Journal of Terrorism Studies

Volume 3
Number 2 *Volume 3 Number 2 November 2021*

Article 5

11-11-2021

MEDIA, GLOBALISASI DAN ANCAMAN TERORISME

agung sukoco
Universitas Indonesia, agsuko37@gmail.com

Muhamad Syauqillah
Universitas Indonesia, muhamadsyauqillah@ui.ac.id

Asep Usman Ismail

Recommended Citation

sukoco, agung; Syauqillah, Muhamad; and Ismail, Asep Usman (2021) "MEDIA, GLOBALISASI DAN ANCAMAN TERORISME," *Journal of Terrorism Studies*: Vol. 3 : No. 2 , Article 5.
DOI: 10.7454/jts.v3i2.1039
Available at: https://scholarhub.ui.ac.id/jts/vol3/iss2/5

JOURNAL OF
Terrorism Studies

Media, Globalisasi & Ancaman Terorisme

Agung Sukoco
Kajian Terorisme Sekolah Kajian Stratejik dan Global Universitas Indonesia
agsuko37@gmail.com

Muhamad Syauqillah
Kajian Terorisme Sekolah Kajian Stratejik dan Global Universitas Indonesia
muhamadsyuaqillah@ui.ac.id

Asep Usman Ismail
Kajian Terorisme Sekolah Kajian Stratejik dan Global Universitas Indonesia
asep.usman@uinjkt.ac.id

Abstrak

Kemajuan ilmu pengetahuan dan tehnologi ternyata juga dimanfaatkan oleh kelompok teroris untuk menjalankan aksi mereka mulai dari propaganda, perekrutan, pelatihan, komunikasi, pengumpulan dana bahkan sampai dengan pencarian informasi dalam rangka penentuan target serangan aksi teror. Selain itu seiring dengan perubahan pola perekrutan maupun método aksi teror maka tidak menutup kemungkinan terhadap adanya serangan terorisme siber. Serangan terorisme siber ini akan mengarah kepada fasilitas vital yang terkait langsung dengan layanan publik. Aksi teror melalui serangan siber ini akan menimbulkan dampak yang lebih luas bahkan dapat merusak sistem suatu negara. Guna melawan terorisme siber ini maka yang harus digunakan yaitu kemampuan kontra terorime siber. Hal ini dapat dilakukan antara lain dengan patroli siber (dunia maya), penangkalan siber, penindakan siber maupun pengawasan siber.

Kata Kunci: Tehnologi, Siber, Terorisme

PENDAHULUAN

Ancaman terorisme saat ini menjadi ancaman serius bagi seluruh dunia, termasuk Indonesia. Perkembangan lingkungan strategis global telah menunjukkan bergesernya kecenderungan ancaman dan konflik yang terjadi dari *inter-state* menjadi *intra-state* . Hal ini disebabkan oleh kemajuan teknologi dan arus informasi yang sangat cepat dan menjadi faktor–faktor yang memaksa setiap negara harus menata kembali sistem pertahanan negaranya. Sistem pertahanan negara menjadi hal yang krusial dalam mewujudkan dan menjamin terjadinya stabilitas nasional yang mantap dan dinamis. Pertahanan negara Indonesia diselenggarakan dalam suatu sistem pertahanan yang bersifat semesta dengan memadukan pertahanan militer dan pertahanan nirmiliter. Kemajuan tehnologi

informasi juga dimanfaatkan oleh jaringan teroris untuk kepentingan aksinya.

Skenario terorisme siber di masa yang akan datang yaitu kelompok terorisme akan memanfaatkan jaringan internet sebagai media dan pusat kendali. Sebagai media di sini maksudnya adalah kelompok teroris ini memanfaatkan jejaring sosial sebagai sarana untuk berkomunikasi dengan anggota kelompoknya baik yang di dalam negeri maupun luar negeri. Di samping itu jejaring media sosial juga dimanfaatkan oleh kelompok teroris untuk melakukan propaganda dalam rangka merekrut anggota baru bahkan sampai dengan melaksanakan baiat dunia maya bagi anggota baru yang akan tergabung dalam jaringan terorisme. Selain memanfaatkan jaringan internet sebagai sarana komunikasi dan perekrutan, kelompok teroris juga memanfaatkannya untuk memberikan instruksi/kontrol kendali dari beberapa aksi teror. Instruksi tentang bagaimana merakit bom, menentukan sasaran maupun mekanisme pelaksanaan aksi teror juga diberikan melalui jaringan internet tersebut.

Peneliti dari Pusat Kajian Terorisme dan Konflik Sosial Universitas Indonesia, Solahudin mengatakan, media sosial mempercepat masuknya paham radikalisasi. Pendapat itu dikemukakan berdasarkan hasil riset yang ia lakukan 2017 lalu. Menurut Solahudin, media sosial terutama aplikasi pesan singkat membantu penyebaran paham radikal. Akan tetapi, rekrutmen anggota kelompok teror masih kerap dilakukan tanpa perantara media sosial (https://tirto.id/peneliti-terorisme-media-sosial-percepat-masuknya-paham-radikal-cKxx).

