

Analisa *Future Terrorism Threat* Dari Serangan Manual ke Serangan Otonom: Transformasi Strategi Terorisme di Era Drone dan Kecerdasan Buatan

Rommy Edward Pryambada^{1*}

¹ Pemerhati Politik & Keamanan Publik, Sekolah Tinggi Ilmu Hukum Dharma Andhiga

Korespondensi penulis: rommyepborneo@gmail.com

Abstract. *The development of drone technology and artificial intelligence (AI) has presented great opportunities in various sectors, but at the same time opened up new loopholes for potential terrorist attacks. This article analyzes the shift in terrorism attack strategies from traditional manual methods to the use of drone-based autonomous systems and AI. Through a descriptive qualitative approach and literature review, this study explores how this technology is used to improve the effectiveness, anonymity, and scale of attacks. The study also discusses threats arising from AI-based drone swarm capabilities, potential cyberattacks on drone systems, and global regulatory lags in anticipating these threats. In addition, this article offers policy recommendations to strengthen national defense systems against the increasingly complex and automated evolution of terrorism threats. These findings are expected to be an early contribution to the development of counter-terrorism strategies that are adaptive to technological advances.*

Keywords: *Terrorism, Drones, Artificial Intelligence, Autonomous Attacks, National Security*

Abstrak. Perkembangan teknologi drone dan kecerdasan buatan (AI) telah menghadirkan peluang besar dalam berbagai sektor, namun sekaligus membuka celah baru bagi potensi serangan terorisme. Artikel ini menganalisis pergeseran strategi serangan terorisme dari metode manual tradisional ke penggunaan sistem otonom berbasis drone dan AI. Melalui pendekatan kualitatif deskriptif dan kajian literatur, penelitian ini mengeksplorasi bagaimana teknologi ini dimanfaatkan untuk meningkatkan efektivitas, anonimitas, dan skala serangan. Studi ini juga membahas ancaman yang muncul dari kemampuan drone swarm berbasis AI, potensi serangan siber terhadap sistem drone, serta ketertinggalan regulasi global dalam mengantisipasi ancaman ini. Selain itu, artikel ini menawarkan rekomendasi kebijakan untuk memperkuat sistem pertahanan nasional terhadap evolusi ancaman terorisme yang semakin kompleks dan terotomatisasi. Temuan ini diharapkan dapat menjadi kontribusi awal dalam pengembangan strategi kontra-terorisme yang adaptif terhadap kemajuan teknologi.

Kata kunci: Terorisme, Drone, Kecerdasan Buatan, Serangan Otonom, Keamanan Nasional

1. LATAR BELAKANG

Perkembangan teknologi dalam dua dekade terakhir telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk dalam domain keamanan dan pertahanan (Lutfiani et al., 2023). Teknologi drone (*Unmanned Aerial Vehicles/UAV*) dan kecerdasan buatan (*Artificial Intelligence/AI*) adalah dua contoh inovasi yang awalnya dikembangkan untuk tujuan damai dan efisiensi operasional, namun kini juga membuka peluang baru bagi ancaman keamanan global (Downey, 2024). Ketersediaan drone komersial yang semakin murah, serta kemajuan AI dalam bidang navigasi, pengenalan pola, dan pengambilan keputusan otomatis, telah menciptakan celah yang dapat dimanfaatkan oleh aktor-aktor non-negara, termasuk kelompok teroris (Dobson, 2015). Transformasi modus serangan terorisme terjadi seiring dengan adopsi teknologi ini (Rakhshandehroo et al., 2023). Jika pada masa lalu serangan teroris umumnya mengandalkan kehadiran fisik pelaku di lokasi serangan, saat ini teknologi

memungkinkan pelaku untuk menjalankan aksi dari jarak jauh tanpa kehadiran langsung, meminimalkan risiko deteksi dan penangkapan (Hazenbergh & Beridze, 2021).

Drone dapat dimodifikasi untuk membawa bahan peledak atau melakukan pengintaian terhadap target, sementara AI memungkinkan sistem ini untuk beroperasi secara otonom tanpa perlu kendali manusia secara real-time (Susdarwono, 2021). Dalam konteks ini, algoritma kecerdasan buatan berperan penting dalam mengendalikan dan mengoptimalkan sistem drone, sehingga memungkinkan pelaku terorisme untuk mengadaptasi taktik dan menganalisis lingkungan operasi secara real time (Sorochkin et al., 2024). Beberapa kasus nyata telah menunjukkan pergeseran ini. Misalnya, ISIS dilaporkan menggunakan drone komersial yang dimodifikasi untuk menyerang pasukan koalisi di Timur Tengah, sementara kelompok Houthi di Yaman memanfaatkan teknologi drone dalam serangan terhadap infrastruktur minyak Arab Saudi. Penggunaan drone swarm sekelompok drone yang dikoordinasikan oleh AI untuk menyerang secara simultan juga menjadi potensi ancaman serius yang dapat melumpuhkan sistem pertahanan konvensional (Waqar et al., 2023). Pemanfaatan teknologi AI ini telah meningkatkan kemampuan drone dalam misi pengintaian, pengawasan, dan bahkan serangan yang sangat terfokus, yang sebelumnya hanya dapat dijalankan oleh sistem militer negara maju, kemampuan machine learning untuk belajar dari data yang diperoleh dari operasi lapangan telah memberikan keunggulan strategis bagi kelompok teroris yang mengadopsi teknologi ini secara inovatif (Downey, 2024).

Potensi ancaman ini tidak hanya menjadi kekhawatiran global, tetapi juga berpotensi terjadi di Indonesia (Korteling et al., 2021). Sebagai negara kepulauan dengan banyak target vital seperti fasilitas pemerintahan, instalasi energi, dan pusat-pusat ekonomi, Indonesia rentan terhadap penyalahgunaan teknologi drone dan AI untuk aksi terorisme (Shankar et al., 2024). Beberapa kelompok radikal domestik telah menunjukkan kemampuan untuk beradaptasi dengan perkembangan teknologi, seperti penggunaan media sosial untuk perekrutan dan propaganda. Maka, tidak menutup kemungkinan dalam waktu dekat, mereka akan mengeksplorasi penggunaan drone bersenjata atau operasi otonom berbasis AI untuk meluncurkan serangan (Wang, 2023). Hal ini menjadi tantangan serius bagi aparat keamanan nasional dalam memperkuat deteksi dini, pencegahan, serta pengembangan sistem pertahanan terhadap ancaman berbasis teknologi tinggi. Situasi ini menuntut adanya pemahaman yang lebih mendalam tentang bagaimana teknologi baru ini diadopsi dalam strategi terorisme modern dan bagaimana upaya mitigasi dapat dikembangkan, apalagi kemudian kemampuan AI kedepannya akan membawa perubahan yang sangat fundamental dalam bidang militer dan keamanan (Johnson, 2019). Artikel ini berupaya memberikan kontribusi terhadap pemahaman

tersebut dengan mengeksplorasi dinamika perubahan modus serangan terorisme di era drone dan kecerdasan buatan. Berdasarkan literatur tersebut, tujuan penelitian ini untuk mengetahui analisa future terrorism threat dari serangan manual ke serangan otonom guna mengetahui transformasi strategi terorisme di era drone dan kecerdasan buatan.

