Urgensi Menguatkan Ketahanan Siber dari Propaganda Terorisme

written by Ahmad Khoiri

Harakatuna.com – Sekolah Kajian Stratejik dan Global Universitas Indonesia (SKSG UI) meluncurkan Policy Paper Kedaulatan Siber Indonesia, pada Senin (18/9) lalu. Kluster Riset SKSG UI mendorong pemerintah untuk memformulasikan landasan hukum yang kokoh dan permanen dalam menciptakan kedaulatan siber tanah air. Pasalnya, Indonesia menjadi negara peringkat keempat dengan pengguna internet terbesar di dunia.

Lalu apa masalahnya? Persoalannya ada pada aspek kerentanan ruang-ruang siber itu sendiri terhadap ancaman kedaulatan Indonesia. Tentu ancamannya kompleks, terutama berkaitan dengan politik. Namun salah satu yang disorot pada seminar tersebut ialah propaganda terorisme. Karena pemanfaatan ruang digital untuk mendiseminasi terorisme sudah masif di sejumlah negara, Indonesia mesti segera memitigasinya.

Sebenarnya, ketahanan siber tidak secara monolitis bermanfaat bagi kontra-radikalisasi dan ancaman terorisme. Ancaman siber yang riskan bagi negara memiliki implikasi serius terhadap keamanan nasional, ekonomi, dan stabilitas

masyarakat secara umum. Di antara jenis ancaman siber yang sangat berbahaya bagi Indonesia ialah serangan siber negara asing, atau yang dikenal sebagai *advanced persistent threats* (APTs).

Ada juga serangan terhadap infrastruktur kritis seperti sistem kelistrikan, air minum, transportasi, dan perbankan, seperti yang pernah terjadi di Iran. Ada juga serangan *ransomware* terhadap institusi pemerintah, seperti mengenkripsi data penting dan mengancam penghapusan kecuali dibayar dengan tebusan miliaran. Serangan ini mengindikasikan kegagalan keamanan data dan pencurian data sensitif.

Selain itu, ada serangan terhadap jaringan militer dan intelijen, juga serangan yang disebut *influence operations*. Ini ketika negara asing atau kelompok tertentu menggunakan dunia siber untuk memengaruhi politik dan opini publik negara lain, termasuk penyebaran disinformasi, propaganda, hingga pengacauan Pemilu. Semua dalam rumpun serangan internet dan komunikasi serta keamanan jaringan nasional (*cyber espionage*).

Teroris *Online*, Ada?

Di era digital ini, ketika dunia bak menyempit karena seluruh elemen telah terhubung satu sama lain, terorisme *online* jadi salah satu ancaman utama bagi keamanan global. Fenomena ini mencakup pemanfaatan internet dan media sosial oleh kelompok teroris untuk menebar propaganda, merekrut ikhwan teroris dan simpatisan terorisme, merencanakan serangan, serta memperluas jaringan mereka. Tak hanya di Indonesia tapi sedunia.

Memang ada? Jelas. Terorisme *online* telah berkembang pesat seiring dengan kemajuan teknologi dan internet. Kelompok teroris, seperti ISIS, Al-Qaeda, JI, JAD, dan lainnya, telah memanfaatkan media sosial, *website*, dan *platform* seperti *YouTube* sebagai alat menyebarkan ideologi ekstrem mereka. Mereka mengunggah video propaganda, materi rekrutmen-kaderisasi, hingga panduan serangan kepada audiens global.

Di Indonesia, secara khusus, dampak teroris *online* dapat terlihat dalam serangan *lone-wolf* yang terjadi di Mabes Polri beberapa tahun lalu. Zakiah Aini, pelaku, adalah teroris *online*, yang terpengaruh doktrin terorisme melalui media sosial di satu sisi, sekaligus menyebarkan keyakinan-keyakinan radikalnya tentang terorisme di internet di sisi lainnya. Namun, dalam kasus Aini, posisi dirinya

sebagai korban propaganda teroris *online*.

