresi (Paterson, 2019). Demikian pula, intelijen yang diperkuat dan pemantauan siber dapat memberikan dampak positif, tetapi garis yang jelas tentang apa yang diizinkan untuk tujuan pencegahan dan apa yang tidak sangat penting (Jones, 2022). Para narasumber juga menekankan tantangan yang sekarang terkenal dalam memoderasi konten yang beragam secara linguistik, terutama ketika dipimpin oleh perusahaan internasional yang sebagian besar berbahasa Inggris dan kemungkinan besar memiliki kapasitas yang terbatas (jika ada) untuk meninjau konten dalam bahasa lokal yang memiliki nuansa (IND5), dan semakin terhambat oleh banyak cara di mana konteks dapat menginformasikan seperti apa konten ekstremis itu.

Tantangan lain yang masih ada termasuk bahwa, meskipun platform media sosial dalam banyak hal telah menjadi mitra yang kooperatif dalam konteks Indonesia, orang-orang yang diwawancarai menemukan bahwa moderasi konten atau penghapusan akun bekerja dengan baik untuk tokoh-tokoh yang “lebih besar” atau tingkat tinggi, namun kurang berhasil untuk mereka yang kurang dikenal atau kurang memiliki posisi di organisasi-organisasi tersebut (IND1). Lebih lanjut, “pemblokiran situs web dan akun media sosial sangat bergantung pada kepatuhan penyedia layanan internet (ISP) dan penyedia platform” (Wibisono et al., 2025, hlm. 153). Indonesia, dengan jumlah penduduk yang besar dan penetrasi internet yang tinggi juga sangat terpapar dengan tantangan global di bidang ini - seperti, misalnya, banyak platform game dan platform yang berdekatan dengan game yang “melakukan sedikit atau bahkan tidak melakukan upaya untuk memoderasi konten ekstremis karena tidak berada di bawah pengawasan yang sama dengan platform media sosial (Lamphere-Englund & White, 2023, hlm.20) dan “obrolan di dalam game sering kali tidak terlalu dimoderasi dibandingkan dengan platform media sosial lain dan aplikasi perpesanan yang tidak dikenali” (ibid, hlm.19).

### **Teknologi Baru dan yang Sedang Berkembang - AI untuk Kontra Terorisme?**

Meskipun teknologi baru seperti kecerdasan buatan (AI) generatif memiliki manfaat yang menjanjikan untuk penegakan hukum, teknologi ini memiliki banyak tantangan hukum dan politik (masalah hak asasi manusia, diterimanya bukti yang dihasilkan oleh AI di pengadilan), tantangan teknis (positif/negatif palsu, bias, kemampuan menjelaskan, kompleksitas konten yang dibuat oleh manusia), dan “bukan solusi yang cepat dan mudah” (UNICRI & UNCCT, 2021). Penelitian telah mencatat hal itu:

*“Tantangan yang terkait dengan operasi dan kapasitas dalam penegakan hukum dan lembaga kontraterorisme berarti penggunaan AI telah dilihat sebagai cawan suci dalam memerangi ekstremisme kekerasan. Kapasitas AI untuk memproses data dalam jumlah besar dengan lebih cepat dan lebih mudah, serta untuk menghubungkan data tersebut dan menemukan pola dan tema, berarti badan-badan intelijen melihatnya sebagai komoditas yang menarik untuk menghadapi masalah dalam mengelola informasi yang berlebihan” (Wan Rosli, 2024, hlm. 48).*

Namun, penting untuk dicatat bahwa AI juga memiliki keterbatasan (seperti model moderasi konten yang berjuang dengan ‘jargon’ teroris, ironi dan humor, dan bahasa minoritas (UNICRI & UNCCT, 2021) dan menimbulkan risiko serta peluang. Respons yang terinformasi dan ‘berukuran tepat’ tidak hanya akan memanfaatkan potensi AI untuk meningkatkan moderasi konten, mengembangkan narasi tandingan, dan meningkatkan intervensi, tetapi juga perlu bergulat dengan dampaknya terhadap media dan lingkungan informasi melalui pendekatan MIL yang diperbarui, memperkuat upaya antimisinformasi dan disinformasi, dan melanjutkan pendidikan bukan hanya bagi siswa dan praktisi tetapi juga seluruh lapisan masyarakat, selain upaya-upaya lainnya (Craanen et al., 2025).



## 4. REKOMENDASI

## 4. Rekomendasi

Laporan Negara ini berupaya memberikan rekomendasi yang dapat ditindaklanjuti yang dapat digunakan untuk mengembangkan pembelajaran berdasarkan temuan dari literatur dan masukan praktisi, untuk memfokuskan upaya di masa depan, memenuhi kebutuhan utama, dan memanfaatkan kapasitas yang ada. Harap diperhatikan bahwa untuk setiap rekomendasi dijelaskan secara lebih rinci, disertai tindakan konkret yang dapat berkontribusi secara nyata terhadap upaya tersebut. Rekomendasi ini tidak dimaksudkan untuk menjadi daftar yang lengkap, melainkan untuk memberikan panduan yang lebih konkret guna mendukung implementasi.

Rekomendasi-rekomendasi tersebut meliputi:

### **Terus mengembangkan dan mendukung kapasitas komunikasi strategis bagi masyarakat sipil, tokoh lokal yang berpengaruh, dan aktor masyarakat lainnya**

Upaya komunikasi strategis merupakan pilar utama dalam upaya menanggapi konten, narasi, serta propaganda ekstremis dan kekerasan ekstremis di ruang daring. Terus mengembangkan kapasitas dan dukungan - melalui penyediaan bantuan teknis, sumber daya, atau pendanaan - organisasi lokal dan pemangku kepentingan pemerintah untuk menciptakan narasi tandingan yang efektif, dan yang terpenting, narasi alternatif dan positif, akan menjadi komponen penting dalam mendukung ekosistem informasi daring yang sehat dan menumbuhkan ketahanan digital. Selain itu, upaya-upaya ini harus merespons pendekatan multisaluran dan spesifik untuk setiap platform yang digunakan oleh teroris dan ekstremis dengan menemui audiens di tempat mereka daring.

