

INTERNET DAN TERORISME: MENGUATNYA AKSI GLOBAL CYBER-TERRORISM MELALUI NEW MEDIA

Eska Nia Sarinastiti¹ dan Nabilla Kusuma Vardhani²

¹Program Studi Kepariwisata, Departemen Bahasa Seni dan Manajemen Budaya, Sekolah Vokasi, Universitas Gadjah Mada, Yogyakarta, Indonesia

Email: ¹eskanias@ugm.ac.id

²Program Studi Bahasa Inggris, Departemen Bahasa Seni dan Manajemen Budaya, Sekolah Vokasi, Universitas Gadjah Mada, Yogyakarta, Indonesia

Email: ²nabilla.kusuma.v@mail.ugm.ac.id

ABSTRAK

Tujuan dari penelitian ini adalah mengeksplorasi tindakan cyber-terrorism global, jenis media baru dalam cyber-terrorism, dan fenomena cyber-terrorism di Indonesia. Penelitian ini menggunakan metode studi kasus, teknik pengumpulan data menggunakan observasi dan dokumentasi. Analisis data menggunakan analisis isi untuk mencari data. Hasil penelitian ini menunjukkan bahwa penggunaan internet untuk tindakan mereka dimotivasi oleh kelemahan media massa (televisi dan media cetak) yang tidak lagi aman dan banyak manipulasi isi tentang aktivitas kelompok teroris. Salah satu kelompok teroris paling canggih dan intensitas tertinggi penggunaan media online untuk kegiatan terorisme adalah kelompok Al-Qaeda. Secara keseluruhan, Internet digunakan oleh teroris untuk kegiatan terorisme serta tindakan cyber-terrorism yang meliputi pelatihan, penggalangan dana, koordinasi, perencanaan dan pelaksanaan tanpa mempresentasikan secara fisik lokasi eksekusi, meng-hack sistem target, menyebarkan propaganda radikal, hasutan, rekrutmen anggota baru, mencari informasi tentang data anggota militer, intelijen, atau pejabat politik. Berdasarkan hasil beberapa penelitian dan laporan media, media online yang secara terbuka dapat kita lihat sebagai media mereka, yaitu youtube, game online, situs web, media sosial (twitter dan facebook), dan majalah online. Indonesia menjadi salah satu negara yang juga memiliki efek kuat dari cyber-terrorism sejak bom Bali pada tahun 2002 sampai sekarang. Ketersediaan dan tingkat kekuatan cyber-terrorism dan peraturan penggunaan media online di sebuah pemerintahan akan menentukan keamanan masyarakat dari kelompok aksi teroris melalui internet.

Kata kunci : global cyber-terrorism, internet, new media

PENDAHULUAN

Semenjak terjadinya serangan 11 September 2001 di New York dan Pentagon, terorisme menerima banyak perhatian dari seluruh dunia. Masyarakat dunia berharap bisa meramal tindakan terorisme yang terjadi selanjutnya karena semua orang percaya terdapat tindakan terorisme yang akan terjadi. Salah satu faktor yang bisa meramalkan tindakan mereka adalah metode apa yang mereka gunakan untuk mengirimkan terror mereka pada populasi targetnya (Brenner, 2002:149). Disinilah media berhubungan dengan terorisme sebagai alat komunikasi mereka.

Terorisme bukan lagi permasalahan lokal dari negara-negara tertentu tapi isu yang mencakup sejumlah aspek internasional. Terorisme merupakan fenomena internasional, maka tanggapan-tanggapannya juga harus internasional (Ganor, 2002:130). Para teroris tersebar dimana-mana dengan menggunakan media sebagai alat komunikasi

mereka maupun sebagai media komunikasi mereka dalam mengkomunikasikan keberadaan mereka pada seluruh dunia. Media komunikasi mereka mulai dari menggunakan buku, majalah, surat kabar, musik, film, *software*, *games* mulai dari bentuk fisik (*hardcopy*) sampai dalam bentuk *softfile* yang disebarkan ke seluruh dunia (Brenner, 2002:150).

Perkembangan era globalisasi yang memunculkan media Internet menjadikan media komunikasi yang digunakan teroris semakin berkembang. Mereka berusaha menyesuaikan kemampuan mereka dengan perkembangan teknologi komunikasi dan informasi yang ada. Kemudian, terjadilah transformasi dari penggunaan media konvensional ke media baru, yakni Internet yang memunculkan fenomena *cyber-terrorism*. *Cyber-terrorism* ini menjadi isu dunia yang menuntut seluruh Negara untuk mampu menguasai dunia Internet guna mengetahui tindakan teroris. Semakin pesat perkembangan teknologi media baru,

semakin canggih juga media yang digunakan oleh teroris dan semakin besar pula tindakan terorisme yang bisa terjadi.

Cyber-terrorism menjadi kajian yang sangat penting dalam new media dan terorisme. Maka dari itu, pada paper ini untuk selanjutnya akan dibahas global *cyber-terrorism*, berbagai jenis media *cyber-terrorism* yang digunakan, serta studi kasus *cyber-terrorism* di Indonesia. Adanya pembahasan ini diharapkan dapat menjadi gambaran aksi *cyber-terrorism* secara global yang semakin kuat melalui beragam jenis new media.