2. KAJIAN TEORITIS

Drone, atau yang secara teknis dikenal sebagai *Unmanned Aerial Vehicles* (UAV), adalah wahana udara yang dioperasikan tanpa awak manusia di dalamnya, baik melalui kendali jarak jauh maupun secara otonom menggunakan algoritma tertentu. Definisi ini mencakup berbagai jenis platform, mulai dari drone mini untuk penggunaan sipil hingga UAV militer berskala besar. Menurut Gettinger (2020), drone awalnya dikembangkan untuk keperluan militer seperti pengintaian dan serangan presisi, namun seiring waktu teknologinya diadaptasi ke berbagai sektor sipil, termasuk pertanian, logistik, dan pemantauan bencana (Wang, 2023).

Evolusi teknologi drone mengalami percepatan sejak awal abad ke-21, didorong oleh kemajuan dalam bidang miniaturisasi sensor, sistem navigasi berbasis *Global Positioning System* (GPS), baterai berkapasitas tinggi, serta kecerdasan buatan. Generasi awal drone bersifat semi-otomatis dengan kontrol penuh dari operator manusia. Saat ini, banyak model drone yang mampu melakukan misi secara mandiri, mulai dari navigasi rute kompleks hingga penghindaran rintangan dan pelaksanaan tugas berbasis visi komputer. Beredar luasnya keberadaan drone di market place memudahkan siapapun terlebih jika itu kelompok teroris yang kemudian memodifikasi dengan biaya yang tidak begitu mahal namun mampu meningkatkan kemampuan drone tersebut .

Transformasi ini tidak hanya meningkatkan kemampuan operasional drone, tetapi juga menurunkan biaya produksi dan memperluas aksesibilitas teknologi ini kepada publik. Akibatnya, aktor-aktor non-negara, termasuk kelompok teroris, memperoleh peluang baru untuk menggunakan drone dalam melaksanakan kegiatan ilegal dan berbahaya. Dengan integrasi AI, drone dapat diprogram untuk mengenali target, menentukan jalur serangan, dan menyesuaikan taktik di lapangan tanpa intervensi manusia langsung, meningkatkan efektivitas sekaligus mengurangi risiko bagi pelaku. Dalam konteks keamanan, kemampuan drone untuk menyusup ke wilayah terlarang, membawa muatan berbahaya, dan melakukan serangan terkoordinasi melalui teknologi swarm menambah kompleksitas tantangan yang dihadapi aparat keamanan nasional maupun internasional (Mehta et al., 2021).

Perkembangan Kecerdasan Buatan dalam Aplikasi Militer dan Sipil

Kecerdasan buatan (*Artificial Intelligence/AI*) didefinisikan sebagai kemampuan sistem komputer untuk melakukan tugas-tugas yang biasanya membutuhkan kecerdasan manusia, seperti persepsi visual, pengenalan suara, pengambilan keputusan, dan penerjemahan bahasa (Gruetzemacher & Whittlestone, 2022; Taboada et al., 2023). Dalam dua dekade terakhir, perkembangan AI telah mengubah banyak aspek kehidupan, termasuk dalam bidang militer dan sipil (Trandberg Jensen & Jensen, 2023).

Dalam aplikasi militer, AI digunakan untuk meningkatkan efektivitas sistem persenjataan, kendaraan tempur otonom, sistem pertahanan udara, serta platform intelijen, pengawasan, dan pengintaian (ISR). Teknologi AI memungkinkan sistem-sistem ini untuk beroperasi lebih cepat, lebih presisi, dan dengan tingkat ketergantungan yang lebih rendah terhadap operator manusia. Contoh konkret penerapan AI dalam militer adalah penggunaan sistem senjata otonom seperti drone tempur MQ-9 Reaper yang mampu melakukan serangan presisi berdasarkan data yang dianalisis secara real-time (Rawat et al., 2022).

Di sektor sipil, AI diterapkan dalam bidang transportasi (mobil otonom), kesehatan (diagnosis berbantuan AI), industri manufaktur (robot industri pintar), hingga dalam layanan publik seperti sistem prediksi cuaca dan analisis data keamanan siber. Integrasi AI dalam kehidupan sehari-hari meningkatkan efisiensi, namun sekaligus menimbulkan tantangan baru dalam bidang keamanan dan etika (Damoah et al., 2021).

Dalam konteks ancaman terorisme, kemajuan AI menghadirkan risiko serius. AI dapat digunakan untuk mengendalikan drone dalam misi serangan, menyusupkan malware ke sistem keamanan digital, atau bahkan mengelola serangan cyber-physical secara otomatis. Teroris dapat memanfaatkan kemampuan AI dalam pengenalan wajah untuk memilih target, navigasi otonom untuk menembus sistem pertahanan, dan pembelajaran mesin untuk mengoptimalkan pola serangan berdasarkan pengalaman masa lalu. Oleh karena itu, pemahaman terhadap perkembangan AI dan implikasinya dalam konteks militer dan sipil menjadi sangat penting dalam merumuskan strategi pertahanan dan kebijakan keamanan nasional (Damoah et al., 2021).