Rekomendasi Spesifik	Tindakan Potensial/ Contoh
Kumpulkan dan tinjau kembali bukti-bukti mengenai apa yang berhasil di tingkat lokal (dengan berinvestasi dalam penelitian, pemantauan dan evaluasi) untuk berbagai kelompok, dengan menekankan narasi positif atau alternatif, dan latihlah para aktor lokal jika diperlukan mengenai strategi yang efektif.	<ul style="list-style-type: none"><li>• Mendukung atau mendanai organisasi yang melaksanakan intervensi komunikasi strategis untuk melakukan analisis mendalam terhadap audiens sasaran dan evaluasi dampak kampanye mereka.</li><li>• Melatih aktor lokal dan komunitas dalam komunikasi strategis yang efektif untuk meningkatkan ketahanan komunitas terhadap narasi ekstremis.</li><li>• Memprioritaskan kampanye narasi alternatif atau positif daripada berusaha melawan narasi yang sudah ada — misalnya, fokus pada kampanye untuk membangun ketahanan daripada berusaha mendiskreditkan atau membantah narasi ekstremis.</li></ul>
Pertimbangkan pendekatan komunikasi strategis yang kreatif dengan penekanan yang lebih besar pada penceritaan (storytelling), termasuk narasi yang beragam. Selain itu, prioritaskan keterlibatan melalui saluran yang berbeda untuk bertemu dengan audiens di tempat mereka berada - misalnya melalui influencer di dunia game, atau di TikTok, jika relevan. Fokus pada peningkatan kesadaran di kalangan pengguna daring tentang taktik ekstremis yang ada, untuk membantu mencegah orang menjadi mangsa disinformasi serta taktik perekrutan.	<ul style="list-style-type: none"><li>• Melakukan riset dan analisis untuk memahami audiens dan cara terbaik untuk menjangkau mereka sebelum mengembangkan kampanye.</li><li>• Mempertimbangkan bagaimana format baru dapat dimanfaatkan secara autentik untuk menceritakan kisah yang dapat mendorong pemikiran kritis, toleransi, dan keterbukaan pikiran.</li><li>• Bekerja sama dengan pihak-pihak yang berwenang dalam bidang teknologi, praktisi pemerintah, dan praktisi komunikasi strategis untuk mengembangkan cara baru dalam meningkatkan kesadaran tentang taktik perekrutan dan disinformasi di tempat-tempat di mana hal tersebut terjadi.</li></ul>
Libatkan kaum muda sebagai aktor kunci dalam pengembangan dan penyampaian pesan; selain itu, pastikan kelompok-kelompok yang terpinggirkan atau minoritas dilibatkan untuk memastikan upaya komunikasi strategis bersifat inklusif dan efektif.	<ul style="list-style-type: none"><li>• Mengembangkan kampanye atau intervensi melalui proses co-design yang melibatkan pihak-pihak dari kelompok marjinal atau rentan.</li><li>• Melakukan penilaian risiko dengan mempertimbangkan kerentanan khusus kelompok marjinal untuk memastikan bahwa pendekatan komunikasi strategis tidak semakin meminggirkan atau menstigmatisasi.</li></ul>

## Memperkuat kapasitas untuk mengidentifikasi tren, menghasilkan bukti, dan memantau narasi dan aktivitas daring di antara para praktisi

Rekomendasi Spesifik	Tindakan Potensial/ Contoh
Kapasitas teknis penggunaan platform digital untuk penelitian dan pemantauan naratif, terutama dalam bahasa lokal (seperti Bahasa Indonesia atau bahasa daerah lainnya) harus menjadi fokus dalam upaya peningkatan kapasitas.	<ul style="list-style-type: none"> <li>• Mendanai pelatihan bagi praktisi lokal dan menyediakan alat yang diperlukan untuk melakukan pemantauan digital dalam bahasa lokal. Hal ini dapat mencakup workshop peningkatan kapasitas tentang analisis media sosial dan penggunaan teknologi dan alat baru yang disesuaikan dengan konteks dan bahasa lokal.</li> <li>• Bekerja sama dengan universitas lokal dan mitra teknologi untuk mengembangkan perpustakaan kata kunci yang spesifik bahasa, yang akan membantu dalam deteksi konten sesuai dengan karakteristik lokal.</li> </ul>
Ringkasan penelitian terbaru yang tepat waktu tentang narasi teroris, ekstremis kekerasan dan ekstremis, aktivitas daring, dan tren saat ini diperlukan untuk menginformasikan tanggapan yang disesuaikan.	<ul style="list-style-type: none"> <li>• Membentuk mekanisme untuk pengembangan penelitian dan analisis yang tepat waktu mengenai tren baru guna menjaga kesadaran dan respons yang terkini terhadap tren dan perkembangan.</li> <li>• Mendukung dan memanfaatkan platform yang sudah ada yang melakukan jenis penelitian ini, seperti Indonesia Knowledge Hub (I-KHub), pusat pengetahuan Indonesia untuk penanggulangan terorisme dan ekstremisme kekerasan. Memastikan penelitian didasarkan pada informasi lokal dan selaras dengan tren terkini, serta dibagikan kepada pemangku kepentingan terkait untuk memastikan respons yang kolaboratif dan terpadu terhadap ekstremisme, ekstremisme kekerasan, dan terorisme.</li> </ul>
Pembelajaran yang berkelanjutan untuk memahami, dan untuk secara efektif memanfaatkan atau mengendalikan dengan baik teknologi terbaru, diperlukan untuk membantu para praktisi mengikuti lanskap digital yang terus berkembang. Para praktisi garis depan mencatat perlunya belajar memanfaatkan teknologi dan tren baru untuk pekerjaan mereka. Sistem peringatan dini untuk ancaman daring masih diperlukan untuk memfasilitasi tindakan proaktif atau pencegahan, yang membutuhkan upaya pemantauan dan mekanisme berbagi informasi.	<ul style="list-style-type: none"> <li>• Mengembangkan dan menerapkan pelatihan peningkatan kapasitas tentang teknologi baru (seperti kecerdasan buatan, amplifikasi algoritmik), serta analisis tren digital.</li> <li>• Membentuk jaringan berbagi informasi untuk mendukung upaya yang tepat waktu dan mencegah duplikasi upaya.</li> <li>• Berinteraksi dengan sektor teknologi serta sektor terkait lainnya untuk memastikan para praktisi sadar dan terinformasi tentang lingkungan digital yang berkembang pesat.</li> </ul>
Pemantauan yang ketat terhadap tren seputar penggunaan E2EE, AI generatif, dan kekhawatiran mengenai potensi eksploitasi ekstremis terhadap layanan dan teknologi keuangan digital, untuk memastikan kebijakan dan pemrograman dapat mengimbangi teknologi baru dan tren daring.	<ul style="list-style-type: none"> <li>• Secara berkala meninjau dan menyesuaikan strategi berdasarkan tren yang muncul dan berkembang di ruang digital untuk memastikan respons yang efektif dan relevan terhadap eksploitasi ruang online oleh kelompok ekstremis dan ekstremis kekerasan, sambil tetap menjaga privasi digital, keamanan, dan hak asasi manusia.</li> </ul>



**Bekerja sama dengan sektor swasta dan perusahaan teknologi untuk memanfaatkan potensi positif AI, termasuk upaya-upaya seperti mendukung pengembangan model pelatihan AI yang dapat memantau aktivitas dan wacana ekstremis, ekstremis dengan kekerasan, dan teroris di berbagai platform secara etis dan efektif, serta dalam bahasa lokal**

Seperti yang dicatat dalam Laporan Negara ini, meskipun AI dan teknologi baru lainnya menghadirkan ancaman, teknologi ini juga menawarkan peluang bagi para praktisi kontra ekstremisme untuk tidak hanya mengimbangi eksploitasi teroris dan ekstremis, tetapi juga memanfaatkannya dengan cara-cara baru dan inovatif. Potensi AI untuk moderasi konten dan mengurangi bahaya bagi moderator manusia telah diidentifikasi; demikian pula potensinya untuk mendukung analisis kebutuhan dan tren, serta pengembangan narasi kontra atau alternatif yang ditargetkan dalam skala besar, adalah beberapa di antara banyak kemungkinan.