Perubahan pola yang dilakukan oleh kelompok radikal teroris yang mengikuti gaya milineal ini tentunya dimaksudkan untuk merekrut kalangan generasi muda sebanyak mungkin. Hal tersebut perlu mendapat perhatian serius dari semua pihak. Generasi muda adalah tahapan/periode pencarian jati diri yang cenderung labil emosinya dan selalu ingin tahu hal-hal yang dianggap baru. Di era sekarang ini generasi muda cenderung menjadikan dunia maya sebagai sumber referensi terhadap berbagai persoalan/kebimbangan yang ditemui termasuk di dalamnya terkait agama. Pada tahapan ini generasi muda menjadi rawan terhadap upaya perekrutan yang dilakukan oleh kelompok radikal teroris.

Di samping itu, perubahan pola pergerakan dengan pemanfaatan kemajuan tehnologi juga dilakukan ISIS dalam proses perekrutan anggota jaringan. Berbagai video tindakan kekerasan oleh ISIS terhadap musuh-musuhnya yang tersebar melalui media sosial ternyata menjadi

propaganda yang efektif untuk menarik pengikut baru dari seluruh dunia (Muhammad Luthfi Zuhdi; Imam Khomaeni Hayatullah, 2020, p. 23). Pemanfaatan media sosial juga dilakukan ISIS untuk meningkatkan peran perempuan dalam gerakan radikal terorisme. Dengan melalui *setting* dan *framing* informasi maka ISIS merekrut serta mengubah peran perempuan dalam gerakannya. Jika awalnya peran perempuan dalam gerakan terorisme masih bersifat tradisional hanya sebagai unsur pendukung dalam pergerakan terorisme, maka saat ini peran perampuan sudah mengalami peningkatan. Secara umum fungsi perempuan dalam kelompok ISIS yaitu sebagai kombatan atau petarung di garis depan, sebagai pengantin jihad baik dalam arti menikah dengan pejuang ISIS maupun pelaku serangan bom bunuh diri, serta fungsi sebagai koordinator pengumpul dana dan logistik (Wijaya, 2020). Fenomena tersebut tentu harus diwaspadai karena di dalam rumah tangga, perempuan adalah tokoh sentral dalam pengasuhan yang akan membentuk moral dan pola pikir dari seorang anak.

Pokok Masalah

Selain dimanfaatkan untuk tindakan kejahatan, ternyata kemajuan ilmu pengetahuan dan tehnologi khususnya di bidang siber juga dimanfaatkan oleh kelompok teroris untuk melancarkan aksinya. Pada era sekarang ini terorisme telah masuk ke sebuah fase yang disebut terorisme baru. Kelompok ini telah memanfaatkan kemajuan tehnologi seperti internet, handphone dan berbagai perangkat software untuk melaksanakan berbagai tindakan teror. Beberapa kegiatan yang dilakukan oleh kelompok teroris dengan memanfaatkan kemajuan tehnologi adalah propaganda, perekrutan dan pelatihan, pengumpulan dana, komunikasi dan penentuan target sasaran dari aksi teror. Dengan adanya keunggulan/keuntungan dari penggunaan media sosial ini maka kelompok radikal terorisme memanfaatkannya untuk beberapa kegiatan/aksi. Pemanfaatan dunia maya tersebut antara lain digunakan untuk pemberian informasi secara aktif tentang kegiatan mereka dalam rangka propaganda guna mendukung proses perekrutan secara langsung maupun tidak langsung melalui website dan media sosial. Pembentukan opini dengan memanfaatkan media sosial internet, melalui tulisan, gambar (meme) dan video, termasuk di dalamnya memberikan instruksi baik untuk perakitan bom maupun mobilisasi guna melakukan aksi teror dan ancaman-ancaman melalui internet. Dunia maya juga digunakan oleh kelompok radikal terorisme untuk pengumpulan dana dan tempat diskusi antara anggota kelompok tersebut. Di

samping itu kelompok radikal teroris juga melakukan perusakan (hacking) kepada situs-situs internet (website) milik negara/lembaga pemerintah.

Seiring kemajuan tehnologi maka tidak menutup kemungkinan teroris akan memanfaatkan media bukan hanya sebagai sarana perekrutan namun juga digunakan sebagai sarana teror itu sendiri. Dengan demikian yang menjadi persoalan adalah, sejauh mana penggunaan media untuk melakukan aksi terorisme dihadapkan dengan pengaruh globalisasi dimana menjadikan negara seperti tanpa batas (*borderless*)?

METODE DAN LANDASAN PEMIKIRAN

Metode penelitian dalam jurnal ini adalah kualitatif deskriptif dimana data diambil dari studi pustaka terhadap beberapa literatur yang terkait dengan materi pembahasan. Dalam merumuskan konsep untuk mengatasi pokok permasalahan di atas maka ada beberapa teori yang dapaat digunakan sebagai landasan pemikiran, antara lain sebagai berikut:

1. Keamanan Siber dalam Perspektif *People, Process, Technology.*

Menurut Fischer, keamanan siber adalah sebuah rangkaian aktifitas dan pengukuran yang dimaksudkan untuk melindungi dari serangan, disrupsi, atau ancaman yang lainnya melalui elemen-elemen *cyberspace* (*hardware, software, computer network*) (Islami, 2017). Berbicara keamanan siber berarti meliputi seluruh infrastruktur yang terkait di dalamnya baik infrastruktur lunak maupun keras. Yang dimaksudkan infrastruktur lunak adalah sumber daya alam yang mengawakinya serta kebijakan, proses maupun protokol dan pedoman yang terkait dalam keamanan siber. Sedangkan infrastruktur keras adalah keseluruhan tehnologi yang digunakan dalam keamanan siber baik berupa *software* maupun *hardware*.

