Cyberterrorism Threats in Indonesia and State Responses

Ancaman *Cyberterrorism* di Indonesia dan Respons Negara

I Putu Hadi Pradnyana (*)

Sekolah Kajian Strategik dan Global Universitas Indonesia
Jalan Salemba Raya No. 4
Jakarta

Muhammad Syaroni Rofii

Sekolah Kajian Strategik dan Global Universitas Indonesia
Jalan Salemba Raya No. 4
Jakarta

Abstract

This article intend to elaborate the threats from cyberterrorism in Indonesia and the anticipation or response made by the state. That tactically, terrorist groups have made various changes and adjustments to launch a plan of terror action. When a target is deemed to be highly secure and difficult to penetrate, the terrorist group then carries out a series of tactical evolutions targeting more vulnerable targets. This praxis is shown in the practices of terrorism that have changed during the last hundred years until now it has adapted to a form of cyberterrorism. This research uses qualitative methods and types of phenomenology. The phenomenon of cyberterrorism is linked to the threat in Indonesia and the government's response to anticipating this problem. The research result shows that most of the terrorist groups in the world, including in Indonesia, have used cyber means to attack certain targets. In responding to cyberterrorism crimes, Indonesia has made several efforts to tackle cyberterrorism through the establishment of special agencies and strengthening regulations. However, there are still things that need to be addressed in order to strengthen the national security system from the threat of cyberterrorism.

Keywords: *industrial revolution 4.0, cyberterrorism, Indonesia*

Abstrak

Penelitian ini bertujuan untuk mengelaborasi ancaman-ancaman yang dapat ditimbulkan dari *cyberterrorism* di Indonesia danantisipasi atau respons yang dilakukan negara. Bahwasanya secara taktikal, kelompok-kelompok teroris telah melakukan berbagai perubahan dan penyesuaian untuk melancarkan rencana aksi teror. Saat target dianggap memiliki keamanan tinggi dan susah ditembus, kelompok teroris kemudian melakukan serangkaian evolusi taktik yang mengarah pada target yang lebih rentan. Praksis ini ditunjukkan dalam praktik-praktik terorisme yang berubah selama seratus tahun terakhir hingga sekarang beradaptasi ke bentuk *cyberterrorism*. Penelitian ini menggunakan metode kualitatif dan jenis fenomenologi. Fenomena *cyberterrorism* dikaitkan dengan ancamannya di Indonesia serta respons pemerintah dalam mengantisipasi masalah tersebut. Hasil penelitian adalah sebagian besar kelompok teroris di dunia termasuk di Indonesia, telah menggunakan sarana siber untuk menyerang target-target tertentu. Dalam merespons kejahatan *cyberterrorism*, Indonesia telah melakukan beberapa upaya dalam menanggulangi *cyberterrorism* baik melalui pembentukan instansi-instansi khusus maupun penguatan regulasi. Namun masih ada hal-hal yang harus dibenahi guna memperkuat sistem keamanan nasional dari ancaman *cyberterrorism*.

Kata kunci: *revolusi industri 4.0, cyberterrorism, Indonesia*

(*) Corresponding Author: hadypradnyana@gmail.com

PENDAHULUAN

Pesatnya arus globalisasi dan liberalisasi pasca Perang Dingin, berpengaruh signifikan terhadap mudahnya perpindahan manusia, barang, dan informasi. Fenomena ini turut membawa gelombang revolusi industri 4.0. Pada dasarnya, revolusi industri 4.0 menekankan pada sebuah sistem yang disebut *cyber physical systems* (CPS) yaitu integrasi jaringan, proses fisik, dan komputer yang terkoneksi erat dengan internet (Dawson, 2018). Dengan kata lain, revolusi industri 4.0 berkaitan pada penggunaan teknologi digital dalam berbagai bidang.

Dinamika gelombang revolusi industri telah mempengaruhi berbagai faktor kehidupan sejak puluhan tahun lalu. Sebelum sampai pada revolusi industri 4.0, dunia telah melewati fase revolusi industri 1.0, 2.0, 3.0, dan saat ini 4.0. Secara garis besar, revolusi industri 1.0 menekankan pada penggunaan air dan uap sebagai tenaga penggerak alat-alat produksi dan transportasi. Dilanjutkan dengan revolusi industri 2.0 pada awal abad ke-20, yang mulai menggunakan tenaga listrik dan gencarnya produksi massal di berbagai bidang. Kemudian pada 1970-an dikenal sebagai era revolusi industri 3.0 yang menghasilkan kombinasi teknologi informasi dan elektronik untuk menjalankan berbagai produksi. Kini dunia mengalami era revolusi industri 4.0 yang menekankan pada penggunaan teknologi digital dalam berbagai bidang. Era revolusi industri 4.0 turut meminimalisasi batas antara industri, teknologi, dunia fisik, dan ruang digital atau siber (Medium, 2018). Guna menyederhanakan fenomena revolusi industri, berikut ilustrasi gelombang revolusi industri 1.0 hingga 4.0.

Four Phases of Industrialization

Sumber: Medium (2018)

Gambar 1. Gelombang revolusi industri

Ruang siber atau *cyberspace* menjadi entitas baru yang dibawa oleh Revolusi Industri 4.0. Pada era ini, *cyberspace* seakan menghilangkan batas-batas fisik. Manusia dengan mudah berinteraksi dengan manusia lain yang secara geografis jaraknya jauh. Akses informasi menjadi semakin cepat dan bebas sehingga memudahkan penyebaran berbagai konten dalam ranah *cyberspace*. Banyak dampak positif yang dihasilkan dari Revolusi Industri 4.0, terutama di bidang ekonomi, teknologi, kesehatan, dsb. Namun disisi lain, Revolusi Industri 4.0 turut memberi dampak negatif. Eskalasi ancaman menjadi semakin kompleks khususnya dalam ranah *cyberspace*. Salah satu ancaman dari era Revolusi Industri 4.0 adalah terorisme di ruang siber atau dikenal sebagai *cyberterrorism*. Sebelum menuju pada analisis ancaman *cyberterrorism* tersebut, tulisan ini akan membahas dahulu mengenai potensi ancaman atas *cyberspace* dan perlunya strategi *cybersecurity*.