Fokus permasalahan pada penelitian ini adalah maraknya peristiwa terorisme yang dilakukan secara viral atau biasa disebut dengan *cyber-terrorism* sejak semakin canggihnya teknologi yang berkembang mulai dari sistem dan perangkatnya. *Cyber-terrorism* menuntut berbagai pihak untuk bisa meningkatkan pengetahuan dan kemampuan mereka tentang seberapa jauh aksi yang dilakukan teroris dunia dalam *cyber-terrorism*. Serta, perlu diketahui jenis media yang digunakan dalam *cyber-terrorism* oleh para teroris di dunia. Selain perhatian dunia, *cyber-terrorism* juga terjadi di Indonesia yang perhatian khusus masyarakat Indonesia sehingga perlu diketahui fenomena *cyber-terrorism* yang ada di Indonesia.

Penelitian ini memiliki tiga tujuan yakni pertama untuk menganalisa sejauh mana aksi global *cyber-terrorism*, kedua untuk menganalisa berbagai jenis media *cyber-terrorism* yang digunakan, dan ketiga untuk menganalisa fenomena *cyber-terrorism* yang ada di Indonesia secara khusus. Landasan teoritis yang digunakan dalam penelitian ini adalah sebagai berikut:

Pendekatan Keterkaitan Terorisme, Teroris, dan New Media

Media dan terorisme menjadi dua tema sentral yang menarik perhatian karena memiliki benang merah. Benang merah antara media dan terorisme tidak terlepas dari aspek komersialisasi berita. Terorisme merupakan sebuah fakta sosial yang dapat dimanfaatkan untuk kepentingan peningkatan konsumsi berita. Sementara itu, terorisme modern memanfaatkan media komunikasi untuk menciptakan efek pada diri khalayak melalui bentuk propaganda terror. Terdapat relasi *symbiotic* antara keduanya yang bertemu pada titik kepentingan akan kebutuhan

informasi dan keinginan untuk diliput oleh media. (Sukarno, 2011:360-361).

Keterkaitan teroris dan media juga diungkapkan oleh Hendropriyono (2009: 218) bahwa terdapat keadaan yang saling menguntungkan (symbiosis mutualisme) antara para teroris dan media. Media telah memperkuat tindakan-tindakan teroris sebagai sesuatu yang penting secara politis di luar porsi yang semestinya. Terorisme merupakan penggunaan secara sengaja atau ancaman menggunakan kekerasan melawan masyarakat sipil atau melawan target masyarakat sipil, untuk mempertahankan tujuan politik. Definisi terorisme tersebut didasarkan pada tiga elemen penting menurut Ganor (2002: 126) diantaranya:

1. Esensi dari tindakan terorisme tersebut dalam penggunaan ancaman atau kekerasan. Berdasarkan definisi ini sebuah aktivitas yang tidak termasuk kekerasan atau ancaman kekerasan tidak akan didefinisikan sebagai terorisme (termasuk protes tanpa kekerasan, demonstrasi perdamaian, pemberontakan pajak, dan sejenisnya).
2. Tujuan tindakan terorisme selalu bersifat politik. Tujuannya adalah mempertahankan tujuan politik, mengubah rezim, mengubah orang dengan kekuasaan, mengubah kebijakan sosial atau ekonomi. Ketidakhadiran tujuan politik, sebuah tindakan tidak bisa didefinisikan sebagai terorisme. Sebuah tindakan kekerasan terhadap masyarakat sipil yang tidak memiliki tujuan politik, kejahatan atau tindakan kriminal tidak berhubungan dengan terorisme. Beberapa ahli memasukkan tujuan ideologi atau agama masuk dalam daftar tujuan yang bersifat politik.
3. Target dari terorisme adalah masyarakat sipil. Terorisme mengeksploitasi kerapuhan masyarakat sipil untuk menimbulkan kegelisahan yang dahsyat dan dan memprovokasi reaksi media yang intens dengan menyerang melawan target masyarakat sipil.

Pada perkembangannya, kemajuan teknologi dan era globalisasi memunculkan media baru (*new media*) yang memungkinkan teroris menyerang dalam beberapa cara yang sebelumnya tidak dapat dibayangkan melalui Internet. Aksi terorisme yang tidak terduga dan mampu tanpa meninggalkan jejak. Serta, aksi terorisme yang tidak terbatas oleh waktu dan keterjangkauan tempat.