2. Teori *Social Construction of Technology* (CSOT).

Menurut Trevor J. Pinch dan Wiebe E. Bijker, tehnologi tidak membentuk pola tindakan manusia, namun tehnologi justru lahir dari dari budaya masyarakat sebagai jawaban atas kebutuhan manusia (Pebrianti, Penyebaran Paham Radikal dan Terorisme dalam Media Internet, 2020). Jadi ilmu pengetahuan dan tehnologi pada dasarnya merupakan rekontruksi budaya melalui proses sosial. Dengan demikian pada dasarnya manusia adalah pencipta tehnologi sehingga perannya adalah sebagai pengendali dan bukan menjadi "budak teknologi". Karena sebagai pengendali maka manusia dapat memanfaatkan teknologi tersebut untuk

kebaikan dan sebaliknya dapat juga untuk keburukan/kejahatan.

3. Teori Ketergantungan Sistem Media.

Melvin Defluer dan Sandra Ball Roceach menyatakan bahwa semakin seseorang tergantung pada suatu media untuk memenuhi kebutuhannya maka media tersebut menjadi semakin penting untuk orang tersebut. (Pebrianti, Penyebaran Paham Radikal dan Terorisme dalam Media Internet, 2020). Kemudahan akses internet baik dalam hal sarana yang digunakan maupun kemudahan untuk diakses dari mana saja membuat orang semakin bergantung pada sistem media. Hal tersebut yang pada akhirnya mendorong semakin menguatnya kekuatan media massa dalam mempengaruhi khalayak ramai sehingga mampu menggambarkan peran media di dalam sistem sosial dan hubungan antara media dengan khalayak ramai tersebut.

HASIL DAN ANALISA

"Kita sedang dalam peperangan dan separuh lebih dari peperangan itu terjadi di media. Kita sedang dalam peperangan media demi merebut hati dan pikiran umat kita." Demikian Ayman al-Zawahiri, pemimpin Al-Qaeda pengganti Osama, pada 2005 menuliskan pesan kepada pimpinan Al-Qaeda di Irak (AQI), Abu Musab al-Zarqawi, tentang perubahan target dan pola terorisme kelompoknya (Huda, 2019, p. 5).

Dalam jurnal yang ditulis oleh Charlie Winter menyampaikan bagaimana sejak tahun 2014, ISIS aktif melaksanakan propaganda dengan mengusung ide kekhalifahan. Berbagai hukum yang berlaku di dalam kekhalifahan dengan jelas dipertontonkan sehingga di satu sisi menimbulkan ketakutan dan kemarahan tapi di sisi lain mampu menarik minat dari kelompok yang mengusung ideologi jihad dan khalifah. Dengan memanfaatkan perkembangan tehnologi internet maka propaganda yang dibuat menjadi tersebar dengan begitu bebas ke seluruh penjuru dunia.

Penggunaan internet sebagai sarana propaganda karena banyaknya kemudahan menjalankan aksinya dengan menggunakan internet tersebut. Melalui métode ini pesan propaganda yang disampaikan akan lebih cepat tersebar ke seluruh dunia dengan jangkauan wilayah yang lebih luas jika dibandingkan harus dilakukan secara manual. Selain itu dengan menggunakan internet ini maka target sasaran propaganda dapat lebih bervariasi dan tidak terbatas pada satu kelompok umur atau komunitas tertentu. Setelah penyebaran propaganda maka selanjutnya kelompok teroris akan memanfaatkan internet sebagai sarana perekrutan. Hal ini dijalankan secara

beriringan dengan aksi propaganda yang dilakukan. Saat penyebaran pesan propaganda secara tidak langsung dilakukan pemilahan dan perekrutan terhadap individu maupun kelompok masyarakat yang sudah terpengaruh dengan propaganda tersebut. Dengan menggunakan métode ini proses perekrutan menjadi lebih soft, tidak mudah terdeteksi namun dampaknya akan lebih parah karena bisa saja keberhasilan proses perekrutan akan terlihat secara menyeluruh di generasi penerus yang saat ini masih anak-anak ataupun remaja. Pemanfaatan kemajuan tehnologi selanjutnya oleh kelompok teroris yaitu untuk pelaksanaan pelatihan. Pada era sebelumnya, pelatihan dilakukan di kamp-kamp pelatihan yang ada di wilayah Timur Tengah maupun kantong-kantong kelompok teroris. Saat ini pelatihan cukup dilakukan dengan mengirimkan modul video sesuai materi yang akan dilatihkan. Sebagai contoh, *The Terrorist Handbook* yang berisi tentang tehnik pembuatan bom maupun *The Mujahadeen Poisons Handbook* yang mengajarkan tentang pembuatan bom kimia yang telah dibagikan dalam website kelompok teroris. Selanjutnya kemajuan tehnologi internet juga dimanfaatkan untuk pengumpulan dana. Dalam aksinya mereka membuat website yang di dalamnya terdapat pedoman untuk mengumpulkan dana sumbangan bagi pergerakan mereka. Website yang dibuat juga disamarkan sehingga tidak mudah terdeteksi oleh pihak berwajib. Selain itu mereka juga memanfaatkan internet dalam melaksanakan aktifitas atau usaha perekonomian yang hasilnya digunakan untuk membiayai aksi teror. Salah satu kasus yang pernah terjadi yaitu penggalangan dana melalui situs http://www.anshar.net. Situs tersebut sengaja didesain berdasarkan ide dari Nordin M Top untuk pengumpulan dana atau dikenal dengan istilah fai. Biaya untuk pembuatan domain situs tersebut juga menggunakan dana yang diperoleh dari tindakan kriminal di dunia maya. Kelompok teroris khususnya Imam Samudera pada saat itu berhasil merekrut seorang hacker meskipun belum sampai dengan taraf pembaiatan. Hacker yang dikenal sebagai Max Fiderman tersebut menggunakan metode *cracking* pada kartu kredit guna memperoleh sejumlah dana untuk kepentingan pembiayaan kegiatan kelompok teroris. Selain itu jaringan terorisme ini juga menggunakan kemajuan tehnologi internet untuk berkomunikasi di internal mereka. Pemanfaatan email, twitter, facebook ataupun web fórum menjadi hal yang rutin dilakukan dalam rangka berkoordinasi baik dalam rangka perencanaan maupun persiapan bahkan