Salah satu konsekuensi dari Revolusi Industri 4.0 adalah permasalahan keamanan nasional di ruang siber atau *cyberspace* yang dihadapi negara. Berbagai aktivitas manusia kini tidak dapat dilepaskan dari ranah dunia maya yang kemudian disebut *cyberspace*. Secara definitif, *cyberspace* berarti jaringan infrastruktur teknologi informasi yang saling tergantung, mencakup internet, jaringan telekomunikasi, dan sistem komputer (National Initiative for Cybersecurity Careers and Studies, 2018). Dengan kata lain, segala aktivitas di ruang internet atau dunia maya termasuk dalam ranah *cyberspace*. Perkembangan teknologi informasi yang dipengaruhi Revolusi Industri 4.0 telah memberi konsepsi baru atas dunia tanpa batas. Dalam arti bahwa perpindahan manusia, barang, dan informasi semakin bersifat *borderless*.

Potensi ancaman sebuah negara bertambah dengan perkembangan aktivitas dalam *cyberspace*. Mengingat sebelum era Revolusi Industri 4.0 negara-negara cenderung berfokus pada keamanan yang bersifat konvensional dan *tangible*. Timbulnya sebuah kondisi ketergantungan manusia terhadap *cyberspace* terutama melalui internet, membuka potensi ancaman yang berbahaya dalam berbagai bidang. *Cyberspace* menjadi arena baru atas tindakan-tindakan kriminal dengan motif yang beragam. Ancaman yang ditimbulkan tersebut membuat negara-negara harus mengambil strategi tepat, sebagai upaya melindungi masyarakat dalam ruang siber. Memperkuat pertahanan dan keamanan dalam *cyberspace* menjadi tantangan negara agar bisa menangkal berbagai potensi ancaman yang dapat terjadi melalui *cyberspace*.

Kondisi tersebut mengakibatkan perlunya langkah-langkah komprehensif di bidang keamanan siber atau *cybersecurity*. Merujuk pada definisi yang disampaikan United States National Initiative for Cybersecurity Careers and Studies (NICCS), keamanan siber atau *cybersecurity* merupakan proses, kapabilitas, dan kegiatan melindungi keamanan sistem informasi serta komunikasi dari ancaman kerusakan, modifikasi ilegal, dan eksploitasi dalam ranah *cyberspace*. Lebih lanjut, *cybersecurity* mencakup tentang strategi, kebijakan, dan standar keamanan maupun operasi dalam *cyberspace* atau dunia maya. Maka diperlukan upaya-upaya pengurangan ancaman, pencegahan, keterlibatan internasional, respons insiden, ketahanan, dan aktivitas pemulihan. Hal ini meliputi operasi jaringan komputer, jaminan informasi, penegakan hukum, diplomasi, militer, dan misi intelijen yang berkaitan dengan keamanan serta stabilitas infrastruktur informasi maupun komunikasi global (National Initiative for Cybersecurity Careers and Studies, 2018). Dengan demikian, *cybersecurity* menekankan pada segala aktivitas atau kegiatan yang bertujuan memberikan proteksi terhadap masyarakat di ranah *cyberspace*.

Revolusi Industri 4.0 memberi warna baru dalam paradigma keamanan nasional melalui *cybersecurity*. Isu keamanan siber bersifat sangat kompleks karena memerlukan keterlibatan berbagai sektor dalam penanganannya atau disebut transdisipliner. Berbagai institusi yang dimiliki negara dituntut untuk berkolaborasi guna menciptakan strategi-strategi *cybersecurity* yang mampu melindungi keamanan masyarakat di bidang *cyberspace* (Goutam, 2015). Serangan atau ancaman yang dapat ditimbulkan dari *cyberspace* sangat variatif. Luasnya celah yang dapat dimanfaatkan oleh pihak-pihak tertentu untuk menimbulkan ancaman di ranah *cyberspace* melatarbelakangi digunakannya ruang ini sebagai arena aksi mereka. Salah satu bentuk ancaman yang ditimbulkan adalah *cyberterrorism*. Artikel ini membahas lebih lanjut mengenai *cyberterrorism* dan ancamannya di Indonesia.

METODE

Artikel ini menggunakan metode penelitian kualitatif dengan jenis penelitian fenomenologi. Metode penelitian kualitatif tepat digunakan untuk meneliti fenomena-fenomena sosial tertentu berdasarkan pengamatan dari peneliti. Definisi fenomenologi menurut Alase (2017) adalah sebuah metodologi kualitatif yang menggiring peneliti menerapkan dan mengaplikasikan kemampuan subjektivitas dan interpersonalnya dalam proses penelitian eksploratori. Dengan kata lain, fenomenologi dapat digunakan dalam menganalisis suatu fenomena terkini dan dikaitkan dengan objek tertentu. Dalam hal ini, fenomena Revolusi Industri 4.0 dan *cyberterrorism* menjadi fokus penelitian yang dikaitkan dengan ancamannya di Indonesia serta respons pemerintah.

Sumber data yang digunakan bersifat sekunder, yang berarti pengamatan melalui sumber-sumber tak langsung seperti buku, jurnal, dokumen, situs resmi, dan lain sebagainya. Teknik penelusuran data menggunakan teknik dokumenter dan *online*.