Rekomendasi Spesifik	Tindakan Potensial/ Contoh
Kerja sama dengan sektor swasta dan perusahaan teknologi untuk memanfaatkan berbagai bentuk keahlian yang relevan dan menciptakan kolaborasi untuk upaya pencegahan dan penanggulangan ekstremisme.	<ul style="list-style-type: none"> <li>Membangun kemitraan kerja yang terstruktur dengan sektor swasta dan teknologi melalui pembentukan kelompok kerja atau pertemuan rutin serupa, untuk memanfaatkan keahlian yang relevan, membangun hubungan, dan mengembangkan bersama alat-alat untuk memantau dan memoderasi konten daring.</li> </ul>
Pastikan bahwa penggunaan teknologi baru untuk pencegahan dan penanggulangan diinformasikan oleh pendekatan yang tidak membahayakan, kontekstual, dan berdasarkan pembelajaran yang dipetik dan praktik-praktik yang baik dari bidang kontra ekstremisme dan ekstremisme kekerasan dalam beberapa dekade terakhir.	<ul style="list-style-type: none"> <li>Mengadopsi pendekatan yang spesifik konteks dan sensitif dalam penggunaan alat teknologi dalam upaya pencegahan dan penanggulangan ekstremisme – misalnya, bekerja sama dengan sektor teknologi untuk melatih model pada bahasa lokal dan dinamika budaya yang spesifik terkait ekstremisme.</li> <li>Menerapkan pertimbangan etis berdasarkan realitas lokal dan pelajaran yang dipetik untuk menghindari konsekuensi yang tidak diinginkan seperti stigmatisasi, sekuritisasi, profiling, dan alienasi komunitas, berdasarkan kelompok marjinal tertentu dalam konteks ini.</li> <li>Mengembangkan mekanisme tinjauan formal atau kelompok penasihat ahli untuk memastikan pengawasan, pengembangan yang aman dan etis, serta penyesuaian konteks yang tepat dalam desain atau implementasi program yang memanfaatkan alat kecerdasan buatan (AI).</li> </ul>
Pertimbangkan cara penggunaan kecerdasan buatan (AI) secara etis dan aman untuk upaya komunikasi strategis berskala besar dan/atau tertarget, seperti gangguan narasi, termasuk pendekatan seperti memanfaatkan pemrosesan bahasa alami (NLP) untuk mendeteksi bahasa ekstremis yang tersembunyi dan pola pesan tersandi.	<ul style="list-style-type: none"> <li>Melanjutkan penelitian tentang cara penerapan alat kecerdasan buatan (AI) untuk mendeteksi narasi ekstremis online sambil memastikan perlindungan yang kuat terhadap privasi, akurasi, dan pencegahan bias dalam konteks lingkungan regulasi Indonesia dan lanskap ekstremisme online.</li> <li>Mendorong pengawasan manusia dalam sistem AI yang digunakan dalam upaya kontra ekstremisme untuk memastikan penggunaan AI yang bertanggung jawab dan etis.</li> </ul>

**Membangun mekanisme koordinasi dan kolaborasi yang sudah ada untuk menciptakan dan/atau memperkuat jaringan berbagi informasi formal dan informal.**

Meskipun RAN PE telah membuat langkah besar dalam menciptakan keterlibatan yang lebih holistik dengan berbagai aktor yang lebih luas untuk mencapai hasil pencegahan, keterlibatan di tingkat masyarakat membutuhkan upaya berkelanjutan untuk memastikan kebijakan dan program yang efektif dapat menjangkau secara luas. Memprioritaskan dialog dan berbagi informasi adalah kunci untuk memfasilitasi keterlibatan tersebut. Para pemangku kepentingan

pemerintah menekankan peluang untuk meningkatkan atau memperkuat pembagian informasi formal di seluruh pemerintahan untuk berkomunikasi mengenai ancaman yang muncul secara lebih efektif.

Rekomendasi Spesifik	Tindakan Potensial/ Contoh
Memperkuat berbagi informasi dan keterlibatan dengan sektor teknologi dan khususnya, para pelaku kepercayaan dan keamanan, harus menjadi tujuan yang berkelanjutan untuk mendukung moderasi konten, tetapi juga untuk membantu mengidentifikasi tren dan mendiagnosis kebutuhan respons.	<ul style="list-style-type: none"> <li>• Meningkatkan mekanisme berbagi informasi antar pemangku kepentingan untuk memfasilitasi keterlibatan dan pertukaran pengetahuan antara pemerintah, sektor teknologi, akademisi, dan masyarakat sipil, guna memastikan peringatan dini dan koordinasi tanggapan terhadap ancaman yang muncul di ruang digital.</li> <li>• Membangun kerangka kerja cepat tanggap yang dapat membantu memberikan tanggapan tepat waktu terhadap ancaman yang muncul melalui berbagi data anonim dan pengembangan bersama alat mitigasi dan strategi.</li> </ul>
Secara umum, jika memungkinkan, upaya untuk melanjutkan, memperkuat, atau meningkatkan kolaborasi dan koordinasi lintas sektor, tingkat pemerintahan, dan antara berbagai aktor mulai dari pemerintah hingga masyarakat sipil, media, dan teknologi, harus tetap menjadi prioritas dalam rangka mendukung pencegahan dan penanggulangan ekstremisme daring yang efektif.	<ul style="list-style-type: none"> <li>• Mendorong kolaborasi lintas sektor dengan memperkuat dan berkomitmen pada kerangka kerja dan mekanisme koordinasi yang menghubungkan aktor nasional, lokal, dan sektoral.</li> <li>• Mendorong penyelenggaraan sesi perencanaan bersama secara rutin, dialog lintas sektor, dan pertukaran informasi untuk upaya pencegahan.</li> </ul>

**Sesuaikan intervensi media dan literasi informasi dengan kebutuhan audiens target (dalam hal penggunaan bahasa, keterlibatan platform, dll.) dan fokus pada upaya jangka panjang dan berkelanjutan yang menyediakan pelatihan, pendampingan, dan dukungan.**

Upaya-upaya literasi media dan informasi (MIL) yang dilakukan oleh berbagai pemangku kepentingan memiliki potensi untuk memasukkan, dan berdampak positif, pada berbagai bidang. Hal ini dapat mencakup:

Rekomendasi Spesifik	Tindakan Potensial/ Contoh
Pertimbangkan literasi dan perlindungan AI sebagai bagian dari pencegahan dan peningkatan kesadaran. Menerapkan MIL di lingkungan daring yang berbeda, seperti ruang game online atau di forum tertutup (seperti platform E2EE).	<ul style="list-style-type: none"> <li>• Mengintegrasikan literasi kecerdasan buatan (AI) dan keamanan digital sebagai bagian dari inisiatif Literasi Media dan Informasi (MIL), dengan konten yang disesuaikan untuk lingkungan digital yang terus berkembang.</li> <li>• Memastikan upaya peningkatan kesadaran mencakup pengembangan keterampilan untuk mengevaluasi secara kritis konten yang dihasilkan oleh AI dan mengenali manipulasi.</li> </ul>
Kembangkan program MIL yang didasarkan pada pemahaman perilaku (misalnya, memanfaatkan skenario online dunia nyata) untuk meningkatkan kemampuan praktis peserta pelatihan.	<ul style="list-style-type: none"> <li>• Memasukkan simulasi, latihan interaktif, dan studi kasus yang spesifik untuk platform – misalnya, yang disesuaikan dengan lingkungan permainan – ke dalam program pelatihan untuk mengembangkan kompetensi praktis dan relevan dengan konteks dalam mengenali dan menanggapi konten berbahaya di ruang daring.</li> </ul>