Studi Terdahulu Tentang Penggunaan Teknologi dalam Serangan Teroris

Berbagai studi terdahulu menunjukkan bahwa teknologi telah menjadi alat penting dalam evolusi taktik terorisme modern. Pada awalnya, teknologi komunikasi seperti internet dan media sosial digunakan untuk propaganda, perekrutan, serta koordinasi antar jaringan teroris lintas negara. Seiring perkembangan, penggunaan teknologi semakin bergeser ke pemanfaatan alat fisik canggih, termasuk drone dan sistem berbasis AI (Sorochnik, O., Sosulin, M., &

Matveev, 2024). Penelitian Ressler (2018) dari Combating Terrorism Center mengungkapkan bahwa ISIS adalah salah satu organisasi teroris pertama yang secara sistematis menggunakan drone komersial untuk tujuan serangan. Mereka memodifikasi drone untuk membawa bahan peledak ringan, melakukan pengintaian medan perang, dan mendokumentasikan serangan untuk kepentingan propaganda. Studi ini menunjukkan bahwa teknologi yang awalnya dikembangkan untuk penggunaan sipil dapat dengan mudah diadaptasi untuk tujuan militeristik oleh aktor non-negara.

Di sisi lain, Gettinger (2020) mendokumentasikan tren global terkait penyebaran teknologi drone dan meningkatnya kekhawatiran mengenai penggunaan UAV dalam serangan terhadap infrastruktur kritis. Dalam kasus serangan terhadap fasilitas minyak Saudi Aramco pada 2019, serangan tersebut diyakini melibatkan kombinasi drone dan rudal jelajah dengan tingkat presisi tinggi, yang memanfaatkan navigasi berbasis GPS dan kemungkinan dukungan AI dalam sistem targeting. Selain itu, laporan dari Hazenberg & Beridze (2021) menekankan bahwa AI berpotensi digunakan oleh kelompok teroris untuk mempercepat proses analisis data intelijen, merancang serangan berbasis prediksi perilaku target, hingga mengotomatiskan serangan cyber terhadap infrastruktur penting. Potensi ini memperbesar risiko serangan yang lebih sulit dideteksi dan diantisipasi oleh otoritas keamanan.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk memahami fenomena transformasi strategi serangan terorisme di era teknologi drone dan kecerdasan buatan. Pendekatan kualitatif dipilih karena fokus penelitian ini adalah untuk mengeksplorasi dan menginterpretasikan makna di balik fenomena penggunaan teknologi canggih dalam aksi terorisme, bukan untuk menguji hipotesis kuantitatif.

Deskriptif berarti bahwa penelitian ini berupaya memberikan gambaran yang sistematis, faktual, dan akurat mengenai fakta-fakta, sifat-sifat, serta hubungan antar fenomena yang diamati. Dengan demikian, artikel ini bertujuan untuk menggambarkan karakteristik perubahan strategi serangan terorisme, pola adaptasi teknologi oleh kelompok teroris, serta respons kebijakan keamanan yang ada.

Sumber data utama dalam penelitian ini diperoleh melalui studi literatur yang mencakup:

- Artikel jurnal ilmiah terkait drone, AI, dan keamanan nasional.
- Buku referensi yang membahas perkembangan teknologi militer dan penggunaan AI.
- Berita dan laporan investigasi yang relevan dengan kasus-kasus penggunaan drone dalam serangan teroris.

Teknik analisis data dilakukan dengan pendekatan analisis isi (*content analysis*) terhadap dokumen-dokumen tersebut untuk mengidentifikasi tema-tema utama, pola, serta hubungan antar konsep yang relevan dengan tujuan penelitian.

Melalui metodologi ini, diharapkan diperoleh pemahaman yang komprehensif mengenai bagaimana kemajuan teknologi drone dan AI telah mengubah lanskap ancaman terorisme serta bagaimana upaya mitigasi dan adaptasi strategi keamanan perlu dikembangkan.

4. HASIL DAN PEMBAHASAN

Transformasi Strategi Terorisme: Dari Manual ke Otonom

Sebelum era digital dan kemajuan teknologi otonom, serangan terorisme tradisional sangat bergantung pada intervensi langsung manusia. Karakteristik utama dari serangan manual tradisional. Pelaku terorisme harus hadir secara fisik di lokasi target, baik sebagai pelaku bom bunuh diri, penembak, ataupun operator bahan peledak. Tingginya keterlibatan manusia menyebabkan risiko yang besar terhadap penangkapan atau kematian di tempat kejadian. Mobilitas serangan terbatas pada kemampuan fisik pelaku dan moda transportasi konvensional. Serangan manual umumnya membutuhkan perencanaan yang panjang dan kompleks, termasuk pengintaian manual, logistik manusia, dan penyamaran. Koordinasi antarpelaku sering kali mengandalkan pertemuan tatap muka, pesan tertulis, atau alat komunikasi sederhana yang lebih mudah disadap.

Contoh nyata dari serangan manual ini antara lain adalah serangan bom Bali 2002, serangan 11 September 2001 di Amerika Serikat, serta berbagai operasi pengeboman bunuh diri yang terjadi di kawasan Timur Tengah dan Asia Tenggara. Meskipun serangan-serangan ini efektif dalam menciptakan ketakutan dan dampak politik, namun ketergantungan pada kehadiran manusia secara langsung membatasi fleksibilitas, skala, dan kerahasiaan operasi terorisme. Hal ini mendorong kelompok-kelompok teroris untuk mencari metode baru yang lebih efisien, aman bagi pelaku, dan memiliki jangkauan operasional yang lebih luas melalui pemanfaatan teknologi. Dalam konteks dinamika kontemporer, kelompok-kelompok ini tidak hanya mengadaptasi pendekatan klasik seperti serangan langsung atau penyusupan, tetapi juga mengeksplorasi dan mengembangkan metode baru yang mencakup aspek propaganda digital, penyusunan jaringan pendanaan inovatif, dan optimalisasi jaringan operasional. Pendekatan inovatif ini memungkinkan mereka untuk meningkatkan efektivitas serangan sekaligus menghindari deteksi oleh aparat keamanan (Araque & Iglesias, 2020).

Adaptasi Kelompok Teror terhadap Teknologi Drone dan AI

Perkembangan teknologi drone dan kecerdasan buatan telah membuka peluang baru bagi kelompok teroris untuk meningkatkan efektivitas operasional mereka. Adaptasi terhadap teknologi ini terjadi melalui beberapa cara utama. Banyak kelompok teroris memodifikasi drone komersial yang tersedia di pasar terbuka untuk membawa bahan peledak ringan, melakukan pengintaian target, hingga menyerang sasaran vital. Contohnya adalah ISIS yang secara sistematis mengembangkan unit UAV untuk menyerang pasukan koalisi dan target militer di Irak dan Suriah.