sampai dengan pelaksanaan aksi teror. Pengendalian jaringan terorisme melalui media sosial tersebut pernah dilakukan oleh Imam Samudera pada saat masih ditahan di Lapas Krobokan Denpasar Bali. Meskipun dikendalikan secara online dari balik jeruji, namun ternyata Imam Samudera berhasil menggerakkan jaringannya untuk melakukan akasi teror yaitu peristiwa Bom Bali II pada tahun 2005. Penggunaan software yang terenkripsi maupun tehnik komunikasi rahasia lainnya tentu diterapkan sebagai bagian penting untuk menyembunyikan dari kemungkinan pendeteksian oleh pihak berwajib. Dalam merencanakan suatu aksi teror, dibutuhkan informasi yang lengkap terkait sasaran yang menjadi target aksi. Upaya memperoleh informasi yang dilakukan oleh kelompok teror saat ini sudah memanfaatkan kemajuan tehnologi internet. Sebagai contoh, mereka akan dengan mudah memperoleh informasi terkait rute yang akan digunakan dalam melaksanakan aksi hanya dengan mengakses *google map*. Di beberapa negara bahkan *blueprint* (cetak biru) sebuah bangunan/institusi telah tersedia di *website* (kanal) publik yang mudah diakses. Dengan demikian hal tersebut memberikan kemudahan mereka jika akan melakukan suatu aksi teror maupun sabotase terhadap fasilitas publik yang ditargetkan.

Selain pemanfaatan kemajuan tehnologi media untuk kepentingan propaganda dan perekrutan kelompok teroris, tidak meutup kemungkinan juga adanya serangan siber yang dilakukan oleh kelompok teroris terhadap fasilitas penting milik negara atau yang terkait kepentingan umum. Jika kelompok teroris memiliki kemampuan serangan siber maka aksi teror yang dilakukan akan menimbulkan dampak yang lebih luas bahkan mungkin sampai dengan menghancurkan sistem yang ada di suatu negara. Sebagai ilustrasi, jika teroris melakukan serangan siber sampai dengan pengambilalihan kendali terhadap fasilitas layanan distribusi air bersih, perbankan ataupun fasiliatas sarana komunikasi dan transportasi maka dapat dibayangkan situasi apa yang akan terjadi di masyarakat. Fasilitas air bersih merupakan kebutuhan vital dari masyarakat sehingga apabila hal tersebut terganggu maka dapat mengancam keselamatan manusia yang menggunakan fasilitas layanan air bersih tersebut. Demikian juga dengan perbankan, jika teroris melakukan serangan siber terhadap perbankan maka dapat dipastikan akan mengganggu sistem ekonomi dari negara tersebut dan dapat menimbulkan kepanikan masyarakat pengguna jasa perbankan. Sedangkan serangan siber terhadap layanan komunikasi dan transportasi akan dapat menyebabkan terjadinya kepanikan

masyarakat pengguna jasa komunikasi dan transportasi, bahkan dapat menimbulkan korban jiwa seandainya pengambilalihan kendali layanan transportasi tersebut menimbulkan kecelakaan yang disengaja sebagai bagian dari aksi teror. Serangan teror di dunia maya kepada fasilitas layanan publik bukan hanya berupa pengambilalihan kendali, namun dapat juga berupa serangan virus yang dapat mengganggu operasional sistem. Hal tersebut pernah terjadi di Indonesia pada tahun 2017 dimana beberapa rumah sakit mendapat serangan dari *ransomware WannaCry*. Akibat dari program jahat tersebut maka layanan medis di sejumlah rumah sakit menjadi terganggu. Hal ini perlu menjadi perhatian serius karena rumah sakit merupakan salah satu unit layanan publik yang sangat vital karena terkait aspek kesehatan sebagai salah satu kebutuhan pokok manusia.

Di negara lain serangan teror melalui dunia maya juga banyak terjadi di beberapa instansi pemerintah maupun swasta. NASA maupun Badan Pertahanan Amerika Serikat menjadi salah satu institusi yang pernah mengalami serangan siber. Akibat serangan tersebut sejumlah data maupun software berhasil diretas dan dicuri. Dari hasil pemeriksaan terhadap tokoh maupun aksi teror diketahui bahwa kelompok tersebut memanfaatkan fasilitas internet untuk berkomunikasi dan berkoordinasi terkait detail serangan terorisme.