Hubungkan dengan bahaya yang lebih luas dan terkait seperti penipuan, perjudian, hoax, dan disinformasi.	<ul style="list-style-type: none"> <li>• Memperluas cakupan upaya ketahanan digital untuk mencakup ancaman daring yang saling terhubung, seperti penipuan, perjudian, hoaks, dan disinformasi.</li> <li>• Menerapkan pendekatan holistik dan akui bahwa ancaman dan bahaya lain yang sudah ada dapat berfungsi sebagai pintu masuk atau penguat bagi konten ekstremis dan manipulasi informasi.</li> </ul>
Kembangkan keterampilan bagi para pelaku media untuk melaporkan secara bertanggung jawab tentang terorisme dan ekstremisme kekerasan.	<ul style="list-style-type: none"> <li>• Mengembangkan pelatihan yang ditargetkan bagi jurnalis dan profesional media tentang pelaporan yang bertanggung jawab terkait terorisme, ekstremisme, dan ekstremisme kekerasan. Pelatihan ini dapat mencakup pertimbangan seperti kerangka etika, menghindari sensasionalisme, melindungi individu dan komunitas, serta menangani konten yang berbahaya dan ekstrem tanpa memperkuatnya.</li> <li>• Bekerja sama dengan pemangku kepentingan terkait seperti dewan pers dan universitas untuk mendukung dampak jangka panjang dari upaya semacam ini.</li> </ul>

**Upaya berkelanjutan untuk menerapkan lensa gender dalam mencegah dan melawan ekstremisme dan ekstremisme kekerasan baik secara luring maupun daring diperlukan untuk memastikan bahwa dinamika dan pendorong radikalisasi dan rekrutmen berbasis gender dipahami dan untuk memastikan upaya untuk melibatkan gender yang berbeda melalui pemrograman, narasi alternatif, atau bentuk intervensi lain yang efektif dan peka gender.**

Penelitian yang sedang berlangsung di bidang terorisme, gender, dan pencegahan telah menyoroti hubungan antara gender dan ekstremisme kekerasan, dan terus menunjukkan bahwa gender yang berbeda rentan terhadap ekstremisme dan ekstremisme kekerasan dengan cara yang berbeda, dapat menjalankan peran yang berbeda berdasarkan gender, dan menjadi sasaran yang berbeda oleh organisasi ekstremis atau teroris, di antara dimensi-dimensi gender lainnya dari ekstremisme sebagai sebuah fenomena. Hal ini berlaku juga di ruang daring, di mana faktor tambahan seperti akses yang dipengaruhi gender, literasi terhadap ruang daring, atau teknologi baru mungkin berperan. Oleh karena itu, ada kebutuhan mendesak yang terus berlanjut untuk memastikan bahwa upaya pencegahan dan penanggulangan mempertimbangkan ekstremisme, ekstremisme kekerasan, dan terorisme melalui lensa gender, dan bahwa respons dirancang untuk secara efektif menjangkau dan memengaruhi audiens dari berbagai gender.

Rekomendasi Spesifik	Tindakan Potensial/ Contoh
Lensa gender yang tidak hanya mempertimbangkan jenis kelamin tetapi juga faktor identitas lain seperti usia, agama, budaya, dan lain-lain diperlukan untuk memahami kebutuhan dan merespons secara efektif.	<ul style="list-style-type: none"> <li>• Mengadopsi perspektif gender yang inklusif dalam penelitian dan program untuk memahami dengan lebih baik kebutuhan, kerentanan, dan peran berbagai kelompok dalam kaitannya dengan ekstremisme online.</li> <li>• Meneliti dan menganalisis bagaimana karakteristik tertentu seperti usia, gender, identitas agama, dan latar belakang budaya dapat memengaruhi pengalaman online individu untuk membantu mengembangkan respons yang lebih terarah serta mekanisme perlindungannya.</li> </ul>
Membangun keberhasilan dalam lingkungan kebijakan Indonesia dari agenda Perempuan, Perdamaian, dan Keamanan (WPS), menyelaraskan upaya pencegahan daring dengan kerangka kerja WPS.	<ul style="list-style-type: none"> <li>• Mendorong kepemimpinan perempuan dalam keamanan digital serta peran aktif mereka dalam mencegah ekstremisme online.</li> <li>• Merancang intervensi online yang memperkuat kesetaraan gender dan pembangunan perdamaian berdasarkan kerangka kerja nasional WPS.</li> </ul>



## REFERENSI



- Abdullah, S. D. A., & Alfatra, S. (2019). Narration of Islamic moderation: Counter over negative content on social media. *Millati: Journal Of Islamic Studies And Humanities*, 4(2), 153–165. <https://doi.org/10.18326/mlt.v4i2.153-165>
- Alava, S., Frau-Meigs, D., & Hassan, G. (2017). Youth and violent extremism on social media: Mapping the research. UNESCO. <https://doi.org/10.54675/STTN2091>
- Anuar, M. I. K. (2024, August 6). Indonesia police investigate social media terrorism recruitment after arrest of teen suspect. *Bernama*. <https://www.bernama.com/en/news.php?id=2326037>
- Arshad, A. (2024, November 11). Indonesians join peaceful rally in Jakarta in solidarity with Palestine. *The Straits Times*. <https://www.straitstimes.com/asia/se-asia/indonesians-join-peaceful-rally-in-solidarity-with-palestine>
- ASEAN. (2018). ASEAN plan of action to prevent and counter the rise of radicalization and violent extremism. <https://asean.org/wp-content/uploads/2025/03/ASEAN-Plan-of-Action-to-Prevent-and-Counter-the-Rise-of-Radicalisation-and-Violent-Extremism-2018-2025.pdf>
- Ayuningtiyas, K. (2024, January 4). Experts: Extremist groups spread disinformation online to provoke conflict during Indonesian election. *BenarNews*. <https://www.benarnews.org/english/news/indonesian/extremist-groups-spread-disinformation-to-provoke-conflict-during-poll-01032024150241.html>
- Barbarossa, E. (2024, May 6). The three phases of Terrorgram (ACC Reports). Accelerationism Research Consortium. <https://www.accresearch.org/accreports/the-three-phases-of-terrorgram>
- BetterEvaluation. (n.d). Social return on investment. <https://www.betterevaluation.org/methods-approaches/approaches/social-return-investment>
- Bodine-Baron, E., Marrone, J., V., Helmus, T. C., & Schlang, D. (2020). Countering Violent Extremism in Indonesia: Using an online panel survey to assess a Social Media Counter-Messaging campaign. RAND. [https://www.rand.org/pubs/research\\_reports/RRA233-1.html](https://www.rand.org/pubs/research_reports/RRA233-1.html)
- Bradley, A. (2025). Right- and left-wing violent extremist abuse of digital technologies in South America, Africa and Asia. UNICRI. <https://unicri.org/Publication-Right-Left-Wing-Violent-Extremist-Digital-Technologies-SouthAmerica-Africa-Asia>
- Charities Aid Foundation. (2025). World Giving Index 2025: A global view of giving trends. <https://www.cafonline.org/insights/research/world-giving-index>
- CIVICUS. (n.d.). Net Promoter Score. <https://monitoring-toolkits.civicus.org/toolkit/net-promoter-score/>
- Craanen, A., Allen, E., & Atamuradova, F. (2025, forthcoming). Artificial Intelligence for Counter Extremism: exploring threats, challenges, opportunities and needs for leveraging generative AI in counter extremism. *Hedayah*.
- Curtis, G. (2020). What Indonesia is getting wrong about women and violent extremism. *The Habibie Center*, No. 18. <https://www.habibiecenter.or.id/img/publication/04eff47fc8417409c08ec9432c2b894f.pdf>
- Dawitri, N., & Amara, M. (2023). Indonesia's low digital civility index -Two sides of Indonesia. <https://doi.org/10.13140/RG.2.2.17889.58721>
- de Carvalho, C. M. (2023). Digital counter and alternative messages to extremist content: Effectiveness and way forward. In *Special Issue: Building Digital Resilience In Preventing and Countering Violent Extremism*. SEARCCT'S Selection of Articles 2023. 72-78. <https://www.searcct.gov.my/wp-content/uploads/2024/08/SOA-2023d.pdf>
- Extremism and Gaming Research Network, 2021.
- Facciani, M. J., Apriliawati, D., & Weninger, T. (2024). Playing Gali Fakta inoculates Indonesian participants against false information. *Harvard Kennedy School (HKS) Misinformation Review*, 5 (4). <https://doi.org/10.37016/mr-2020-152>
- Fahmy, S. (2024, January 25). The Gaza War and the danger of extremism. *Carnegie Endowment for International Peace*. <https://carnegieendowment.org/sada/2024/01/the-gaza-war-and-the-danger-of-extremism?lang=en>
- Halida, R., Hanan, D., Prasetyo, H., Lamphere-Englund, G., & Hamonangan, A. (2023). 2022 National Survey Report: Violent extremism, democracy, and religious attitudes in Indonesia. *Lembaga Survei Indonesia (LSI)*. Jakarta, Indonesia. <https://www.lsi.or.id/post/copy-of-violent-extremism-report>

