Kontra-Terorisme Berbasis Teknologi, Mungkinkah?

written by Ahmad Khoiri

Harakatuna.com – Densus 88 kembali meringkus terduga teroris di Lombok Timur, NTB. Identitas rinci yang bersangkutan masih dirahasiakan. Namun, afiliasinya sudah terkonfirmasi, yakni Jama'ah Ansharud Daulah (JAD). Ini membuat banyak pihak terkejut. Selain karena lokasi penggerebekan dekat dengan pesantren NW yang notabene moderat, juga karena pertanyaan reflektif muncul, bagaimana strategi kontra-terorisme ke depan?

Penggerebekan, tentu saja, bukan hasil operasi grasah-grusuh. Densus 88 tidak akan beraksi kecuali telah melakukan tracking dan monitoring sebelumnya—dan mengurai persentase bahaya teroris itu sendiri. Karena itu, bagi sementara masyarakat yang sangsi atas terduga teroris, mereka mesti menyadari satu hal; sejumlah besar teroris JAD sudah tertangkap, dan mereka yang mendekam di penjara akan membocorkan jaringan-jaringannya. Ini rahasia umum.

Tetapi, mungkinkah kontra-terorisme dilakukan tanpa bantuan rekan teroris, atau eks-napiter, dan murni melalui kinerja integratif para *stakeholder* itu sendiri? Demikian karena cara konvensional terlihat monoton. Terlepas dari fakta bahwa

pendampingan eks-napiter itu penting, mereka tidak akan menjual informasi rahasia secara cuma-cuma. Artinya, butuh dana yang lumayan untuk mengorek info tersebut. Padahal, hari ini teknologi sudah canggih.

Di sisi lain, eks-napiter tidak selamanya bisa dijadikan sumber informasi. Suatu hari pasti ada *human error*, karena mereka sentimental. Pada saat sumber daya timbal balik tidak mereka dapatkan, apakah mereka masih bisa berkompromi? Atau justru berbalik haluan, atau bermain dua kaki, misalnya? Untuk alasan-alasan itulah, kontra-terorisme berbasis teknologi mesti diarusutamakan. Dengan kinerja serius, cara ini jauh lebih efektif dan efisien.

Berbasis Teknologi

Di era digital dan teknologi yang terus berkembang pesat, kelompok teroris semakin marak menggunakan *platform* daring dan media sosial sebagai alat diseminasi propaganda, rekrutmen ikhwan baru, serta rencana serangan. Karena itu, menjelajahi peran teknologi dalam kontra-terorisme merupakan hal yang urgen. Lalu, apa saja yang dapat dilakukan untuk merealisasikan hal tersebut? Sedikitnya ada lima langkah.

Pertama, deteksi dan monitoring online. Bagaimana teknologi bisa dimanfaatkan untuk mendeteksi dan memantau aktivitas terorisme di dunia maya? Penggunaan algoritma cerdas dan AI untuk mengidentifikasi pola perilaku dan konten yang mencurigakan, dalam hal ini, sangat *recommended*. Untuk strategi ini, lembaga penegak hukum dan intelijen memegang porsi utama dalam memantau dan menyelidiki kegiatan daring tersebut.

Kedua, kolaborasi dengan platform media sosial. Facebook, Instagram, TikTok dll itu dapat dijadikan mitra pemerintah untuk membantu memerangi propaganda teroris. Misalnya, dengan penghapusan konten yang berbau terorisme, memblokir akun-akun afiliasi teroris, dan melaporkan aktivitas yang mencurigakan—postingan kamuflase, misalnya—kepada pihak berwenang. Yang terakhir ini konteksnya adalah aduan masyarakat. Tentu, pengaduan itu juga secara online.

Ketiga, pencarian dan analisis data. Ini membantu dalam identifikasi pola dan tren terorisme. Ini boleh jadi legal atau bahkan ilegal, namun dalam rangka kontra-terorisme hukumnya legal. Langkah ini mencakup analisis *big data*, juga teknik *data mining* untuk menganalisis informasi dari sumber-sumber terbuka,

panggilan telepon, pesan teks, dan data elektronik lainnya. Tujuannya jelas: memahami jaringan terorisme dan memprediksi serangan potensial mereka.

Keempat, teknologi keamanan. Ini mirip adegan-adegan Hollywood, ketika teknologi seperti CCTV, pengenalan wajah, deteksi bahan peledak, dan pengamanan perbatasan dikerahkan untuk mengantisipasi serangan terorisme. *Kelima*, perlindungan data-privasi. Hal yang juga mesti diperhatikan ialah tantangan pengumpulan dan pemanfaatan data untuk keperluan kontra-terorisme. Menjaga privasi individu merupakan keniscayaan.

Mungkinkah Bisa?

Pertanyaannya adalah, apakah mungkin Indonesia mampu melakukan itu semua? Apakah sumber daya mendukung? Kontra-terorisme berbasis teknologi berurusan dengan *resources* yang canggih. Artinya, Indonesia mesti melihat juga potensi merealisasikannya. Menkominfo, dalam hal ini, sangat berandil besar. Sayangnya kinerja mereka sejauh ini belum optimal—untuk tidak mengatakan nihil kinerja. Kontra-terorisme justru jadi fokus aparat.

Karena itu, untuk memperbesar kemungkinan Indonesia mampu mengonter terorisme melalui teknologi, sumber daya juga perlu ditingkatkan. Teknik *spying* harus lebih daripada sekadar memanfaatkan tracking akun social media—sesuatu yang bisa dilakukan orang banyak. Intinya, di era keterbukaan informasi dan digitalisasi yang masif, kontra-terorisme tidak selaiknya hanya memanfaatkn informan eks-napiter belaka.

Hasil informasi dari mereka cenderung tebang pilih dan tidak merata. Sebagai contoh, investigasi terhadap eks-teroris JI, hasilnya jelas akan merugikan JAD. Begitu pun sebaliknya. Para teroris itu partisan. Mempercayai mereka seratus persen bukanlah ide bagus. Sudah saatnya dunia digital dimanfaatkan untuk kontra-terorisme. Seluruh resources mesti diarahkan ke situ. Hasilnya jelas lebih efektif dan merata, karena algoritmanya jelas dan teknologi itu tidak partisan.

Jadi, mungkinkah itu semua terjadi? Sangat mungkin, tergantung seberapa besar komitmen para *stakeholders* terhadap penanggulangan terorisme di satu sisi, dan seserius apa optimalisasi sumber daya di sisi lainnya. Kontra-terorisme berbasis teknologi, lagi pula, tidak bisa ditolak. Jika teknologi tidak dimanfaatkan untuk kontra-terorisme, ia akan dimanfaatkan untuk menyebarkan terorisme. Jadi, siapa yang mau selangkah lebih maju?

Wallahu A’lam bi ash-Shawab…