Guna mencegah kemungkinan adanya serangan siber yang dilakukan oleh kelompok teroris maka perlu dibangun suatu sistem untuk mengamankan jaringan komputer yang ada di fasilitas-fasilitas penting terutama yang berhubungan langsung dengan layanan publik. Sistem yang dibangun harus memikiki kemampuan untuk mendetsksi secara dini adanya serangan siber kemudian secara cepat melokalisir dan menghancurkan ataupun menghentikan serangan siber tersebut. Dengan demikian sistem ini harus memiliki kemampuan untuk mencegah kemungkinan adanya serangan siber baik berupa *hacking* maupun sabotase kontrol kendali dari fasilitas vital tersebut.

Relevansi Dalam Konteks Indonesia

Menanggapi fenomena tersebut maka perlu dilakukan langkah-langkah pencegahan guna menghambat radikalisme di dunia maya. Langkah-langkah tersebut antara lain melakukan perlawanan narasi (*counter narrative*) terhadap propaganda yang disebarkan oleh kelompok radikal teror. Mencegah proses radikalisasi yang terjadi melalui media internet (radikalisasi online). Mencegah konten-konten negatif yang berupa provokasi, penyebaran kebencian, permusuhan, dan ajakan

kekerasan yang mengarah pada tindakan teror termasuk di dalamnya penyebaran berita bohong (hoaks). Membentengi masyarakat dari keterpengaruhan ideologi dan indoktrinasi kelompok teror melalui dunia maya. Meningkatkan pengetahuan masyarakat untuk menolak paham teror (terorisme) melalui kegiatan literasi media. Memperkaya khazanah pengetahuan masyarakat dengan perbandingan informasi yang kredibel dan konten edukatif yang mencerahkan. Menjalin sinergitas seluruh komponen bangsa, khususnya dengan para pegiat dunia maya, dalam mencegah penyebaran paham dan ideologi radikal.

Di era milenial sekarang ini maka pola ceramah keagamaan juga sebaiknya diubah. Pelaku teror yang sebalumnya identik dengan jenggot dan celana cingkrang sekarang sudah berubah sebagaimana diperlihatkan oleh para pelaku bom Sarinah. Ini menandakan bahwa pola gerakan teroris telah berubah mengikuti perkembangan situasi saat ini. Dengan demikian pola perlawanan terhadap penyebaran paham radikal terorisme juga sebaiknya diubah. Jika tausiah keagamaan selama ini dilakukan secara formal, maka saat ini sebaiknya dilakukan dengan pendekatan yang lebih informal. Jika sebelumnya lebih banyak mengunakan dalil naqli maka saat ini perlu juga diberikan porsi yang lebih untuk dalil aqli. Hal tersebut untuk mengimbangi pola penyesatan ajaran agama yang dibenturkan dengan logika berfikir. Selanjutnya kegiatan ceramah keagamaan yang sebelumnya banyak dilakukan di forum resmi dengan baju gamis maka perlu diubah dengan forum tidak resmi, bisa di mana saja dan pakaian yang digunakan juga lebih kasual. Hal ini dilakukan untuk menarik minat generasi milenial yang lebih sering mengakses ajaran agama dari internet yang kebenarannya masih diragukan bahkan menyesatkan. Pesan-pesan keagamaan dan perdamaian yang disampaikan juga harus lebih membumi dalam artian lebih menarik dan mudah dipahami. Ruang dakwah digital harus terus diisi dan dikembangkan untuk mengeliminir pengaruh propaganda kelompok terorisme yang berkembang di media sosial.

Langkah pencegahan terorisme siber tidak hanya terfokus kepada aspek tehnologi saja, tetapi juga harus didukung aspek lainnya antara lain aspek hukum, penyiapan kemampuan sumber daya manusia yang akan mengawaki sistem tersebut maupun hubungan kerja sama antar lembaga. Aspek hukum yang dimaksudkan yaitu adanya dukungan kebijakan dan regulasi terkait keamanan siber. Selain memberikan perlindungan hukum terhadap petugas yang melakukan kontra terorisme siber, aturan hukum ini

juga diharapkan mampu memberikan ketegasan penindakan hukum terhadap pelaku terorisme siber. Sering terjadi beberapa uanggahan di media sosial yang mengandung konten radikal terorisme namun tidak bisa diambil tindakan secara cepat. Hal ini terjadi karena masih ada keraguan terkait dasar hukum yang akan digunakan dalam penindakan tersebut. Di samping itu, masih sering terjadi perdebatan dalan penentuan sebuah konten apakah sudah dapat digolongkan sebagai propaganda, radikal, terorisme atau baru merupakan sebuah pemikiran. Celah-celah seperti ini yang selalu dimanfaatkan oleh jaringan terorisme untuk melakukan propaganda guna merekrut maupun mencari pembenaran atas segala bentuk aksi mereka.

Langkah selanjutnya yaitu meningkatkan kemampuan dari sumber daya manusia yang mengawaki sistem yang ada di fasilitas vital terkait dengan layanan publik. Peningkatan kemampuan di sini meliputi pengetahuan mendeteksi potensi adanya serangan siber dan mampu melakukan langkah-langkah pencegahan untuk melokalisir dampak kerusakan akibat dari serangan siber tersebut. Di samping kemampuan deteksi, personel yang mengawaki sebuah sistem jaringan vital juga diharapkan memiliki kemampuan melakukan tindakan balasan terhadap serangan siber. Selain itu yang penting adalah menumbuhkan kewaspadaan untuk tidak sembarangan mengunduh suatu program karena tidak menutup kemungkinan hal tersebut merupakan awal masuknya serangan siber.