HASIL DAN PEMBAHASAN

Hasil

Secara taktikal, kelompok-kelompok teroris telah melakukan berbagai perubahan dan penyesuaian untuk meluncurkan rencana aksi teror. Saat target dianggap memiliki keamanan tinggi dan susah ditembus, kelompok teroris kemudian melakukan serangkaian evolusi taktik yang mengarah pada target yang lebih rentan. Praksis ini ditunjukkan dalam praktik-praktik terorisme yang berubah selama seratus tahun terakhir. Mulai dari pembunuhan tokoh-tokoh politik di awal abad ke-20, lalu pembajakan pesawat dan penyanderaan oleh kelompok-kelompok teroris Timur Tengah pada tahun 1970-an, serangan terhadap unit-unit polisi dan tentara serta peledakan bom oleh IRA pada tahun 1990-an, hingga pergeseran ke arah memaksimalkan korban sipil dengan serangan bunuh diri dalam 15 tahun terakhir (Cambridge Centre for Risk Studies, 2017). Hal ini menunjukkan bahwa kelompok-kelompok teroris telah melakukan berbagai upaya evolusi taktikal dalam meluncurkan rencana aksinya.

Pada era revolusi industri 4.0, *cyberspace* menjadi rentan oleh aksi-aksi terorisme atau disebut *cyberterrorism*. Dengan sejarah kemajuan teknik taktis terorisme tersebut, para pengamat telah berspekulasi pada masa depan terorisme global, termasuk *cyberterrorism* (Cambridge Centre for Risk Studies, 2017). Tak dapat dipungkiri, perkembangan teknologi dan informasi di era Revolusi Industri 4.0 menyediakan sebuah arena baru yang dinamakan *cyberspace* terhadap kelompok teroris untuk memperluas berbagai aktivitasnya. Salah satu bukti sederhana atas asumsi ini adalah sebagian besar kelompok teroris telah memiliki dan mengoperasikan *website*. Dalam beberapa kasus, kelompok-kelompok teroris bekerja sama dengan kelompok kejahatan terorganisir dan menggunakan teknologi untuk penyebaran propaganda, penggalan dana atau pencucian uang, perekrutan anggota baru, hingga pelatihan-pelatihan terkait rencana aksi teror. *Cyberspace* dijadikan sarana untuk melakukan komunikasi dan koordinasi yang berkaitan dengan strategi-strategi teror mereka (Hoffman, 2006). Maka dari itu, negara dituntut bertindak selangkah lebih maju untuk meredam aksi-aksi dari *cyberterrorism*. Mengingat sulitnya melakukan penelusuran dan pelacakan aktivitas kelompok-kelompok teroris di ranah *cyberspace*.

Ruang gerak *cyberterrorism* yang dipengaruhi pesatnya perkembangan teknologi dan informasi di era revolusi industri 4.0 sudah seharusnya dibatasi. Sebelum menuju pada analisis tersebut, perlu dipahami definisi mengenai *cyberterrorism*. Menurut Center for Strategic and International Studies, *cyberterrorism* merupakan sebuah serangan yang direncanakan dengan motivasi politis oleh kelompok, agen rahasia, atau individu terhadap sistem komputer dan informasi, yang dapat menyebabkan dampak fisik terhadap target non-kombatan dari serangan tersebut. Keith Lourdeau selaku Asisten Direktur Divisi Cyber FBI memaparkan *cyberterrorism* sebagai tindakan kriminal yang dilakukan oleh pihak-pihak dengan kemampuan di bidang teknologi komputer dan telekomunikasi, yang dapat menyebabkan kekerasan, kerusakan, atau gangguan layanan untuk menimbulkan reaksi ketakutan masyarakat. Tujuannya adalah mempengaruhi pemerintah maupun masyarakat untuk mengakui serta mendukung agenda sosial, politik, dan ideologi yang digagas oleh pelaku *cyberterrorism* (Colarik, 2006).

Berdasarkan definisi-definisi tersebut, dapat dinyatakan bahwa *cyberterrorism* meliputi berbagai aktivitas atau kegiatan teroris yang menggunakan *cyberspace* sebagai media komunikasi dan koordinasi ataupun sebagai target sasaran. Satu hal mendasar yang membedakan *cyberterrorism* dengan tindakan-tindakan kriminal lain di ranah *cyberspace* adalah adanya motivasi politik yang melatarbelakangi aksi-aksi yang dilakukan. Selain itu, tujuan yang ingin diperoleh adalah aspek psikologis dari target guna menciptakan reaksi ketakutan masyarakat. Dengan kata lain, *cyberterrorism* mengacu pada dua inti

LITERATUS is a journal published by Neolectura, issued two times in one year. Literatus is a scientific publication media in the form of conceptual paper and field research related to social impact and cultural studies. It is hoped that LITERATUS can become a media for academics and researchers to publish their scientific work and become a reference source for the development of science and knowledge.

Our focus:
Social and Culture

Our Scope:
Humanities, Education, Management, History, Economics, Linguistics, Literature, Religion, Politics, Sociology, Anthropology, and others.

aktivitas. Pertama adalah sebagai sarana komunikasi dan koordinasi terkait penggunaan *cyberspace* terutama internet, baik untuk menyebarkan propaganda, melakukan rekrutmen, menggalang dana, mencuci uang, dan melatih anggota. Kedua adalah sebagai target sasaran langsung, yakni mengeksploitasi, mencuri, dan merusak fasilitas-fasilitas terkait bidang *cyber* yang dimiliki pemerintah ataupun masyarakat sipil.

Pembahasan

Berbagai manifestasi dari *cyberterrorism* telah terjadi dalam beberapa tahun terakhir, khususnya sejak awal abad ke-21 atau ketika dimulainya era revolusi industri 4.0. Pada tulisan ini, contoh kasus *cyberterrorism* dibagi menjadi dua kategori, yaitu *Hybrid Cyberterrorism* dan *Pure Cyberterrorism*.