Selain untuk serangan fisik, drone digunakan untuk merekam operasi dan menyebarkan video serangan ke media sosial, meningkatkan efek psikologis terhadap lawan dan menarik simpatisan baru. Meski masih dalam tahap awal, terdapat indikasi bahwa beberapa kelompok mulai mengeksplorasi penggunaan algoritma AI sederhana untuk navigasi otomatis, pengenalan target, dan pengaturan pola serangan drone secara mandiri tanpa operator manusia secara langsung. Adaptasi lebih lanjut terlihat pada konsep serangan berbasis "swarm," di mana banyak drone kecil digunakan secara bersamaan untuk membingungkan sistem pertahanan lawan. Hal ini telah diuji dalam beberapa konflik bersenjata di Timur Tengah.

Adaptasi ini menunjukkan bahwa kelompok teroris terus mengikuti dan mengeksploitasi kemajuan teknologi untuk mengatasi keterbatasan mereka dalam sumber daya dan meningkatkan kapabilitas serangan mereka. Ketersediaan teknologi ini di pasar sipil tanpa kontrol ketat mempercepat proses adopsi tersebut. Dengan kemampuan untuk menyerang dari jarak jauh, meningkatkan kerahasiaan operasi, serta meminimalkan risiko terhadap pelaku, penggunaan drone dan AI oleh kelompok teroris diprediksi akan terus berkembang dalam kompleksitas dan skala dalam beberapa tahun ke depan.

Potensi Ancaman di Era Drone dan AI

Era drone dan kecerdasan buatan (AI) menghadirkan tantangan baru yang kompleks terhadap keamanan nasional dan internasional. Ancaman yang muncul tidak hanya berasal dari penggunaan individual drone untuk serangan langsung, tetapi juga dari pengembangan teknik serangan massal, otomatisasi pengambilan keputusan, serta manipulasi sistem pertahanan melalui serangan siber berbasis AI.

a. *Swarm Drone Attack*

Swarm drone merupakan teknik di mana sejumlah besar drone kecil dikendalikan secara terkoordinasi untuk menyerang target tertentu. Dengan algoritma AI, drone-drone ini dapat mengatur formasi, berbagi informasi dalam jaringan, dan beradaptasi terhadap perubahan

lingkungan secara mandiri. Potensi destruktif dari swarm drone sangat besar karena dapat mengatasi sistem pertahanan udara konvensional yang dirancang untuk menghadapi ancaman tunggal. Selain itu, swarm drone memiliki kemampuan untuk melakukan manuver evasif, mengubah jalur serangan secara real-time, dan membagi peran masing-masing unit, seperti drone penyerang, drone pengalihan perhatian, dan drone pengintai. Koordinasi dinamis ini membuat swarm drone jauh lebih sulit untuk dilawan dibandingkan dengan ancaman drone tunggal.

Kemampuan swarm untuk memperbanyak jumlah serangan dari berbagai arah secara simultan dapat menyebabkan sistem pertahanan kewalahan, bahkan yang dilengkapi dengan radar modern sekalipun. Terlebih lagi, teknologi ini dapat digunakan untuk menyerang infrastruktur vital seperti pembangkit listrik, fasilitas komunikasi, atau fasilitas pemerintahan, yang dapat menyebabkan kerusakan sistemik dan efek domino yang luas terhadap stabilitas sosial dan ekonomi. Proliferasi drone telah menyebabkan fenomena penggunaan ganda di mana teknologi yang awalnya dikembangkan untuk pengawasan dan operasi militer juga dapat dieksploitasi oleh kelompok teroris untuk tujuan jahat. Di antara potensi ancaman yang muncul adalah pemanfaatan kawanan drone, yang dapat memungkinkan teroris untuk melakukan serangan yang terkoordinasi dan kompleks terhadap infrastruktur penting dan target sipil. Dengan biaya relatif rendah dan tingkat keberhasilan tinggi, swarm drone menjadi salah satu ancaman paling serius dalam skenario ancaman terorisme berbasis teknologi masa depan. Jika teknologi ini jatuh ke tangan kelompok teroris, dampaknya dapat jauh lebih destruktif dibandingkan serangan konvensional.

b. AI dalam Navigasi, Target Acquisition, dan Decision-Making

Integrasi kecerdasan buatan (*Artificial Intelligence*) dalam operasi drone menghadirkan perubahan besar dalam hal navigasi, akuisisi target, dan pengambilan keputusan. Sistem navigasi berbasis AI memungkinkan drone untuk terbang secara mandiri melewati medan yang kompleks tanpa bantuan manusia, menggunakan teknologi seperti computer vision, GPS, dan sensor penginderaan jarak jauh. Dengan demikian, drone dapat menghindari rintangan secara otomatis, memilih jalur penerbangan optimal, dan beradaptasi terhadap perubahan kondisi lingkungan secara real-time. Dalam akuisisi target (*target acquisition*), AI memanfaatkan algoritma pengenalan wajah, pengenalan objek, dan analisis pola untuk mengidentifikasi dan membedakan target prioritas di antara kerumunan atau infrastruktur lainnya. Kemampuan ini memungkinkan drone untuk melakukan seleksi target dengan tingkat presisi tinggi tanpa perlu keterlibatan operator secara langsung, sehingga meningkatkan efektivitas serangan sekaligus mengurangi kemungkinan salah sasaran.

Dalam aspek pengambilan keputusan (*decision-making*), AI dapat menganalisis data dalam jumlah besar dari berbagai sensor onboard untuk menentukan kapan, bagaimana, dan dengan metode apa serangan harus dilakukan. Drone yang dilengkapi AI mampu membuat keputusan taktis di medan operasi berdasarkan logika pemrograman dan pembelajaran mesin, bahkan dalam situasi yang tidak terduga. Fitur ini sangat mengkhawatirkan dalam konteks terorisme karena memungkinkan serangan dilaksanakan tanpa jeda waktu yang dibutuhkan untuk menunggu perintah manusia. Penerapan AI dalam ketiga aspek ini menciptakan tantangan besar bagi sistem keamanan konvensional karena mempercepat waktu reaksi serangan, meningkatkan akurasi serangan, memperbesar skala kerusakan, dan mengaburkan jejak pelaku.

c. Kerentanan Siber

Kerentanan siber pada sistem drone dan jaringan pendukungnya menjadi ancaman serius di era modern. Drone modern mengandalkan jaringan komunikasi nirkabel untuk navigasi, kontrol, dan pertukaran data, membuatnya rentan terhadap serangan siber seperti pembajakan (*hijacking*), spoofing GPS, dan *denial of service* (DoS).