- Harmoni Program. (2023). Violent Extremism and Social Media. Trends in Indonesia: 2018-2023. USAID Harmoni. Jakarta, Indonesia
- Hasbi, A. H. bin M., & Mok, B. (2023). Digital Vacuum: The evolution of IS central's media outreach in Southeast Asia. *Counter Terrorist Trends and Analyses*, 15(4), 1–8. <https://www.jstor.org/stable/48743372>
- Hunter, S., d'Amato, A. L., Elson, J. S., Doctor, A. C., & Linnell, A. (2024). The Metaverse as a future threat landscape: An interdisciplinary perspective. *Perspectives on Terrorism*, 18(2), 100–118. <https://www.jstor.org/stable/27315310>
- Hwang, J. C., & Frank, H. (2024). Jemaah Islamiyah disbands itself: How, why, and what comes next? The Soufan Center. <https://thesoufancenter.org/intelbrief-2024-september-26/>
- IPAC. (2018). Indonesia and the tech giants vs ISIS supporters: Combating violent extremism online. In IPAC: Vol. No. 48. [http://file.understandingconflict.org/file/2018/07/IPAC\\_Report\\_48.pdf](http://file.understandingconflict.org/file/2018/07/IPAC_Report_48.pdf)
- Ismail, N. H. (2022). Countering online radicalisation in Southeast Asia through the 5M framework. RSIS. <https://rsis.edu.sg/rsis-publication/rsis/countering-online-radicalisation-in-southeast-asia-through-the-5m-framework/>
- Ismail, N. H. (2023). Online radicalisation of the Indonesian diaspora. *Counter Terrorist Trends and Analyses*, 15(3), 15–20. <https://www.jstor.org/stable/48732712>
- Ismaizam, M. A. (2023). Malicious use of artificial intelligence by terrorists: Assessing future risks. In Special Issue: Building Digital Resilience In Preventing and Countering Violent Extremism. SEARCCT'S Selection of Articles 2023. 161-165. <https://www.searcct.gov.my/wp-content/uploads/2024/08/SOA-2023d.pdf>
- Jamhari, J. & Testriono, T. (2021). The roots of Indonesia's resilience against violent extremism. *Studia Islamika*, 28(3). <http://dx.doi.org/10.36712/sdi.v28i3.23956>
- Jofre, M., Aziani, A., & Villa, E. (2024). Terrorist financing: Traditional vs. Emerging financial technologies. *Terrorism and Political Violence*, 1–14. <https://doi.org/10.1080/09546553.2024.2433635>
- Johnston, M. F., Iqbal, M., & True, J. (2020). The Lure of (violent) extremism: gender constructs in online recruitment and messaging in Indonesia. *Studies in Conflict and Terrorism*, 46(4), 470–488. <https://doi.org/10.1080/1057610x.2020.1759267>
- Jones, S. (2022). Terrorism and extremism in Indonesia and the Southeast Asian region. *Southeast Asian Affairs*, 162–174. <https://www.jstor.org/stable/27206>
- Kemp, S. (2025, February 25). Digital 2025: Indonesia - DataReportal – global digital insights. DataReportal. <https://datareportal.com/reports/digital-2025-indonesia>
- Kepios and We Are Social. (2025, February). Digital 2025: Indonesia (v. 02) [Report]. We Are Social & Kepios. [https://wearesocial.com/wp-content/uploads/2025/02/Digital\\_2025\\_Indonesia\\_v02.pdf](https://wearesocial.com/wp-content/uploads/2025/02/Digital_2025_Indonesia_v02.pdf)
- Lamphere-Englund & White, J. (2023). The Online Gaming ecosystem: Assessing digital socialisation, extremism risks and harms mitigation efforts. GNET. <https://gnet-research.org/2023/05/26/the-online-gaming-ecosystem/>
- Lamphere-Englund, G. (2025) 2024 Resource List: Violent extremism, radicalization, and gaming. GIFCT. <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-EG-Resources-1.1.pdf>
- Lamphere-Englund, G., White, J., Wallner, C., Newhouse, A., (2025, pending), Building Resilience Against Violent Extremism Digitally: Trialing a new gender-based approach among gamers, *Frontiers in Psychology*.
- Lamphere-Englund, G., Hamonangan, A., and Putri, F. (2022). Pathways of resilience to violent extremism in Indonesian higher education: A mixed method study using the building resilience against violent extremism (BRAVE) Approach. USAID Harmoni. Jakarta, Indonesia. <https://www.crisconsortium.org/research-reports-pathways-to-resilience>
- McDonald, B. (2024). The drones of Hayat Tahrir al-Sham: The development and use of UAS in Syria. GNET. <https://gnet-research.org/2024/12/20/the-drones-of-hayat-tahrir-al-sham-the-development-and-use-of-uas-in-syria/>
- McDonnell, I., & MacKinnon, T. (2020). Case study: Misinformation in Indonesia. GeoPoll. <https://www.geopoll.com/misinformation-indonesia/>