Kemudian langkah yang tidak kalah pentingnya dalam pencegahan serangan terorisme siber adalah kerja sama antar lembaga. Hal tersebut dilakukan untuk memastikan bahwa pola penanganan serangan terorisme siber dilaksanakan secara terpadu dan terkoordinasi. Jika tidak dilakukan secara terkoordinasi maka tidak menutup kemungkinan justru akan menyebabkan terjadinya saling serang antar sistem jaringan karena memang sengaja diarahkan atau ditimbulkan oleh kelompok penyerang siber.

Langkah-langkah pencegahan yang telah disebutkan di atas sifatnya adalah untuk meminimalisir penyebaran paham radikal terorisme namun tidak menghilangkan keberadaannya di dunia maya. Dengan demikian diperlukan langkah yang lebih aktif untuk menangkal pemanfaatan dunia maya oleh kelompok terorisme. Langkah kontra terorisme siber yang dapat dilakukan yaitu melalui patroli siber (dunia maya), penangkalan siber, penindakan siber maupun pengawasan siber. Langkah tersebut dilakukan guna mengeliminir pemanfaatan jejaring media

sosial oleh kelompok terorisme untuk melakukan propaganda, perekrutan, komunikasi antar anggota jaringan maupun penggalangan dana.

Patroli siber dilaksanakan untuk memonitor keberadaan dan aktifitas situs online yang menyebarkan faham radikal terorisme. Dalam patroli siber ini juga dapat ditujukan untuk mengetahui ada tidaknya pengikut baru yang berhasil direkrut oleh kelompok teroris. Pelaksanaan patroli siber ini harus dilakukan secara meluas ke seluruh lapisan masyarakat termasuk di dalamnya adalah kepada para ASN, TNI-Polri maupun pegawai BUMN. Hal ini penting dilakukan karena terkadang di dunia nyata kelompok ini tidak menunjukkan bahwa sudah terpengaruh oleh ideologi radikal terorisme karena terikat dengan aturan. Akan tetapi di dunia maya, keterpengaruhan tersebut akan terlihat nyata karena mereka merasa aman. Setelah dilaksanakan patroli siber dan ditemukan adanya warga masyarakat maupun ASN, TNI-Polri atau pegawai BUMN yang terpengaruh faham radikal terorisme maka selanjutnya dilakukan pembinaan kepada yang bersangkutan.

Selain patroli siber maka langkah aktif yang dapat dilakukan berikutnya ada penangkalan siber. Penangkalan siber ini lebih diutamakan kepada sistem jaringan yang digunakan oleh fasiltas vital. Di dalam langkah ini maka dibuat sebuah sistem ataupun mekanisme yang memiliki kemampuan untuk mendeteksi setiap upaya serangan siber terhadap jaringan vital tersebut. Selain memiliki kemampuan mendeteksi maka diharapkan sistem yang dibuat juga memiliki ketahanan untuk menangkal setiap serangan siber yang ditujukan kepada fasilitas vital tersebut. Jika sistem yang dibangun belum mampu secara maksimal dalam menangkal serangan siber terorisme, maka paling tidak sistem ini mempunyai kemampuan untuk mengeliminir dan melokasir serangan siber terorisme tersebut sehingga tidak merusak jaringan yang memiliki fungsi vital.

Tindakan aktif berikutnya adalah penindakan siber. Langkah ini merupakan upaya agresif terhadap keberadaan siber terorisme. Dalam penindakan siber maka sistem yang dibangun memiliki kemampuan untuk melawan bahkan sampai dengan melakukan serangan balik terhadap aktifitas siber terorisme. Penindakan siber ini juga mempunyai kemampuan yang lebih serius di antaranya sampai dengan pemblokiran/pemutusan akses ke situs tertentu. Selain itu pada langkah penindakan siber ini dilengkapi dengan kemampuan dan kewenangan untuk mengungkap data admin dari sebuah situs yang terlibat jaringan radikal terorisme maupun yang melakukan serangan siber.

Dengan adanya kemampuan dan kewenangan tersebut maka dapat digunakan sebagai data awal dalam rangka langkah penegakan hukum oleh instansi terkait.

Semua langkah tindakan di atas baik yang sifatnya pencegahan maupun yang bersifat aktif mempunyai tujuan untuk menghilangkan radikalisasi online maupun siber terorisme. Langkah tindakan yang diambil tersebut dapat dipastikan tidak mudah untuk dilaksanakan. Tindakan menghilangkan radikalisasi online tersebut khususnya yang bersifat aktif tentunya akan menimbulkan protes/ditentang oleh para aktifis demokrasi karena dinilai bertentangan dengan hak kebebasan berpendapat. Protes tersebut adalah wajar terjadi di era demokrasi seperti sekarang ini, namun tidak boleh menyurutkan upaya penghentian fenomena radikalisasi online. Pemerintah seharusnya tidak boleh ragu-ragu dalam mengambil langkah pemblokiran/pemutusan akses terhadap situs yang melakukan siber terorisme, menyebarkan propaganda dan ajaran faham radikal terorisme maupun yang terlibat dalam pengumpulan dana untuk jaringan terorisme. Hal ini dikarenakan langkah tindakan tersebut sudah diatur dalam Pasal 40 Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Di sinilah perlunya kerja sama dan kepedulian semua pihak dan lembaga terkait untuk mendukung langkah pemerintah dalam mengambil tindakan tegas terhadap situs yang terlibat dalam jaraingan terorisme. Dukungan tersebut diimplementasikan secara lebih luas dalam bentuk keikutsertaan untuk memberikan pemahaman kepada khalayak ramai tentang pentingnya langkah yang telah diambil oleh pemerintah.