Pembajakan drone memungkinkan pihak yang tidak berwenang mengambil alih kendali drone dan menggunakannya untuk tujuan berbahaya, termasuk menyerang target sipil atau militer. Teknik spoofing GPS, yaitu manipulasi sinyal GPS yang diterima drone, dapat menyebabkan drone tersesat atau diarahkan ke target yang tidak diinginkan. Serangan DoS dapat melumpuhkan sistem komunikasi dan navigasi drone, membuatnya tidak dapat beroperasi dengan efektif.

Selain itu, adanya integrasi AI dalam sistem drone meningkatkan kompleksitas kerentanannya. Algoritma AI dapat menjadi sasaran serangan adversarial, yaitu upaya untuk memanipulasi model AI dengan model input yang dirancang sedemikian rupa sehingga AI mengambil keputusan yang salah, seperti contoh salah mengenali target atau rute penerbangan. Lebih jauh lagi, serangan terhadap infrastruktur *cloud* atau pusat data yang mendukung operasi drone juga dapat menyebabkan kebocoran data sensitif atau manipulasi misi drone secara massal. Dengan semakin terhubungnya berbagai sistem dalam *Internet of Things* (IoT), risiko penyebaran serangan siber ke jaringan luas dipastikan akan juga meningkat.

Oleh karena itu, penguatan *cybersecurity* dalam semua lapisan operasional drone, termasuk enkripsi komunikasi, autentikasi multi-faktor, dan proteksi terhadap AI adversarial, menjadi kebutuhan mendesak untuk mencegah eksploitasi teknologi ini oleh kelompok teroris. Ancaman-ancaman ini menunjukkan bahwa di era teknologi maju, garis antara serangan fisik dan siber menjadi semakin kabur. Oleh karena itu, dibutuhkan pendekatan keamanan yang

terintegrasi, adaptif, dan berbasis teknologi untuk menghadapi ancaman dari penggunaan drone dan AI oleh kelompok teroris.

Keterbatasan Regulasi dan Upaya Mitigasi

Perkembangan pesat teknologi drone dan kecerdasan buatan belum sepenuhnya diimbangi oleh kerangka regulasi yang memadai di tingkat nasional maupun internasional. Banyak negara, termasuk Indonesia, masih berfokus pada regulasi penggunaan drone dalam sektor sipil seperti untuk kebutuhan komersial dan hobi, tanpa memperhatikan potensi eksploitasi untuk tujuan terorisme.

a. Keterbatasan Regulasi

Sebagian besar peraturan yang ada hanya mengatur aspek teknis penerbangan drone, seperti batas ketinggian, area terlarang (*no-fly zones*), dan izin operasional. Regulasi terkait integrasi AI dalam sistem drone, pengamanan siber untuk kontrol drone, dan pencegahan penyalahgunaan teknologi otonom untuk tujuan kejahatan masih sangat terbatas. Di tingkat internasional, belum ada konvensi global yang spesifik mengatur penggunaan senjata otonom dan teknologi berbasis AI dalam konteks non-negara, termasuk terorisme. Inisiatif seperti "*Convention on Certain Conventional Weapons*" (CCW) baru sebatas membahas senjata otonom dalam konflik bersenjata antarnegara, sehingga celah hukum untuk penggunaan oleh kelompok teroris tetap terbuka.

b. Upaya Mitigasi

Upaya mitigasi terhadap ancaman ini dapat dilakukan melalui beberapa langkah strategis. Pemerintah perlu memperbarui dan memperluas regulasi terkait drone dan AI dengan memasukkan aspek keamanan nasional, termasuk pembatasan teknis pada fitur otonomi drone dan sistem pertahanan anti-drone yang lebih canggih. Perlindungan terhadap sistem komunikasi drone, basis data operasional, dan algoritma AI harus diperkuat melalui standar keamanan siber yang ketat, termasuk enkripsi tingkat tinggi dan sistem deteksi intrusi.

Investasi dalam teknologi pendeteksian dan penonaktifan drone berbahaya, seperti sistem radar kecil, jammer frekuensi radio, dan drone interceptor, menjadi langkah penting untuk menghadapi ancaman swarm attack dan serangan individu. Mengingat sifat ancaman yang lintas batas, diperlukan kerja sama antarnegara dalam berbagi intelijen, menetapkan standar global penggunaan drone dan AI, serta mengembangkan protokol respons cepat terhadap insiden terkait teknologi otonom. Edukasi kepada masyarakat tentang bahaya penyalahgunaan teknologi drone dan AI, serta pelatihan kepada aparat penegak hukum dan militer dalam mendeteksi dan menanggulangi ancaman ini. Langkah-langkah tersebut harus

diintegrasikan dalam strategi nasional keamanan dan pertahanan untuk memastikan kesiapsiagaan menghadapi ancaman terorisme berbasis teknologi di masa depan.

Implikasi terhadap Strategi Kontra-Terrorisme

Kemajuan teknologi drone dan kecerdasan buatan mengharuskan strategi kontra-terorisme untuk beradaptasi dan mengembangkan pendekatan baru yang lebih proaktif, terintegrasi, dan berbasis teknologi. Implikasi utama terhadap strategi kontra-terorisme meliputi beberapa aspek berikut:

a) Perluasan Deteksi dan Intelijen Teknologi

Strategi kontra-terorisme harus mengutamakan deteksi dini terhadap potensi ancaman berbasis drone dan AI. Ini memerlukan investasi pada sistem pemantauan berbasis radar mini, sensor akustik, serta penggunaan AI dalam analisis intelijen untuk memprediksi pola serangan berbasis data besar (big data). Selain itu, diperlukan pengembangan sistem pemantauan udara berbasis jaringan terdistribusi (distributed sensor networks) yang mampu mengidentifikasi keberadaan drone dalam berbagai kondisi geografis dan cuaca. Sistem ini harus terintegrasi dengan pusat komando dan kontrol nasional untuk memungkinkan respons cepat dan efektif. Penerapan teknologi pengenalan perilaku (behavior recognition) berbasis AI dalam menganalisis aktivitas drone juga menjadi krusial. Teknologi ini dapat membedakan antara drone komersial biasa dan drone yang menunjukkan perilaku mencurigakan, seperti terbang mendekati objek vital atau melanggar zona larangan terbang.