Kategori pertama yaitu *Hybrid Cyberterrorism* mengacu pada *cyberspace* terutama internet yang digunakan sebagai sarana komunikasi dan koordinasi untuk menyebarkan propaganda, melakukan rekrutmen, menggalang dana, mencuci uang, dan melatih anggota. Internet digunakan oleh kelompok-kelompok teroris untuk menyebarkan propaganda atas ideologi mereka. Selain sebagai strategi radikalisme, penyebaran berbagai konten seperti foto atau video pembunuhan, pemenggalan, eksekusi mati, dan lain sebagainya yang dilakukan oleh kelompok teroris bertujuan untuk menimbulkan rasa takut masyarakat luas. Adapun beberapa *platform* yang digunakan adalah Facebook, Twitter, Instagram, Tumblr, VKontakte, justPaste.it, Youtube, dll. Misalnya Daesh yang memiliki tujuh agensi media yang beroperasi di bawah pusat komando medianya dan 37 kantor media yang tersebar di berbagai negara. Contoh lain adalah Al-Qaeda yang membentuk media yang dikenal sebagai *The Global Islamic Media Front* (GIMF) dan *As-Sahab* (Zerzri, 2017). Tujuannya tentu sebagai sarana untuk menyebarkan berbagai konten kepada masyarakat di seluruh dunia melalui internet atau *cyberspace*.

Salah satu aplikasi yang digunakan untuk menyebarkan konten propaganda oleh kelompok-kelompok teroris sejak tahun 2015 adalah Telegram. Aplikasi ini digunakan karena enkripsi dan penggunaannya yang lebih aman. Pada Agustus 2016, institusi media jihadis yang bernama *Al-Sumud* merilis sebuah *link* di Telegram untuk akses ke aktivitas-aktivitas terorisme yang dilakukan di Somalia dan Maghreb. Ada juga yang disebut *Orlando Channel–Omar Mateen*, sebuah saluran Telegram yang merilis publikasi mengenai artikel dan video pembantaian di Orlando (Zerzri, 2017). Publikasi-publikasi yang dapat diakses oleh anggota atau simpatisan teroris melalui aplikasi Telegram tersebut tentu membuat semangat jihad mereka semakin tinggi. Sehingga motivasi untuk melakukan serangkaian aksi teror semakin bertambah. Selain itu karena sifatnya yang dapat diakses secara umum, membuat publikasi-publikasi tersebut memungkinkan menimbulkan rasa ketakutan bagi masyarakat non-simpatisan terorisme.

Dalam bidang komunikasi dan koordinasi antar anggota atau organisasi terorisme lain, mereka menggunakan berbagai *platform*. Pada ranah media sosial seperti Telegram dan aplikasi sistem pesan terenkripsi seperti Kik, SuperSpot, Wickr, Whatsapp, Gajim. Media lain yang digunakan adalah ruang obrolan *game online*, pesan berkode atau steganografi untuk diskusi rahasia, dan perencanaan atau koordinasi serangan fisik serta perencanaan operasi peretasan. Misalnya, layanan telepon VoIP digunakan selama serangan Mumbai pada tahun 2008 (Zerzri, 2017).

Bentuk lain dari *cyberterrorism* pada kategori *Hybrid Cyberterrorism* adalah sebagai sarana penggalan dana. Salah satu contohnya adalah kampanye *Arm Us* yang bertujuan menggalang dana untuk ke arah "*Jihad for Allah*", mempersenjatai mujahidin dengan senjata dan amunisi, pembuatan senjata dan rudal dan bom, pelatihan fisik, mempromosikan syariah dan dakwah (dakwah), dan mendirikan propaganda jihad.

Contoh lain adalah kampanye penggalangan dana “*Your Sons at Your Service*” untuk mensponsori keluarga mujahid yang mencapai 100 US Dollar per bulan (Zerzri, 2017).

Cyberterrorism juga meliputi *data mining* untuk mengumpulkan informasi tempat dan individu tertentu sebagai target potensial terkait serangan serta perekrutan. pada insiden 11 September 2001 atau 9/11, Al-Qaeda menggunakan internet untuk mengumpulkan informasi seperti waktu penerbangan. Selain itu mereka juga menggunakan internet sebagai sarana berbagi informasi dan mengkoordinasikan rencana aksi.

Selain itu, DAESH dan kelompok-kelompok terorisme lainnya menggunakan media sosial untuk memilih individu untuk tujuan radikalisisasi atau rekrutmen. Perekrut mengidentifikasi target potensial dengan melakukan monitoring profil Facebook dan utas percakapan. Perekrut kemudian melakukan pemeriksaan lebih lanjut dengan menambahkan mereka sebagai teman dan hanya melakukan komunikasi pribadi hanya setelah perekrut yakin dengan kesetiaan individu-individu yang ingin berafiliasi dengan kelompok terorisme. Kelompok-kelompok terorisme menggunakan *platform* yang disebut *Dark Net* untuk menyebarkan materi pelatihan dalam melakukan serangan fisik. *Dark Net* juga digunakan untuk mendistribusikan pedoman dan instruksi terkait pembekalan terhadap anggota ataupun simpatisan. Hal ini dilakukan untuk memperkuat pertahanan *cyber* dan meningkatkan kemampuan serangan kelompok-kelompok teroris (Zerzri, 2017).

Dengan demikian, ancaman *cyberterrorism* dalam kategori *Hybrid Cyberterrorism* meliputi berbagai aspek. Seperti penyebaran propaganda, komunikasi dan koordinasi antar anggota ataupun kelompok teroris lain, penggalangan dana, *data mining*, rekrutmen, serta pelatihan. Meski bersifat mengancam secara tidak langsung, ancaman-ancaman yang ditimbulkan dari *Hybrid Cyberterrorism* perlu diantisipasi. Bebasnya ruang gerak kelompok-kelompok teroris di dunia maya mempermudah perencanaan dan realisasi dari serangan fisik yang tentunya membahayakan keamanan masyarakat luas.