Guna mengeliminir adanya protes dari para penggiat demokrasi maupun menghindari kemungkinan adanya penyalahgunaan wewenang, maka dapat dibentuk sebuah badan/lembaga ad hoc yang bertugas menganalisa suatu situs/konten. Badan/lembaga ad hoc inilah nantinya yang akan mengeluarkan rekomendasi jika ada situs/konten yang memuat paham radikal maupun berafiliasi dengan jaringan terorisme termasuk diantaranya sebagai sarana pengumpulan dana. Untuk menjaga kredibilitas badan/lembaga ad hoc tersebut maka dipilih dari orang yang menguasai agama, ahli hukum, ahli tehnologi informasi dan ahli bidang profesi terkait lainnya. Efektifitas dari lembaga tersebut juga sangat tergantung dari kemampuan personel yang ada di dalamnya untuk bekerja sama. Dalam hal ini mereka harus

menanggalkan kepentingan kelompok yang diwakilinya dan benar-benar berprinsip bahwa segala hal yang mereka kerjakan adalah untuk kebaikan umat manusia melalui pencegahan penyebaran faham radikal terorisme. Dengan adanya langkah tersebut maka diharapkan radikalisasi online bukan hanya dapat diminimalisir penyebarannya tetapi juga dapat dihilangkan dari dunia maya.

PENUTUP

Dari keseluruhan uraian di atas dapat disimpulkan bahwa kemajuan ilmu pengetahuan dan tehnologi ternyata juga dimanfaatkan oleh kelompok teroris untuk menjalankan aksi mereka mulai dari propaganda, perekrutan, pelatihan, komunikasi, pengumpulan dana bahkan sampai dengan pencarian informasi dalam rangka penentuan target serangan aksi teror. Selain itu seiring dengan perubahan pola perekrutan maupun metode aksi teror maka tidak menutup kemungkinan terhadap adanya serangan terorisme siber. Aksi teror sabotase yang dilakukan di dunia maya baik melalui pengiriman virus maupun pengambilalihan kontrol kendali dari sebuah sistem jaringan akan berdampak sangat luas di masyarakat. Guna melawan penggunaan dunia maya oleh terorisme ini maka yang harus digunakan yaitu kemampuan kontra terorime siber. Langkah tersebut ada yang sifatnya lebih mengarah kepada upaya pencegahan dan ada juga yang sifatnya aktif. Langkah-langkah tersebut antara lain melakukan perlawanan narasi (*counter narrative*) terhadap propaganda kelompok radikal terorisme, mencegah proses radikalisasi yang terjadi melalui media internet (radikalisasi online), mencegah konten-konten negatif yang berupa provokasi, penyebaran kebencian, permusuhan, dan ajakan kekerasan termasuk di dalamnya penyebaran berita bohong (hoaks), membentengi masyarakat dari keterpengaruhan ideologi dan indoktrinasi kelompok teror melalui dunia maya, meningkatkan pengetahuan masyarakat untuk menolak paham teror (terorisme), memperkaya khazanah pengetahuan masyarakat dengan perbandingan informasi yang kredibel dan konten edukatif yang mencerahkan serta menjalin sinergitas seluruh komponen bangsa dalam mencegah penyebaran paham dan ideologi radikal. Langkah pencegahan terorisme siber tidak hanya terfokus kepada aspek tehnologi beserta kontennya saja, tetapi juga harus didukung aspek lainnya antara lain aspek hukum dalam arti perlunya landasan hukum yang dapat digunakan oleh pihak berwenang dalam penanggulangan terorisme siber, penyiapan kemampuan sumber daya manusia yang akan mengawaki sebuah sistem jaringan

tehnologi khususnya yang bersifat vital maupun hubungan kerja sama antar lembaga dalam pencegahan terorisme siber. Langkah tindakan bersifat aktif dalam pencegahan terorisme siber yang dapat dilakukan antara lain dengan patroli siber (dunia maya), penangkalan siber, penindakan siber maupun pengawasan siber. Berbagai langkah tersebut kemungkinan besar akan mendapat protes atau ditentang oleh aktifis demokrasi karena dianggap mengekang kebebasan dan melanggar HAM. Guna menghilangkan keragu-raguan terhadap tindakan blokir, pemutusan akses maupun take down dan tindakan hukum lainnya atas sebuah konten atau akun di media sosial, maka dapat dibentuk sebuah badan/lembaga ad hoc. Badan/lembaga ini terdiri dari gabungan beberapa tokoh berkompeten sesuai bidangnya yang bertugas untuk menilai apakah sebuah konten maupun akun di media sosial mengandung unsur radikal terorisme ataupun masuk ke dalam jaringan terorisme. Dari hasil penilaian tersebut akan digunakan oleh pihak berwajib untuk mengambil langkah tindakan yan sesuai dengan aturan perundangan yang berlaku. Keseluruhan langkah tersebut dilakukan guna mengeliminir pemanfaatan jejaring media sosial oleh kelompok terorisme untuk melakukan propaganda, perekrutan, komunikasi antar anggota jaringan maupun penggalangan dana.