- McRae, D., del Mar Quiroga, M., Russo-Batterham, D., Doyle, K., & Platform, A. (2022). A progovernment disinformation campaign on Indonesian Papua. *Harvard Kennedy School (HKS) Misinformation Review*, 3 (5).  
<https://doi.org/10.37016/mr-2020-108>
- Middle East Media Research Institute. (2024, February 2). Dari-language review: TikTok accounts show widespread use of the platform by Afghan Taliban and Islamic State. MEMRI Jihad and Terrorism Threat Monitor. <https://www.memri.org/jtm/dari-language-review-tiktok-accounts-shows-widespread-use-platform-afghan-taliban-and-islamic>
- Modulate. (2024). Modulate and Activision case study. <https://www.modulate.ai/case-studies/modulate-activision-case-study>
- Mohd Nor, M. W.. (2023) All-of-society approach to address hate speech. In Special Issue: Building Digital Resilience In Preventing and Countering Violent Extremism. SEARCCT'S Selection of Articles 2023. 97-107.  
<https://www.searcct.gov.my/wp-content/uploads/2024/08/SOA-2023d.pdf>
- Mok, B., & Satria, A. (2024). Indonesian terrorists' attempts to interfere with the 2024 Indonesian election. GNET.  
<https://gnet-research.org/2024/02/12/indonesian-terrorists-attempts-to-interfere-with-the-2024-indonesian-election/>
- Monaghan, K., & Rodriguez, C. (2023). Mis-and Disinformation: Extremism in the Digital age. CTPN.  
<https://www.london.gov.uk/sites/default/files/2023-12/CTPN%20Report%202023%20-%20Mis-and%20Disinformation%2C%20Extremism%20in%20the%20Digital%20Age%20%28Single%20Pages%29.pdf>
- Mujani, S., & Kuipers, N. (2020). Who believed misinformation during the 2019 Indonesian election? *Asian Survey*, 60(6), 1029–1043, <https://doi.org/10.1525/as.2020.60.6.1029>
- Nasir, N. M., & Nurmansyah, M. I. (2020). Misinformation related to COVID-19 in Indonesia. Institutional Repository UIN Syarif Hidayatullah. <https://repository.uinjkt.ac.id/dspace/handle/123456789/63519>
- Newton, J. (2024). Staying Alive: The Indonesian pro-IS community's online resilience and the 'Lone Actor' threat in 2025. RSIS. <https://rsis.edu.sg/ctta-newsarticle/staying-alive-the-indonesian-pro-is-communitys-online-resilience-and-the-lone-actor-threat-in-2025/>
- Newton, J., Prasad, H., Moner, Y., & Kyaw, N. N. (2021). Polarising narratives and deepening fault lines: Social media, intolerance and extremism in four Asian nations. GNET. <https://gnet-research.org/2021/03/02/polarising-narratives-and-deepening-fault-lines-social-media-intolerance-and-extremism-in-four-asian-nations/>
- Newzoo. (2025). Global games market report 2024. Newzoo. <https://newzoo.com/insights/trend-reports/newzoo-global-games-market-report-2024-free-version>
- Nuraniyah, N. (2017). 10. Online extremism: the advent of encrypted private chat groups. In E. Jurriens (Ed.), *Digital Indonesia: Connectivity and Divergence* (pp. 163-186). Singapore: ISEAS Publishing.  
<https://doi.org/10.1355/9789814786003-016>
- Nuraniyah, N. (2019). The evolution of online violent extremism in Indonesia and the Philippines. GNET.  
<https://gnet-research.org/wp-content/uploads/2019/12/5.pdf>
- Paterson, T. (2019). Indonesian cyberspace expansion: a double-edged sword. *Journal of Cyber Policy*, 4 (2), 216–234.  
<https://doi.org/10.1080/23738871.2019.1627476>
- Phelan, A., Gayatri, I. H. O., True, J., Marddnt, A., Riveros-Morales, Y., & Gama, S. J. (2021). Gender analysis of violent extremism and the impact of COVID-19 on peace and Security in ASEAN: Evidence-based Research for Policy. UN Women – Asia-Pacific. <https://asiapacific.unwomen.org/en/digital-library/publications/2022/03/gender-analysis-violent-extremism-covid19-peace-and-security-asean>
- Rahman, M. F., Irsyadi, M. M., Ferdiansyah, H., Suma, M. A., & Trinanda, D. (2023). Strategic efforts of Bincangsyariah.com and Islami.co editorials in spreading counter-narrative extremism on the Internet. *Al-Balagh: Jurnal Dakwah Dan Komunikasi*, 8(2), 249 – 282, <https://doi.org/10.22515/albalagh.v8i2.7582>
- Rahman, M. F., Suma, M. A., Ferdiansyah, H., & Irsyadi, M. M. (2021). Kontra narasi ekstremisme online melalui media islam moderat di Indonesia. Lembaga Penelitian dan Pengembangan Masyarakat (LP2M), UIN Syarif Hidayatullah Jakarta.
- Sadeghi, M., & Blachez, I. (2025, March 6). A well-funded Moscow-based global “news” network has infected Western artificial-intelligence tools worldwide with Russian propaganda. NewsGuard's Reality Check.  
<https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global>