Lebih jauh, penggunaan analitik prediktif dalam analisis intelijen diperlukan untuk mengantisipasi rencana serangan sebelum dieksekusi. Analitik ini dapat menggabungkan berbagai sumber data, mulai dari aktivitas online, pembelian komponen drone, hingga perubahan pola komunikasi kelompok teroris. Deteksi dan intelijen teknologi yang diperluas juga membutuhkan pelatihan khusus bagi personel keamanan dan intelijen untuk mengoperasikan dan menginterpretasikan data dari sistem-sistem canggih tersebut secara efektif.

b) Penguatan Pertahanan Aktif terhadap Drone

Dalam menghadapi ancaman dari drone, baik yang dikendalikan manusia maupun berbasis AI, penguatan pertahanan aktif menjadi sangat penting. Ini melibatkan pengembangan dan penerapan teknologi anti-drone yang dapat mendeteksi, melacak, mengidentifikasi, dan menetralkan ancaman drone dengan cepat. Sistem pertahanan aktif dapat mencakup penggunaan jammer elektromagnetik untuk mengganggu sinyal komunikasi antara drone dan operatornya, serta mengacaukan sistem navigasi berbasis

GPS. Selain itu, teknologi laser anti-drone dan senjata energi terarah (*Directed Energy Weapons/DEW*) mulai banyak dikembangkan untuk menghancurkan drone secara presisi tanpa menimbulkan kerusakan tambahan di sekitarnya. Pertahanan aktif juga mencakup *deployment drone "interceptor"* yang mampu mengejar dan menangkap atau menonaktifkan drone musuh di udara. Sistem seperti ini penting terutama dalam skenario serangan swarm, di mana kecepatan dan kemampuan multi-target sangat dibutuhkan.

Di samping pengembangan teknologi, strategi pertahanan aktif harus mencakup penempatan sistem ini di area vital seperti bandara, instalasi energi, fasilitas pemerintahan, pusat perbelanjaan besar, dan area publik strategis lainnya. Integrasi pertahanan aktif dengan pusat komando terpadu akan meningkatkan respons waktu nyata terhadap ancaman. Penguatan pertahanan aktif terhadap drone menjadi elemen kunci dalam menciptakan lapisan proteksi berlapis yang tidak hanya reaktif tetapi juga proaktif dalam menghadapi evolusi ancaman di era drone dan kecerdasan buatan.

c) **Revisi Kebijakan Keamanan Nasional**

Dalam menghadapi era baru ancaman berbasis drone dan kecerdasan buatan, revisi kebijakan keamanan nasional menjadi langkah yang tidak terelakkan. Kebijakan yang sebelumnya difokuskan pada ancaman konvensional kini harus diadaptasi untuk mengantisipasi dan merespons ancaman teknologi otonom. Diperlukan dokumen kebijakan nasional yang khusus mengatur mitigasi ancaman drone dan AI, termasuk pengembangan protokol pencegahan, deteksi, dan respons terhadap insiden drone berbahaya. Revisi terhadap undang-undang terkait penerbangan, keamanan nasional, dan teknologi informasi perlu dilakukan untuk mengakomodasi perkembangan teknologi dan memperkuat pengawasan penggunaan drone dan AI.

Pemerintah harus mengatur distribusi, impor, ekspor, dan penjualan drone, komponen AI, serta perangkat lunak terkait untuk mencegah jatuhnya teknologi ini ke tangan pihak-pihak yang berniat jahat. Karena banyak ancaman berasal dari dimensi siber, perlu ada integrasi yang lebih kuat antara kebijakan anti-terorisme dan strategi keamanan siber nasional. Kebijakan keamanan nasional harus memberikan perhatian khusus terhadap perlindungan instalasi vital negara (*critical infrastructure*) dari serangan drone dan AI.

Revisi kebijakan harus bersifat dinamis, responsif terhadap perkembangan teknologi global, serta berbasis pada prinsip pencegahan, deteksi dini, dan respons adaptif terhadap ancaman.

d) **Penguatan Kolaborasi Lintas Sektor**

Penguatan kolaborasi lintas sektor menjadi krusial dalam menghadapi ancaman drone dan kecerdasan buatan. Pemerintah tidak dapat bekerja sendiri; keterlibatan sektor swasta, komunitas teknologi, akademisi, dan masyarakat sipil menjadi pilar utama dalam membangun sistem pertahanan yang adaptif dan responsif. Industri teknologi, telekomunikasi, manufaktur drone, dan perusahaan *cybersecurity* perlu dilibatkan dalam pengembangan sistem deteksi, pencegahan, dan respons terhadap serangan drone. Kemitraan ini harus mencakup pertukaran informasi tentang ancaman baru dan kolaborasi dalam inovasi teknologi anti-drone (Waqar et al., 2023).

Universitas dan lembaga riset memiliki peran penting dalam melakukan penelitian dan pengembangan teknologi baru untuk menghadapi ancaman berbasis AI dan drone. Program penelitian bersama dapat mempercepat inovasi dalam sistem pertahanan aktif dan sistem analitik prediktif berbasis AI. Edukasi publik dan pelibatan komunitas lokal penting untuk membangun jaringan deteksi dini berbasis masyarakat. Program kesadaran keamanan teknologi perlu digalakkan untuk melatih masyarakat dalam mengidentifikasi dan melaporkan aktivitas drone mencurigakan. Koordinasi antara lembaga intelijen, militer, penegak hukum, dan badan regulator perlu diperkuat melalui pembentukan satuan tugas khusus (*task force*) yang fokus pada ancaman drone dan AI (Özer & Türkmen, 2023).