Lalu siapa teroris *online* yang sebenarnya? Yaitu sosok di balik *platform* yang berhasil meradikalisasi Aini. Dan tentu saja Aini bukan satu-satunya. Pelaku dan korban teroris *online* ibarat puncak gunung es—lebih banyak yang tidak mengemuka. Jika diselisik lebih jauh, pemanfaatan siber sebagai media propaganda terorisme tidak jauh dari fakta bahwa teroris tidak mau ambil risiko penangkapan, di samping efektivitasnya yang lebih besar.

Ancaman teroris *online* tentu saja tidak dapat disepelekan. Mereka melakukan rekrutmen global, memungkinkan kelompok teroris merekrut anggota baru mereka dari seluruh dunia. Mereka menggunakan media sosial dan pesan pribadi untuk menghubungi korban yang rentan secara emosional dan ideologis. Masih ingat ratusan WNI yang hendak hijrah ke Suriah beberapa tahun lalu? Itu bukti rekrutmen teroris secara *online* itu berhasil.

Harus diakui, internet mempermudah proses radikalisasi. Tak sulit untuk menyebarkan propaganda terorisme. Bahkan, teroris *online* menggunakan internet untuk berkomunikasi dalam merencanakan serangan. Seluruh pusat diseminasi propaganda juga sudah menggunakan jaringan siber. Semua itu jelas tidak bisa dibiarkan. Beberapa langkah mitigasi perlu segera ditempuh untuk menjaga kedaulatan Indonesia.

Langkah Mitigasi

Ada lima hal, jika mengelaborasi paparan dalam kajian SKSG UI kemarin dengan tantangan terorisme terkini. *Pertama*, monitor intelijen *online*. Ini tugas pemerintah, mulai dari BSSN, polisi siber, hingga BIN. *Kedua*, regulasi kebijakan. Kemenkominfo dapat ambil peran dalam langkah ini, bersama dengan masyarakat secara kolaboratif. *Ketiga*, kolaborasi internasional. Ini masih dalam konteks tugas serta peran pemerintah.

Keempat, penegakan hukum. Ini karena beberapa teroris melakukan pemanfaatan siber dalam propaganda mereka disebabkan lemahnya penegakan hukum, dan mereka menyadari peluang itu. *Kelima*, peran serta masyarakat. Selama ini kedaulatan siber hanya menjadi tugas pemerintah dan sama sekali tidak ada keterlibatan masyarakat di dalamnya. Padahal, masyarakat dengan keterampilan tertentu dapat menjadi mitra. Ini perlu disadari.

Menguatkan ketahanan siber adalah langkah penting untuk melindungi data, sistem, dan infrastruktur dari serangan siber yang berpotensi merusak. Pelakunya beragam, namun propaganda terorisme adalah yang paling dekat dengan masyarakat. Karenanya, langkah mitigasi adalah sesuatu yang niscaya. Kelima langkah tadi hanya uraian secara umum. Secara spesifik, Indonesia mesti melakukan berbagai upaya.

Upaya-upaya yang dimaksud ialah kepekaan terhadap keamanan, kebijakan keamanan siber, pemantauan dan deteksi dini, perimeter keamanan, pemutakhiran sistem dan *software*, *sandboxing* dan segmentasi jaringan, enkripsi data sensitif, manajemen akses yang ketat, pengelolaan kata sandi yang kuat, penyimpanan cadangan data, serta reaksi tanggap cepat terhadap insiden yang terjadi—aksi teror, misalnya.

Upaya lainnya yaitu mengaudit dan menilai keamanan secara teratur, kerja sama dengan pihak eksternal yang dapat dipercaya, kepemimpinan yang kuat dalam keamanan siber, serta pendidikan terus-menerus untuk masyarakat. Semua itu mesti dilakukan secara kontinu. Seluruh pihak harus menyadari bahwa menguatkan ketahanan siber adalah tugas yang tidak pernah selesai dan dinamis, sedinamis propaganda terorisme itu sendiri.

Wallahu A'lam bi ash-Shawab…