- Saiz, G. (2025). Virtual Threats: Terrorist Financing via Online Gaming. RUSI. <https://www.projectcraaft.eu/research-briefings/https://static1.squarespace.com/static/5e399e8c6e9872149fc4a041/t/681ccf124419647df74eb0ac/1746718484160/594-craaft-ii-bp1-terrorist-financingpdf>
- Saltman, E., & Hunt, M. (2023). Insight: Borderline Content: Understanding the gray zone. GIFCT. <https://gifct.org/2023/06/29/borderline-content-understanding-the-gray-zone/>
- Sarwono, J. S. (2024). CaliphateTok: How Islamic State (IS) leverages social media in Indonesia and the Power of Counter-Narratives. GNET. <https://gnet-research.org/2024/11/28/caliphate-tok-how-islamic-state-is-leverages-social-media-in-indonesia-and-the-power-of-counter-narratives/>
- Schlegel, L. (2021). Extremists' use of gaming (adjacent) platforms: Insights regarding primary and secondary prevention measures. EUROPEAN COMMISSION Radicalisation Awareness Network. [https://home-affairs.ec.europa.eu/system/files/2021-08/ran\\_extremists\\_use\\_gaming\\_platforms\\_082021\\_en.pdf](https://home-affairs.ec.europa.eu/system/files/2021-08/ran_extremists_use_gaming_platforms_082021_en.pdf)
- Schmidt, L. (2018). Cyberwarriors and Counterstars: Contesting Religious Radicalism and Violence on Indonesian Social Media. *Asiascape: Digital Asia*, 5(1-2), 32-67. <https://doi.org/10.1163/22142312-12340088>
- Schmidt, L. (2021). Aesthetics of authority: 'Islam Nusantara' and Islamic 'radicalism' in Indonesian film and social media. *Religion*, 51(2), 237-258. <https://doi.org/10.1080/0048721X.2020.18068387>
- Shah, R., Irpan, A., Turner, A. M., Wang, A., Conmy, A., Lindner, D., ... & Dragan, A. (2025). An approach to technical AGI safety and security. arXiv preprint arXiv:2504.01849. <https://arxiv.org/abs/2504.01849>
- Sulaimarl, N. & De Lang, N. E. (2024). Emerging threats and trends of terrorism and violent extremism online. SEARCCT'S Selection of Articles 2024, 21-29. [https://www.searcct.gov.my/wp-content/uploads/2024/12/v4\\_Draft-SOA-2024-Publisher.pdf](https://www.searcct.gov.my/wp-content/uploads/2024/12/v4_Draft-SOA-2024-Publisher.pdf)
- Lamphere-Englund, G., & Thompson, E. (2024). 30 years of trends in terrorist and extremist games. GNET. <https://gnet-research.org/2024/11/01/30-years-of-trends-in-terrorist-and-extremist-games/>
- Sumpter, C. (2024). Decentralising and coordinating P/CVE through the Indonesia Knowledge Hub (I-KHub). *Counter Terrorist Trends and Analyses*, 16(4), 10-16. <https://www.jstor.org/stable/48794705>
- Suryana, A. (2023). Indonesia's moderate Muslim websites and their fight against online Islamic extremism. ISEAS – Yusof Ishak Institute. [https://www.iseas.edu.sg/wp-content/uploads/2023/09/TRS15\\_23.pdf](https://www.iseas.edu.sg/wp-content/uploads/2023/09/TRS15_23.pdf)
- Syam, H. M., & Nurrahmi, F. (2020). "I don't know if it is fake or real news": How little Indonesian University students understand social media literacy. *Jurnal Komunikasi: Malaysian Journal of Communication*, 36(2), 92-105. <https://doi.org/10.17576/JKMJC-2020-3602-06>
- Tio, R. & Kruber, S. (2022). Online P/CVE Social Media Efforts. In G. Barton, M. Vergani, & Y. Wahid (Eds.), *Countering Violent and Hateful Extremism in Indonesia. Islam, Gender and Civil Society* (pp. 233-254). Palgrave Macmillan. [https://doi.org/10.1007/978-981-16-2032-4\\_11](https://doi.org/10.1007/978-981-16-2032-4_11)
- Ummah, N. H., & Fajri, M. S. A. (2020). Communication strategies used in teaching Media information Literacy for combating hoaxes in Indonesia: A case study of Indonesian National Movements. *Informacijos Mokslai*, 90, 26-41. <https://doi.org/10.15388/im.2020.90.48>
- UNICRI & UNCCT. (2021) Countering terrorism online with Artificial Intelligence - An overview for law enforcement and counter-terrorism agencies in South Asia and South-East Asia. <https://unicri.org/Publications/Countering-Terrorism-Online-with-Artificial-Intelligence-%20SouthAsia-South-EastAsia>
- United Nations Office on Drugs and Crime. (2020). Darknet cybercrime: Threats to Southeast Asia. UNODC Regional Office for Southeast Asia and the Pacific. <https://www.unodc.org/roseap/uploads/archive/documents/darknet/index.html>
- Varagur, K. (2015, December 2). World's Largest Islamic Organization Tells Isis to Get Lost. The Huffington Post. [https://www.huffingtonpost.com/entry/indonesian-muslims-counter-isis\\_us\\_565c737ae4b072e9d1c26bda?guccounter=1](https://www.huffingtonpost.com/entry/indonesian-muslims-counter-isis_us_565c737ae4b072e9d1c26bda?guccounter=1)
- Veilleux-Lepage, Y., & Füredi, Z. (2025). Beyond the FGC-9: How the Urutau redefines the global 3D-printed firearm movement. GNET. <https://gnet-research.org/2025/01/08/beyond-the-fgc-9-how-the-urutau-redefines-the-global-3d-printed-firearm-movement/>
- Wan Rosli, W. R. (n.d.). Violent extremism and Artificial intelligence: A Double-Edged Sword in the context of ASEAN. *Commonwealth Cyber Journal*, 46-48. <https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2024-06/ccj-2-1-violent-extremism-ai-wan-rosli.pdf>



- Ware, J. (2023). The third generation of online radicalization. Program on Extremism at George Washington University. <https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/2023-06/third-generation-final.pdf>
- West, L. J. (2021). The impact of technology on extremism. In L. Close & D. Impiombato (Eds.), COUNTERTERRORISM YEARBOOK 2021 (pp. 29–32). Australian Strategic Policy Institute. <http://www.jstor.org/stable/resrep31258.9>
- White, J., Wallner, C., Lamphere-Englund, G., Love Frankie, Kowert, R., Schlegel, L., Kingdon, A., Phelan, A., Newhouse, A., Saiz Erasquin, G., & Regeni, P. (2024). Radicalisation through gaming: The role of gendered social identity (Whitehall Report). RUSI. <https://www.rusi.org/explore-our-research/publications/whitehall-reports/radicalisation-through-gaming-role-gendered-social-identity>
- Wibisono, A. A., Kumendong, R., & Maulana, I. (2024). Indonesia's Handling of Terrorists' Cyber Activities: How Repressive Measures Still Fall Short. *Journal of Asian Security and International Affairs*, 12(1), 134-160. <https://doi.org/10.1177/23477970241298764> (original work published 2025)
- Wiegold, L., Winkler, C., & Jaskowski, J. (2024). Camera, action, play: An exploration of extremist activity on video- and livestreaming platforms. GNET. <https://gnet-research.org/2024/07/18/camera-action-play-an-exploration-of-extremist-activity-on-video-and-livestreaming-platforms/>
- Yani, A. A. (2021). An examination of Indonesia's Anti-Terrorism policy during the COVID 19: The rise of Digital-Based Terrorism Propaganda among Youths. *Hasanuddin Journal of Social & Political Sciences*, 1 (2), 77–85. <https://journal.unhas.ac.id/index.php/hjsps/article/view/19920>
- Yilmaz, K., & Atamuradova, F. (2022). A comparative analysis of ISIS Channels On Telegram. *Sicurezza, Terrorismo E Società*, 16, 67-68. <https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/12/SicTerSoc16-Kamil-Yilmaz-%E2%80%93-Farangiz-Atamuradova-A-comparative-analysis-of-ISIS-Channels-On-Telegram.pdf>
- Zao-Sanders, M. (2025, April 9). How people are really using gen AI in 2025. *Harvard Business Review*. <https://hbr.org/2025/04/how-people-are-really-using-gen-ai-in-2025>

## Lampiran A: Ringkasan Sesi Presentasi Indonesia

Pada akhir proses penelitian, Hedayah bekerja sama dengan BNPT Indonesia menyelenggarakan sesi gabungan di Jakarta, Indonesia pada tanggal 19 Juni 2025 untuk mempresentasikan temuan-temuan penelitian, membuka kesempatan untuk bertanya dan berdiskusi dengan para pemangku kepentingan yang berpartisipasi dalam penelitian, serta menyoroti penelitian dan kegiatan pelengkap yang dipimpin oleh pemerintah Indonesia.