Kategori kedua dari contoh kasus *cyberterrorism* adalah *Pure Cyberterrorism*. Kategori ini mengacu pada serangan langsung terhadap infrastruktur *cyber* milik korban, seperti komputer, jaringan, dan informasi yang tersimpan di dalamnya. Tujuan dasarnya adalah untuk mencapai tujuan politik, agama, dan ideologi. Dalam beberapa tahun terakhir, beberapa kelompok peretas atau *hacker* yang berafiliasi dengan DAESH telah aktif meretas *web host* untuk merusak situs internet, menyebarkan propaganda ekstremis agama, membuka panggilan perang siber di media sosial, serta merusak layanan dan bisnis *online*. Untuk meningkatkan kemampuan peretasan dan memperkuat posisi mereka di dunia maya, beberapa kelompok *hackers* tersebut bergabung dalam sebuah organisasi. Seperti Ghost Caliphate Section, the Sons Caliphate Army, the Caliphate Cyber Army, dan United Cyber Caliphate (Zerzri, 2017). Ambisi dari kelompok-kelompok *hacker* ini adalah meretas situs-situs resmi milik pemerintah untuk menyerukan pesan-pesan tertentu.

Salah satu contoh kasusnya adalah Fallaga, kelompok *hacker* Tunisia yang berafiliasi dengan DAESH. Kelompok ini melakukan penyerangan dan perusakan terhadap beberapa situs web milik Kementerian Kesehatan Inggris. Mereka menggantikan laman web tersebut dengan foto-foto perang di Suriah, memasukkan pesan *Stop the Killing in Syria*, dan tanda pagar #Op-Rusia atau #Save-Aleppo (Zerzri, 2017).

Cyberterrorism bukan lagi sebuah hal utopis yang dapat mengancam negara. Perkembangan teknologi informasi dalam ranah *cyberspace* mengakibatkan eskalasi ancaman menjadi semakin kompleks. Apabila tidak ditangani dengan tepat, keamanan fasilitas *cyber* milik negara maupun masyarakatnya dapat terancam. Maka dari itu, tulisan ini kemudian membahas tentang tantangan dan strategi Indonesia dalam menanggulangi ancaman *cyberterrorism*.

Contoh kasus tersebut menunjukkan kapabilitas atau kemampuan yang dimiliki kelompok-kelompok *hacker* pro-terorisme tidak dapat dianggap remeh. Apabila situs resmi pemerintah Inggris yang notabene memiliki keamanan tinggi dapat diretas kelompok *hackers* milik organisasi teroris, maka negara-negara lain, terutama Indonesia sudah harus meningkatkan keamanan infrastruktur siber secara besar-besaran. Selain melindungi keamanan fasilitas siber milik negara, Indonesia juga harus memproteksi keamanan siber milik masyarakat sipil seperti akun-akun media sosial pribadi. Hal ini penting dikarenakan akun-akun media sosial terintegrasi dengan data-data pribadi pemilik. Jika data-data ini dapat diretas oleh kelompok teroris, tentu mempermudah mereka untuk melancarkan aksi *cyberterrorism* baik kategori *Hybrid Cyberterrorism* maupun *Pure Cyberterrorism*.

Misalnya pada *Hybrid Cyberterrorism*. Ketika negara tidak mampu menghadirkan keamanan optimal terkait bidang *cyberspace*, ancaman-ancaman yang dapat ditimbulkan akan sangat vital. Penyebaran propaganda, komunikasi dan koordinasi antar anggota ataupun kelompok teroris lain, penggalangan dana, *data mining*, rekrutmen, serta pelatihan dari kelompok-kelompok teroris akan dengan leluasa dilakukan. Meski bersifat mengancam secara tidak langsung, ancaman-ancaman yang ditimbulkan dari *Hybrid Cyberterrorism* tetap perlu diantisipasi. Bebasnya ruang gerak kelompok-kelompok teroris di dunia maya mempermudah perencanaan dan realisasi dari serangan fisik yang tentunya membahayakan keamanan masyarakat luas.

Di samping itu, negara harus mengantisipasi ancaman-ancaman *cyberterrorism* dalam kategori *Pure Cyberterrorism*. Hal ini mengacu pada serangan langsung terhadap fasilitas siber milik korban, seperti komputer, jaringan, dan informasi yang tersimpan di dalamnya. Tujuan dasarnya adalah untuk mencapai tujuan politik, agama, dan ideologi. Contoh sederhana adalah ketika kelompok teroris mampu mengakses data-data pribadi melalui akun sosial media milik masyarakat sipil. Kelompok teroris tersebut akan dengan bebas dapat mengancam korban bermodalkan data pribadi yang telah diperoleh. Korban tentu tidak ingin data-data pribadinya, apalagi yang bersifat sensitif tersebar luas di internet. Kondisi ini mengakibatkan korban cenderung melakukan berbagai hal atas instruksi kelompok teroris demi menjaga data-data personalnya tetap aman. Misalnya seperti mengirim sejumlah uang kepada kelompok teroris, melakukan perilaku kriminal, serta tindakan-tindakan lain sesuai arahan kelompok teroris tersebut. Begitu pula pada perlindungan fasilitas siber resmi milik pemerintah. Maka dari itu, negara harus hadir dan memastikan keamanan fasilitas-fasilitas siber milik pemerintah dan setiap masyarakatnya.