DAFTAR PUSTAKA

Buku

Barry Buzan, Ole Waever, Jaap de Wilde. (1998). *Security A New Framework for Analysis.* Colorado: Lymne Rienner Publishers, Inc.

Creswell, J. (2013). *Research Design-Pendekatan Kualitatif, Kuantitatif dan Mixed.* California: Pustaka Pelajar.

Dr. Mukhammad Ilyasin, M.Pd; Dr. M. Abzar D., M.Ag; Mohammad Kamaluddin, M.Si. (2017). *Teroris dan Agama.* Jakarta: Kencana Prenadamedia Group.

Drs. Yustinus Semiun, M. O. (2018). *Teori-teori Kepribadian Behavioristik.* Sleman: PT Kanisius.

Gray, C. S. (2007). *War, Peace and International Relations.* Canada: Routledge.

Hendropriyono, A. (2020). *Terorisme Fundamentalis Kristen, Yahudi, Islam.* Jakarta: PT. Kompas Media Nusantara.

Lubis, D. A. (2014). *Filsafat Ilmu, Klasik Hingga Kontemporer.* Depok: PT. Rajagrafindo Persada.

Osinga, F. P. (2007). *Science, Strategy and War.* New York: Routledge.

Robin H. Gurwitch Phd, Betty Pfefferbaum MD, JD & Michael J.T. Leftwich. (2002). The Impact of Terrorism on Children. *Journal of Trauma Practice*.

Sandole, D. J. (2007). *Peace and Security in the Postmodern World.* New York: Routledge.

Sindhunata. (2020). *Teori Kritis Sekolah Frankfurt.* Jakarta: PT. Gramedia Pustaka Utama.

Soekanto, S. (2000). *Sosiologi Suatu Pengantar*. Jakarta: PT Raja Grafindo Persada.

Sugiyono, P. (2012). *Metode Penelitian Kuantitatif, Kualitatif dan R & D.* Bandung: CV Alfabeta.

Prof. Dr. Irfan Idris, M. (2018). *Deradikalisasi; Kebijakan, Strategi dan Program Penanggulangan Terorisme.* Yogyakarta: Cahaya Insani.

Williams, P. D. (2008). *Security Studies: An Introduction.* New York: Routledge.

Jurnal

Adkins, G. (2013). Red Teaming teh Red Team: Utilizing Cyber Espionage to Combat Terrorism. *Strategic Security*.

Arianti, V. (2018). Participation of Children in Terrorist Attack in Indonesia. *Counter Terrorist Trends and Analyses*.

Aryo C.K. Wardana, Rodon Pedrason, Triyoga Budi Prasetyo. (2018). Implementasi Digital Forensik Brunei Darussalam dalam Membangun Keamanan Siber. *Jurnal Prodi Perang Asimetris*.

Baldwin, D. A. (1997). The Concept of Security. *International Studies*, 5-26.

Carter, A. B. (2001). The Architecture of Government in the Face of Terrorism. *International Security*, 5-23.

Cerny, P. G. (2005). Terrorism and the New Security Dilemma. *Naval War College Review*.

Huda, A. Z. (2019). Melawan Radikalisme Melalui Kontra Narasi Online. *Journal of Terrorism Studies*, 1-15.

Islami, M. J. (2017). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Pemilaian Global Cybersecurity Index. *Masyarakat Telematika dan Informasi*, 137-144.

Keating, M. G. (2005). The Machinery of Australian National Security Policy. *Autralian Defence Forces Journal*.

Mahturai Rian Fitra; Arthur Josias Simon Runturambi. (2020). Implementation of Smartphone Navigation Features by Combined Forces in Determining The Hazards of Terrorism in Poso. *Journal of Terrorism Studies*, 1-8.

Meredith Box, Gavan McCormack. (2004). Terror in Japan: The Red Army (1969-2001) and Aum Supreme Truth (1987-2000). *The Asia-Pacific Journal*.

Muhamad Syauqillah, Ph.D; I Esti Suyanti, M.Pd. (2020). Proceedings Homeland Security Conference 2020. *Homeland Security Conference 2020.* Jakarta: Pusat Riset Sekolah Kajian Stratejik dan Global Universitas Indonesia.

Muhamad Syauqillah; Marella Al Faton. (2019). Transmission of Global and Regional Extrimism in Indonesia. *Journal of Terrorism Studies*, 1-17.

Muhammad Luthfi Zuhdi; Imam Khomaeni Hayatullah. (2020). Narrative for Terrorism and Transnationalism ISIS Theology Through The Doctrine of Religion. *Journal of Terrorism*, 20-31.

Nasrullah, R. (2012). Politik Siber dan Terorisme Virtual. *Esensia*.

Pebrianti, A. (2020). Penyebaran Paham Radikal dan Terorisme dalam Media Internet. *Sosiologi*, 73-80.

Wardani, L. A. (2018). Analisis Implementasi Kerja Sama Filipina dan Amerika Serikat dalam Penanggulangan Aksi Terorisme di Filipina. *Journal of International Relations*.

Wijaya, T. I. (2020). Peran manipulasi Informasi Terhadap Keikutsertaan Perempuan Dalam Gerakan Terorisme. *Journal of Terrorism Studies*, 94-113.