Kolaborasi lintas sektor ini harus bersifat berkelanjutan, berbasis kepercayaan, serta difasilitasi oleh kerangka kerja formal yang jelas agar sinergi antaraktor dapat berjalan optimal dalam menghadapi ancaman teknologi masa depan.

c. **Pelatihan dan Simulasi Respons Ancaman**

Pelatihan dan simulasi respons ancaman menjadi elemen fundamental dalam meningkatkan kesiapsiagaan menghadapi serangan berbasis drone dan kecerdasan buatan. Mengingat karakteristik ancaman yang dinamis, adaptif, dan berbasis teknologi canggih, maka strategi pelatihan harus dikembangkan secara berkelanjutan dan kontekstual. Aparat keamanan, militer, dan penegak hukum harus mendapatkan pelatihan teknis tentang pengoperasian sistem deteksi drone, penggunaan alat anti-drone, pengenalan teknologi AI yang digunakan dalam sistem serangan, serta teknik mitigasi ancaman siber. Simulasi harus melibatkan skenario berbasis ancaman aktual, seperti serangan drone swarm terhadap fasilitas vital, penyusupan drone ke wilayah terlarang, atau upaya pembajakan jaringan kontrol drone. Pendekatan ini membantu pasukan keamanan dalam memahami kompleksitas ancaman dan mengasah respons taktis. Diperlukan latihan yang melibatkan koordinasi antara berbagai lembaga seperti militer, polisi, dinas pemadam kebakaran, layanan kesehatan darurat, dan

badan intelijen untuk membangun interoperabilitas dalam respons ancaman drone (Özer & Türkmen, 2023).

Pemanfaatan simulasi virtual dan augmented reality (VR/AR) serta sistem berbasis AI dalam latihan dapat meningkatkan efektivitas pelatihan dan memungkinkan skenario latihan yang lebih kompleks tanpa risiko operasional di dunia nyata. Setiap sesi pelatihan dan simulasi perlu diikuti dengan evaluasi mendalam untuk mengidentifikasi kekuatan dan kelemahan respons, yang kemudian digunakan untuk memperbaiki prosedur dan protokol yang ada. Pelatihan dan simulasi yang konsisten, realistis, dan terintegrasi akan membentuk kesiapan operasional yang lebih kuat dalam menghadapi evolusi modus serangan terorisme berbasis drone dan kecerdasan buatan (Buchelt et al., 2024).

d. Kampanye Edukasi Publik dan Sosialisasi Risiko

Kampanye edukasi publik dan sosialisasi risiko memegang peranan penting dalam membangun ketahanan sosial terhadap ancaman teknologi baru seperti drone dan kecerdasan buatan. Publik yang teredukasi dengan baik dapat menjadi mata dan telinga tambahan bagi aparat keamanan serta berperan aktif dalam pencegahan serangan. Beberapa hal dibawah ini dapat dijadikan bentuk edukasi terhadap public secara luas. Pemerintah dan lembaga terkait perlu menginisiasi program-program sosialisasi untuk meningkatkan pemahaman masyarakat tentang potensi penyalahgunaan drone dan AI, termasuk bagaimana mengenali aktivitas yang mencurigakan. Informasi tentang regulasi penggunaan drone, prosedur pelaporan aktivitas mencurigakan, serta panduan keselamatan terkait drone harus disebarluaskan secara luas melalui televisi, radio, media sosial, dan portal daring resmi. Melibatkan komunitas lokal dalam pelatihan dasar tentang identifikasi ancaman berbasis drone dan prosedur pelaporan cepat kepada aparat berwenang. Mengadakan simulasi terbuka tentang bagaimana menghadapi potensi serangan drone dapat meningkatkan kewaspadaan dan kesiapsiagaan masyarakat umum. Mensosialisasikan pentingnya registrasi drone yang digunakan masyarakat umum serta penerapan sistem labeling agar setiap unit drone dapat dilacak dan diidentifikasi secara sah (Slimani et al., 2024).

Dengan membangun budaya keamanan berbasis partisipasi publik, risiko terhadap penyalahgunaan teknologi dapat ditekan lebih dini, serta memperkuat ketahanan nasional dalam menghadapi ancaman terorisme berbasis teknologi modern. Melalui pendekatan komprehensif yang adaptif terhadap perkembangan teknologi, strategi kontra-terorisme dapat lebih efektif dalam melindungi keamanan nasional dan mengantisipasi evolusi modus serangan terorisme berbasis drone dan kecerdasan buatan (Maguluri et al., 2023).

5. KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa perkembangan teknologi drone dan kecerdasan buatan telah membawa perubahan mendasar dalam strategi serangan terorisme. Pergeseran dari serangan bentuk manual tradisional ke serangan model otonom menunjukkan bagaimana kelompok teroris beradaptasi dengan inovasi teknologi untuk meningkatkan efektivitas, jangkauan, dan anonimitas operasi mereka.

Penggunaan drone berbasis AI memperkenalkan ancaman baru yang jauh lebih kompleks dibandingkan metode serangan konvensional, terutama melalui teknik serangan swarm, akuisisi target otomatis, serta potensi pembajakan sistem melalui serangan siber. Dalam konteks ini, negara-negara, termasuk Indonesia, harus mengantisipasi dan merespons dengan langkah-langkah strategis yang komprehensif. Penelitian ini juga menggarisbawahi bahwa saat ini terdapat keterbatasan signifikan dalam regulasi nasional dan internasional untuk mengontrol penggunaan teknologi ini secara efektif. Oleh karena itu, diperlukan revisi kebijakan keamanan nasional, pengembangan sistem pertahanan aktif terhadap drone, serta peningkatan kapasitas intelijen berbasis teknologi canggih.

Strategi kontra-terorisme di era drone dan AI harus mengedepankan deteksi dini, respons cepat, pelatihan berkelanjutan, kolaborasi lintas sektor, serta pemberdayaan masyarakat melalui kampanye edukasi yang intensif. Hanya melalui pendekatan yang adaptif, kolaboratif, dan berbasis inovasi teknologi, keamanan nasional dapat diperkuat dan ancaman terorisme berbasis teknologi modern dapat diantisipasi secara efektif. Penelitian ini diharapkan menjadi kontribusi awal untuk mendorong diskursus lebih lanjut mengenai pentingnya reformulasi strategi kontra-terorisme di era revolusi teknologi, serta menjadi dasar bagi penyusunan kebijakan yang lebih responsif dan antisipatif di masa depan. Penggunaan teknologi drone dan AI juga menyentuh ranah hukum dan etika, saran lain yang penting adalah melakukan kajian mendalam terhadap regulasi internasional yang ada, serta implikasi etis dari penggunaan teknologi yang sama oleh negara dan aktor non-negara.