Gelombang revolusi industri 4.0 membawa konsekuensi terhadap tantangan pemerintah dalam upaya memperkuat *cybersecurity* khususnya dari ancaman *cyberterrorism*. Terkait hal tersebut, Indonesia telah melakukan berbagai langkah strategis untuk menanggulangi ancaman *cyberterrorism*. Salah satunya adalah melalui pembentukan institusi khusus yang menangani bidang siber nasional. Peraturan Presiden Nomor 53 Tahun 2017 yang kemudian direvisi Perpres Nomor 133 Tahun 2017 mengamanatkan pembentukan Badan Siber dan Sandi Negara (BSSN). Secara umum, badan ini bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengkonsolidasikan semua unsur yang terkait dengan keamanan siber. Dalam situs resmi BSSN, disampaikan pula tujuan strategis Strategi Keamanan Siber Indonesia adalah tercapainya ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber dan keamanan siber pada ekonomi digital. Strategi Keamanan Informasi Indonesia ini diharapkan dapat menjadi salah satu fondasi kepercayaan dunia kepada Indonesia dalam berbagai forum keamanan siber internasional (BSSN, n.d.). Dengan demikian, BSSN menjadi ujung

tombak Indonesia dalam menjamin *cyber security* secara nasional termasuk dari ancaman *cyberterrorism*.

Namun bukan berarti BSSN menjadi satu-satunya instansi negara yang bertanggungjawab atas keamanan siber nasional. Diperlukan kolaborasi dari berbagai instansi pemerintah untuk mewujudkan keamanan siber yang maksimal. Maka dari itu pada November 2018, Indonesia menggelar *Sub Regional Meeting on Counter Terrorism* sebagai forum diskusi negara kawasan Asia Tenggara di Jakarta. Pertemuan tersebut khusus membahas penanganan terorisme dan tindak lanjut dari pertemuan serupa yang sebelumnya diselenggarakan di Manado pada Juli 2018. Forum ini berfokus pada *Responding to the Advancement of Strategies and Tactics of the Terrorist*.

Hal tersebut dilatarbelakangi oleh perkembangan teknologi informasi di era revolusi industri 4.0 yang turut membawa ancaman negatif. Sarana teknologi informasi yang semakin canggih dapat digunakan untuk mendukung aktivitas-aktivitas berbahaya seperti terorisme, penyebaran konten *hoax*, radikalisme, propaganda, dan lain sebagainya. Kelompok-kelompok teroris dapat dengan mudah melakukan berbagai aktivitas tersebut dengan memanfaatkan media sosial, enkripsi, email, *cryptocurrency*, dan berbagai *platform* lainnya. Dalam *press release*-nya pada November 2018, BSSN mendalami indikasi penggunaan media sosial oleh teroris untuk melakukan propaganda, rekrutmen, komunikasi, dan melaksanakan aksi teror. BSSN berwenang sebagai fasilitator para pemangku kepentingan keamanan siber yaitu Kemenkopolhukam, Kemenkumham, Kemlu, Kemhan, Kemenkominfo, BNPT, BIN, POLRI, dan PPATK untuk berkolaborasi dengan penyedia layanan dan infrastruktur komunikasi, entitas ekonomi digital, serta komunitas digital dari berbagai negara. Hasil yang ingin dicapai adalah menyepakati penyusunan aturan bersama penanganan terorisme di ranah siber atau *cyberterrorism* (BSSN, 2018).

Meski telah memiliki badan khusus dalam penanganan *cyber* dan *cyberterrorism*, Indonesia belum dapat dikatakan kuat secara institusional terkait isu tersebut. Wewenang BSSN dalam kontra *cyberterrorism* belum jelas. Begitu pun strategi-strategi BSSN dalam penanganan *cyberterrorism* belum memperlihatkan progres yang optimal. Di samping itu, terdapat kewenangan yang tumpang tindih dalam kontra *cyberterrorism* antar lembaga negara. Sejauh mana otoritas yang dimiliki BSSN, Kemenkominfo, BNPT, BIN, dan instansi lainnya terkait penanganan *cyberterrorism* belum dipetakan secara komprehensif. Dari sisi perundang-undangan, Indonesia belum cukup kuat dalam menjerat pelaku *cyberterrorism*. Saat ini hanya ada dua undang-undang yang dapat dikaitkan dengan tindakan *cyberterrorism*, yaitu Undang-Undang No. 5 tahun 2018 tentang perubahan atas Undang-Undang No. 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme dan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE). Kedua UU tersebut belum mengatur secara tegas mengenai tindakan-tindakan yang berkaitan dengan *cyberterrorism*. Hal ini tentu menimbulkan permasalahan terhadap strategi kontra *cyberterrorism* di Indonesia.

Indonesia memiliki potensi ancaman *cyberterrorism* yang signifikan di era revolusi industri 4.0. Selain ancaman terhadap fasilitas *cyber* milik negara, ancaman fasilitas *cyber* pribadi milik masyarakat juga tidak dapat dikesampingkan. Ditambah lagi dengan pesatnya perkembangan internet dan pengguna internet di Indonesia, menjadi tantangan pemerintah untuk menghadirkan keamanan digital di ruang siber. Menurut data dari Asosiasi Penyedia Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia pada tahun 2017 mencapai 143,26 juta jiwa atau setara 54,7% dari total populasi masyarakat Indonesia (APJII, 2018). Besarnya angka pengguna internet di Indonesia juga disampaikan oleh situs Internet World Stats pada Maret 2019, yang merilis peringkat negara dengan pengguna internet tertinggi. Dalam rilis tersebut, Indonesia masuk peringkat kelima pengguna internet tertinggi di dunia, di bawah Tiongkok, India, Amerika Serikat, dan Brazil (Internet World Stats, 2019). Jumlah pengguna internet di

LITERATUS is a journal published by Neolectura, issued two times in one year. Literatus is a scientific publication media in the form of conceptual paper and field research related to social impact and cultural studies. It is hoped that LITERATUS can become a media for academics and researchers to publish their scientific work and become a reference source for the development of science and knowledge.