### Sambutan Pembukaan

Sambutan pembukaan disampaikan oleh:

- ◆ Bapak Andhika Chrisnayudhanto - Deputi Bidang Kerjasama Internasional, Badan Nasional Penanggulangan Terorisme (BNPT)
- ◆ Ibu Esther Perry - Counselor, Kedutaan Besar Australia di Jakarta
- ◆ Ibu Anna Sherburn - Wakil Direktur Eksekutif, Hedayah

Para pembicara menyoroti berbagai upaya yang sedang berlangsung untuk mengatasi ekstremisme dan ekstremisme berbasis kekerasan di dunia maya serta pentingnya untuk terus memahami dan menanggapi tantangan ini, dan menegaskan kembali komitmen terhadap upaya-upaya tersebut.

### Diskusi Panel

Dengan kerangka yang telah dihadirkan oleh sambutan-sambutan ini, sesi dilanjutkan dengan diskusi panel penelitian.

Diskusi ini meliputi presentasi hasil dari Laporan Negara Indonesia tentang Memahami & Mencegah Ekstremisme dan Ekstremisme Kekerasan Online di Asia Tenggara yang ditulis oleh Hedayah. Informasi lebih lanjut tentang temuan dan rekomendasi Hedayah dapat ditemukan di bagian awal Laporan Negara ini.

Presentasi dari Kementerian Komunikasi dan Digital (Komdigi) menguraikan mekanisme mereka untuk moderasi konten, dan bagaimana proses ini bekerja dalam praktiknya, memberikan konteks penting tentang metode yang digunakan dan tantangan yang terkait dengan upaya-upaya tersebut. Rekomendasi utama yang disoroti adalah mendorong peningkatan literasi media dan kesadaran akan tantangan dan konten ekstremisme, tidak hanya untuk pemerintah tetapi juga di antara para pelaku utama lainnya, dan memperluas kerja sama dengan lembaga-lembaga lain untuk merespons ancaman dan kebutuhan ini dengan lebih baik.

Presentasi dari Indonesia Knowledge Hub on Countering Terrorism and Violent Extremism (I-KHub) dari BNPT membagikan hasil dari Outlook mereka baru-baru ini. Melihat penurunan serangan yang terkait dengan tanggapan pemerintah sejauh ini, presentasi ini juga mencatat peningkatan tren konten ekstremis yang terlihat di berbagai platform. Oleh karena itu, presentasi ini menyoroti perlunya mempertimbangkan titik temu antara ancaman teknis dan kerentanan sosial, yang bersama-sama membentuk konteks radikalisisasi. Rekomendasi utama meliputi penguatan pendekatan non-formal untuk membangun ketahanan dan investasi dalam upaya regional untuk memanfaatkan kecerdasan buatan (AI) untuk mendeteksi konten ekstremis dengan melibatkan mitra masyarakat sipil.

Outlook ini dan produk lainnya tersedia di I-KHub di [www.ikhub.id](http://www.ikhub.id).

## Umpan Balik & Diskusi

Setelah presentasi ini, disediakan waktu untuk bertanya dan berdiskusi dengan para peserta. Diskusi ini menggarisbawahi hal-hal berikut:

- ◆ Tantangan yang ada seputar gender dan inklusivitas: Menyoroti secara positif bahwa Laporan Negara ini menyebutkan tantangan-tantangan ini, dan menekankan bahwa narasi seputar ekstremisme, kekerasan, dan terorisme daring tidak pernah netral gender, dan biasanya menargetkan berdasarkan gender, bahkan mencatat tren kelompok ekstremis atau ekstremis kekerasan yang memanfaatkan Bahasa dan istilah hak-hak perempuan untuk mengadvokasi untuk terlibat dalam ekstremisme kekerasan untuk mendukung otonomi tubuh perempuan. Penggunaan narasi gender yang regresif oleh kelompok ekstremis dan ekstremis kekerasan secara luring juga menimbulkan risiko merembet ke ruang dan wacana luring, sejalan temuan Laporan Negara tentang ketidakpatutan, dan lebih lanjut menekankan perlunya memastikan bahwa kelompok-kelompok yang terpinggirkan yang tidak dianggap rentan terhadap narasi ekstremis dan ekstremis kekerasan tidak diabaikan dalam upaya penanggulangan ekstremisme, dan dapat menjadi mitra dalam upaya-upaya penanggulangan yang potensial.
- ◆ Peran kontra narasi yang efektif dalam mengurangi radikalisasi: Menekankan perlunya upaya kolaboratif untuk menciptakan dan menyebarkan narasi tandingan (atau narasi positif dan alternatif), dengan mencatat bahwa upaya penghapusan (yaitu, moderasi konten) mungkin kuat, tetapi konten baru terus dibuat dan kita tidak dapat mengandalkan upaya moderasi saja untuk membangun ketahanan daring dan mencegah ekstremisme daring.
- ◆ Perubahan lanskap online, literasi media dan informasi, serta kecerdasan buatan: Menekankan tantangan yang ditimbulkan oleh rendahnya literasi digital dan media dan informasi (MIL), terutama dalam menghadapi AI generatif, dengan mencatat perlunya untuk terus memantau kemunculan teknologi baru.

Pertanyaan-pertanyaan yang diajukan oleh para peserta mengenai temuan-temuan penelitian juga disertakan:

- ◆ Tren apa yang dicatat dalam laporan mengenai bagaimana perangkat daring digunakan untuk merekrut, meradikalisasi, dan memobilisasi, dalam rangka mendukung prioritas upaya dan intervensi strategis.
- ◆ Kelompok mana yang paling produktif dalam membagikan konten ekstremis atau kekerasan ekstremis secara daring?
- ◆ Apa maksud dari penargetan anak-anak di platform game, dan apa tujuan dari upaya tersebut?
- ◆ Jenis konten ekstremis atau kekerasan ekstremis apa saja, dan jenis narasi apa saja, yang berkembang di dunia maya saat ini? Bagaimana peristiwa politik global dapat membentuk dan memperkuat pesan dari konten lokal Indonesia?

## Pemangku Kepentingan yang Berpartisipasi

Sesi ini dihadiri (secara langsung dan daring) oleh perwakilan dari organisasi-organisasi berikut:

- ◆ Badan Nasional Penanggulangan Terorisme (BNPT)
- ◆ Kementerian Komunikasi dan Digital
- ◆ Detasemen Khusus (Densus) 88 Antiteror (Polri)
- ◆ Kementerian Luar Negeri
- ◆ Badan Siber dan Sandi Negara
- ◆ Kementerian Agama
- ◆ Kementerian Pendidikan Dasar dan Menengah
- ◆ Kedutaan Besar Australia Jakarta
- ◆ Kedutaan Besar Inggris Jakarta
- ◆ Aktivisme Lintas Batas
- ◆ Pusat Kajian Radikalisme dan Deradikalisasi (PAKAR)
- ◆ Forum LSM Internasional untuk Pembangunan Indonesia (INFID)
- ◆ PeaceGeneration Indonesia
- ◆ AMAN Indonesia
- ◆ Wahid Foundation
- ◆ Universitas Teknologi Nanyang
- ◆ Hedayah

Hedayah berterima kasih kepada semua pihak yang telah mengambil bagian dalam penelitian ini dan berbagi keahlian dan umpan balik selama proses penelitian, serta semua yang telah menghadiri acara ini.







Hedayah

Countering Extremism  
& Violent Extremism

[WWW.HEDAYAH.COM](http://WWW.HEDAYAH.COM)



HEDAYAH\_CVE



HEDAYAH