DAFTAR REFERENSI

- Araque, O., & Iglesias, C. A. (2020). An approach for radicalization detection based on emotion signals and semantic similarity. *IEEE Access*, 8, 17877–17891. <https://doi.org/10.1109/ACCESS.2020.2967219>
- Buchelt, A., Adrowitzer, A., Kieseberg, P., Gollob, C., Nothdurft, A., Eresheim, S., Tschatschek, S., Stampfer, K., & Holzinger, A. (2024). Exploring artificial intelligence for applications of drones in forest ecology and management. In *Forest Ecology and Management* (Vol. 551). <https://doi.org/10.1016/j.foreco.2023.121530>

- Damoah, I. S., Ayakwah, A., & Tingbani, I. (2021). Artificial intelligence (AI)-enhanced medical drones in the healthcare supply chain (HSC) for sustainability development: A case study. *Journal of Cleaner Production*, 328. <https://doi.org/10.1016/j.jclepro.2021.129598>
- Dobson, T. K. (2015). Entropy and Self Organization: An Open System Approach to the Origins of Homeland Security Threats. *Homeland Security Affairs*.
- Downey, A. (2024). Algorithmic predictions and pre-emptive violence: artificial intelligence and the future of unmanned aerial systems. *Digital War*, 5(1–2), 123–133. <https://doi.org/10.1057/s42984-023-00068-7>
- Gettinger, D. (2020). The Drone Databook. *The Center for the Study of the Drone at Bard College*, 53(9), 1689–1699.
- Gruetzemacher, R., & Whittlestone, J. (2022). The transformative potential of artificial intelligence. *Futures*, 135. <https://doi.org/10.1016/j.futures.2021.102884>
- Hazenbergh, A., & Beridze, I. (2021). Artificial Intelligence and Robotics for Law Enforcement. *United Nations Interregional Crime and Justice Research Institute (UNICRI) The International Criminal Police Organization (INTERPOL)*.
- Johnson, J. (2019). Artificial intelligence & future warfare: Implications for international security. *Defense and Security Analysis*, 35(2), 147–169. <https://doi.org/10.1080/14751798.2019.1600800>
- Korteling, J. E. (Hans., van de Boer-Visschedijk, G. C., Blankendaal, R. A. M., Boonekamp, R. C., & Eikelboom, A. R. (2021). Human- versus Artificial Intelligence. *Frontiers in Artificial Intelligence*, 4. <https://doi.org/10.3389/frai.2021.622364>
- Lutfiani, N., Wijono, S., Rahardja, U., Iriani, A., Aini, Q., & Septian, R. A. D. (2023). A Bibliometric Study : Recommendation based on Artificial Intelligence for iLearning Education. *APTISI Transactions on Technopreneurship*, 5(2). <https://doi.org/10.34306/att.v5i2.279>
- Maguluri, L. P., Arularasan, A. N., & Boopathi, S. (2023). Assessing security concerns for ai-based drones in smart cities. In *Effective AI, Blockchain, and E-Governance Applications for Knowledge Discovery and Management*. <https://doi.org/10.4018/978-1-6684-9151-5.ch002>
- Mehta, P. L., Kalra, R., & Prasad, R. (2021). A Backdrop Case Study of AI-Drones in Indian Demographic Characteristics Emphasizing the Role of AI in Global Cities Digitalization. *Wireless Personal Communications*, 118(1). <https://doi.org/10.1007/s11277-020-08014-6>
- Özer, T., & Türkmen, Ö. (2023). Low-cost AI-based solar panel detection drone design and implementation for solar power systems. *Robotic Intelligence and Automation*, 43(6). <https://doi.org/10.1108/RIA-03-2023-0022>
- Rakhshandehroo, S., Duits, N., Bergman, D., Verkes, R. J., & Kempes, M. (2023). Psychopathology in female offenders of terrorism and violent extremism: a systematic review. In *Frontiers in Psychiatry* (Vol. 14). <https://doi.org/10.3389/fpsy.2023.1123243>

- Rawat, B., Bist, A. S., Apriani, D., Permadi, N. I., & Nabila, E. A. (2022). AI Based Drones for Security Concerns in Smart Cities. *APTISI Transactions on Management (ATM)*, 7(2). <https://doi.org/10.33050/atm.v7i2.1834>
- Shankar, A., Behl, A., Pereira, V., Chavan, M., & Chirico, F. (2024). Exploring enablers and inhibitors of AI-enabled drones for manufacturing process audits: A mixed-method approach. *Business Strategy and the Environment*, 33(5). <https://doi.org/10.1002/bse.3679>
- Slimani, H., El Mhamdi, J., & Jilbab, A. (2024). Assessing the advancement of artificial intelligence and drones' integration in agriculture through a bibliometric study. *International Journal of Electrical and Computer Engineering*, 14(1). <https://doi.org/10.11591/ijece.v14i1.pp878-890>
- Sorochkin, O., Sosulin, M., & Matveev, Y. A. (2024). Prospects of military aviation through the integration of uavs, ai and the latest technologies. *Communication, Informatization and Cybersecurity Systems and Technologies*, 1(6), 215–220. <https://doi.org/https://doi.org/10.58254/viti.6.2024.17.215>
- Susdarwono, E. T. (2021). Artificial Intelligence (Ai) Drone Dalam Pertahanan : Problem Dan Kemajuan. *Jurnal Ilmiah Intech : Information Technology Journal of UMUS*, 3(01).
- Taboada, I., Daneshpajouh, A., Toledo, N., & de Vass, T. (2023). Artificial Intelligence Enabled Project Management: A Systematic Literature Review. *Applied Sciences (Switzerland)*, 13(8). <https://doi.org/10.3390/app13085014>
- Trandberg Jensen, M., & Jensen, O. B. (2023). The Social Life of a Barrier: A Material Ethnography of Urban Counter-terrorism. *Space and Culture*, 26(1). <https://doi.org/10.1177/1206331220985445>
- Wang, L. (2023). AI-powered drone-based automated inspection of FAST. *Light: Science and Applications*, 12(1). <https://doi.org/10.1038/s41377-023-01094-6>
- Waqar, A., Othman, I., Hamah Sor, N., Alshehri, A. M., Almujiabah, H. R., Alotaibi, B. S., Abuhussain, M. A., Bageis, A. S., Althoey, F., Hayat, S., Benjeddou, O., Alsulamy, S. H., & Aljarbou, M. (2023). Modeling relation among implementing AI-based drones and sustainable construction project success. *Frontiers in Built Environment*, 9. <https://doi.org/10.3389/fbuil.2023.1208807>