Our focus:
Social and Culture

Our Scope:
Humanities, Education, Management, History, Economics, Linguistics, Literature, Religion, Politics, Sociology, Anthropology, and others.

Indonesia yang tinggi dapat membuka celah atas ancaman-ancaman melalui *cyberspace* seperti *cyberterrorism*.

Di samping itu, ancaman lain muncul dari lemahnya *cyber capability* di Indonesia. Pengamat pertahanan siber dari Communication & Information System Security Research Center (CISSReC) Indonesia, Pratama Perdana, menyatakan bahwa pertahanan siber atau *cyber security* yang dimiliki Indonesia saat ini masih tergolong lemah. Bahkan jika dibandingkan dengan negara tetangga yaitu Singapura, kapabilitas *cyber security* Indonesia masih jauh di bawah. Ia turut menambahkan bahwa peningkatan *cyber security* sangat penting untuk keamanan nasional. Sangat berbahaya apabila sistem komunikasi dan informasi di Indonesia suatu saat lumpuh total akibat serangan *cyber* dan Indonesia belum pada level yang siap untuk mengantisipasinya (Merah Putih, 2019). Hal senada juga diungkapkan oleh pakar politik dan keamanan internasional dari Universitas Indonesia, Andi Wijayanto. Ia menyatakan bahwa data-data penting nasional sangat rentan dicuri. Baik yang sifatnya transaksi keuangan hingga data-data personal masyarakat seperti tanggal lahir, nomor induk kependudukan, dan pengamanan kartu kredit. Mengacu pada Networked Readiness Index (NRI), Indonesia menempati posisi ke-76 pada aspek kesiapan jejaring. Sedangkan Malaysia berada di posisi 30 (Antara News, 2017). Maka dari itu dapat dikatakan bahwa kapabilitas *cyber security* Indonesia masih belum cukup mumpuni untuk menangkal berbagai ancaman *cyber*, termasuk *cyberterrorism*.

Indonesia sejatinya dapat menjadikan Amerika Serikat sebagai percontohan kontra *cyberterrorism*. AS menganggap ancaman *cyber*, termasuk *cyberterrorism* sebagai prioritas yang memerlukan antisipasi khusus terkait dengan keamanan nasionalnya. Hal ini ditunjukkan sejak tahun 2000 ketika Presiden Clinton mendeklarasikan strategi keamanan yang disebut *Defending America's Cyberspace*. Strategi ini kemudian mengamankan dibentuknya tiga institusi baru yang berwenang dalam *cybersecurity* nasional. Pertama adalah *The Federal Incident Responses Capability* (FedCIRC) yang bertugas membangun pusat analisis investigasi ancaman di seluruh jaringan komputer non-militer milik negara. Sedangkan untuk jaringan komputer dan siber militer ditangani oleh *Joint Task Force-Computer Network Defense* (JTF-CND). Institusi kedua adalah *National Security Incident Response Center* (NSIRC) yang menyediakan bantuan terhadap FedCIRC dan JTF-CND jika terjadi serangan terhadap sistem siber yang mengancam keamanan nasional AS. Institusi ketiga adalah *National Infrastructure Protection Center* yang bertanggungjawab untuk memperingatkan ancaman, analisis strategi, dan penegakan hukum terkait ancaman-ancaman dari *cyberspace* (United States Executive Office of the President, 2009). Pembentukan tiga institusi ini beserta pemisahan kewenangan yang jelas dan terstruktur memperlihatkan keseriusan AS dalam menangani ancaman-ancaman dari *cyberspace* termasuk *cyberterrorism*.

Dalam ranah yang spesifik tentang *cyberterrorism*, Kementerian Pertahanan AS pada tahun 2010 membentuk *US Cyber Command*. Salah satu tugas utama dari badan ini adalah melindungi seluruh jaringan pertahanan dan mendukung operasi militer serta *counter cyberterrorism* (Rachmat, 2015). Di samping itu, dalam dokumen resmi *National Cyber Strategic* yang rilis pada September 2018, kebebasan internet AS dapat membuka celah bagi gerakan terorisme di ruang *cyber* atau *cyberterrorism*. Dengan tetap memegang prinsip kebebasan, AS terus mendorong untuk ditingkatkannya *cyber security* negara serta masyarakat dari berbagai ancaman yang dapat ditimbulkan (White House, 2018). Hal tersebut menunjukkan langkah strategis AS dalam peningkatan *power* negara terkait kontra terorisme di ranah *cyberspace*. AS sebagai negara dengan kemajuan teknologi informasi tinggi perlu menjamin *cyber security* nasionalnya, baik fasilitas pemerintah atau fasilitas masyarakat sipil. Apalagi dalam menghadapi Revolusi Industri

4.0, negara sudah seharusnya bertindak sebagai pelindung utama keamanan dan keselamatan *cyberspace*-nya dari berbagai ancaman, termasuk *cyberterrorism*.

Indonesia sudah seharusnya melakukan langkah-langkah baru dalam strategi kontra *cyberterrorism*. Aktivitas teroris yang semakin dinamis melalui *cyberspace* di era revolusi industri 4.0 membuat pemerintah dituntut bertindak cepat dan tepat. Ancaman-ancaman yang dapat ditimbulkan oleh *cyberterrorism* pun bukan lagi sesuatu utopis. Berbagai contoh kasus *cyberterrorism* memperlihatkan ruang gerak teroris di ranah *cyberspace* semakin bebas, baik dalam bentuk *Hybrid Cyberterrorism* maupun *Pure Cyberterrorism*. Ditambah lagi dengan fakta tingginya pengguna internet di Indonesia seakan menjadikan *cyberspace* masyarakat Indonesia sebagai target menggiurkan oleh pelaku *cyberterrorism*. Maka dari itu, strategi-strategi baru diperlukan untuk meredam aksi *cyberterrorism*. Baik dengan pembentukan instansi baru yang khusus menangani *cyberterrorism* atau memperkuat serta memperluas kewenangan BSSN maupun instansi yang terkait lainnya dalam hal kontra *cyberterrorism*.

PENUTUP

Era Revolusi Industri 4.0 membawa eskalasi ancaman baru terutama di ruang siber atau *cyberspace*. Salah satu bentuk ancaman dalam *cyberspace* adalah *cyberterrorism*. Hal ini tidak lepas dari fakta sejarah bahwa kelompok-kelompok teroris telah melakukan berbagai upaya evolusi taktikal dalam melancarkan rencana aksinya. Memasuki era revolusi industri 4.0, terorisme memiliki arena baru dalam melancarkan rencana aksinya yang disebut sebagai *cyberterrorism*. Berbagai contoh kasus yang dipaparkan memperlihatkan bahwa *cyberterrorism* bukan lagi sebuah hal utopis yang dapat mengancam negara.

Dalam konteks ini, Indonesia perlu melakukan sejumlah langkah strategis untuk meredam aksi *cyberterrorism*. Apalagi kapabilitas *cybersecurity* Indonesia saat ini masih lemah. Meski telah memiliki badan khusus yaitu Badan Siber dan Sandi Negara (BSSN) dalam upaya perlindungan fasilitas siber dari berbagai ancaman termasuk *cyberterrorism*, Indonesia belum dapat dikatakan kuat secara institusional terkait isu tersebut. Di samping itu, secara peraturan perundang-undangan, UU No. 5 Tahun 2018 tentang Perubahan atas Undang-Undang No. 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme tentang Pemberantasan Tindak Pidana Terorisme dan UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) belum cukup tegas dalam menindak pelaku *cyber terrorism*. Terkait kelemahan tersebut, Indonesia dapat mencontohkan Amerika Serikat yang memiliki sejumlah badan khusus dalam pengamanan dunia siber dan *cyberterrorism*. Dengan demikian, Indonesia dapat mengantisipasi berbagai bentuk ancaman *cyber* khususnya *cyberterrorism* di era revolusi industri 4.0 dengan lebih komprehensif.

DAFTAR PUSTAKA

- APJII. (2018). *Buletin APJII edisi Maret 2018*. Diakses dari <https://apjii.or.id/download/file/BULETINAPJIIEDISI22Maret2018.pdf>
- Antara News. (2017). *Pakar: Pertahanan Siber Indonesia Masih Lemah*. Diakses dari <https://jogja.antaranews.com/berita/351229/pakar-keamanan-siber-indonesia-masih-lemah>
- BSSN. (2018). *Press Release Antisipasi Cyber Terrorism, BSSN Siap Sinergikan Pemangku Kepentingan Keamanan Siber di Asia Tenggara*. Diakses dari https://bssn.go.id/wp-content/uploads/2018/11/PRESS-RELEASE_SRM-ON-CT-JAKARTA.pdf

Cambridge Centre for Risk Studies. (2017). *Cyber Terrorism: Assessment of the Threat to Insurance; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge*. Diakses dari

https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/pool-re-cyber-terrorism.pdf

Colarik, A. M. (2006). *Cyber Terrorism: Political and Economic Implications*. London: Idea Group Publishing.

Goutam, R. K. (2015). Importance of Cybersecurity. *International Journal of Computer Applications* Vol. 111 (7). hlm. 14-17. Diakses dari <https://pdfs.semanticscholar.org/5cfb/7a5bd2e6c181e8a69ebd49b1dadb795f493b.pdf>

Hoffman, B. (2006). *The Use of the Internet By Islamic Extremists: Testimony presented to the House Permanent Select Committee on Intelligence*. Diakses dari https://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf

Internet World Stats. (2019). *Top 20 Countries with the Highest Numbers of Internet Users*. Diakses dari <https://www.internetworldstats.com/top20.htm>

Medium. (2018). *Fintech and the 4th Industrial Revolution*. Diakses dari <https://medium.com/@alcormna/fintech-and-the-4th-industrial-revolution-b328088399dc>

Merah Putih. (2019). *Pertahanan Siber Indonesia Masih Lemah, Pengamat: Yang Dibahas Jokowi dan Prabowo Hanya Unicorn*. Diakses dari <https://merahputih.com/post/read/pertahanan-siber-indonesia-masih-lemah-pengamat-yang-di-bahas-jokowi-dan-prabowo-hanya-unicorn>

National Initiative for Cybersecurity Careers and Studies. (2018). *Explore Terms: A Glossary of Common Cybersecurity Terminology*. Diakses dari <https://niccs.us-cert.gov/about-niccs/glossary#cybersecurity>

Rachmat, A. N. (2015). *Keamanan Global: Transformasi Isu Keamanan Pasca-Perang Dingin*. Bandung: Alfabeta

White House. (2018). *National Cyber Strategy*. Diakses dari <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

Zerzri, M. (2017). *The Threat of Cyber Terrorism and Recommendations for Countermeasures*. Diakses dari <https://www.cap-lmu.de/download/2017/CAPerspectives-Tunisia-2017-04.pdf>

LITERATUS is a journal published by Neolectura, issued two times in one year. Literatus is a scientific publication media in the form of conceptual paper and field research related to social impact and cultural studies. It is hoped that LITERATUS can become a media for academics and researchers to publish their scientific work and become a reference source for the development of science and knowledge.

Our focus:
Social and Culture

Our Scope:
Humanities,
Education,
Management,
History,
Economics,
Linguistics,
Literature,
Religion,
Politics,
Sociology,
Anthropology,
and others.