Internet dan Cyber-terrorism

Kelompok teroris di dunia yang paling dikenal salah satunya adalah Al-Qaeda. Teroris menggunakan Internet sebelum peristiwa 11 September 2001. Media Internet dikenal sebagai alat yang sangat kuat untuk organisasi teroris. Sebelum tahun 1999, hampir 30 kelompok teroris ditemukan di Internet oleh Departemen Pemerintahan Amerika Serikat. (Banez, 2010: 16). Namun, lebih kuatnya lagi peranan Internet untuk mereka ketika pasca terjadi peristiwa 9/11, kepemimpinan Al-Qaeda berusaha menyebarkan video dari persembunyian mereka di Pakistan melalui televisi Al-Jazeera, akan tetapi mereka frustrasi dengan segmen mereka yang sangat sedikit sehingga pesan bisa jadi disalahpersepsikan yang kemudian membuat mereka beralih pada Internet untuk meng-*upload*-nya secara lebih jelas dan detail tanpa adanya pengeditan. (Gardner, 2013).

Pemanfaatan Internet oleh Al-Qaeda didasari alasan bahwa media massa seperti televisi dan majalah akhir-akhir ini mengancam keamanan organisasi dan anggota mereka. Televisi memiliki keterbatasan waktu untuk menyiarkan berita yang panjang dan padat sebagai pengaplikasian ideologi mereka. Bahkan, media massa dianggap tidak aman oleh mereka yang memungkinkan pesan mereka diambil oleh pihak yang berkepentingan dan memutarbalikkan fakta yang mempengaruhi opini publik terhadap tindakan mereka. (Soriano, 2008:16)

Teroris membangun jaringan yang semakin kuat dengan adanya Internet. Meskipun banyak anggota yang dipenjara dan meninggal, aksi propaganda mereka terus dilakukan dan semakin meluas, bahkan tanpa jejak dengan adanya Internet ini. Seperti yang dilakukan pihak Al-Qaeda yang berada di Pakistan setelah pihak angkatan Udara Amerika menyerang Damadola Pakistan, mereka berusaha menyusup pada *web* Amerika Serikat dengan propagandanya bahwa mereka mengingatkan pihak Amerika bahwa mereka akan terus menteror. (Soriano, 2008:15). Internet menyediakan papan pesan dan *chat room* untuk *recruitment* para teroris, membeli bom, membeli tiket pesawat, mengkoordinasikan serangan dan berkumpul dalam satu tempat tanpa hadir secara fisik (Lumbaca&Gray, 2011:47).

Adanya Internet mereka berusaha meng-*hack* beberapa situs milik pemerintahan Amerika Serikat dan beberapa Negara Barat sekutunya. Oleh karena itu,

mereka berusaha menghapuskan kelemahan mereka dengan menempatkan organisasi pada penggunaan teknologi baru. Organisasi Osama Bin Laden pada cara ini memilih menyebarkan pengembangan berita mereka kebanyakan saat ini pada Internet.

Internet ini kemudian memunculkan istilah *cyber-terrorism* dimana sekelompok teroris menggunakan *cyberspace* (berbagai aplikasi Internet) dalam melakukan aksi terorisme mereka. Internet memungkinkan penyebaran informasi yang cepat, sedikit resiko, dan murah pada beragam konstituen, mulai dari perekrutan yang potensial hingga potensi memperoleh *partner* yang prospektif dalam organisasi teroris (Seib & Janbek, 2011: 21). Banyak dari mereka menggunakan *cyberspace*, contohnya kelompok yang ditemukan Abu Musab Al-Zarqawi dari faksi Al-Qaeda di Saudi hampir tidak pernah kontak langsung dengan media massa, mereka memfokuskan aktivitas komunikasi mereka dalam *cyberspace*. Metode ini menghindarkan mereka dari penerimaan perhatian media secara luas. Secara paradoks, media massa sendiri menggunakan *web* untuk mencari jejak dan pesan tentang terorisme terbaru yang mereka lakukan yang akan mendorong munculnya opini publik secara internasional. (Soriano, 2008:15)

Untuk Al-Qaeda, Internet bukan hanya metode untuk meraih media yang lebih aman dan lebih cepat, tapi juga merupakan titik balik dari bangkitnya strategi komunikasi yang efektif dibandingkan dengan media tradisional. Pertama kalinya *cyberspace* mampu memungkinkan komunikasi secara langsung antara teroris dengan publiknya. Internet bukan hanya mengisi keterbatasan media massa, tapi Internet juga memungkinkan mereka untuk menghindari sejumlah aturan moral yang terdapat dalam media massa dan membatasi tindakan mereka, dan hal ini menguntungkan untuk strategi tindakan terorisme mereka. Seperti yang dilakukan sekelompok jihad seiring dengan invasi Iraq tahun 2003, Internet bukan hanya memungkinkan mereka menghindari resiko operasional, tapi memungkinkan mereka mendapatkan akses dengan menyusup sistem media tradisional seperti Al-Jazeera (Soriano, 2008:16-17).

BAHAN DAN METODE PENELITIAN

Bahan-bahan yang digunakan dalam penelitian ini adalah lebih pada peralatan penelitian seperti laptop, modem, paketan data internet, dan alat

tulis dalam mencari informasi dan menganalisis berbagai bentuk new media yang menjadi media *cyber-terrorism* mulai dalam bentuk audio visual sampai pada tulisan. Penelitian ini menggunakan penelitian kualitatif dengan metode studi kasus. Metode studi kasus dipilih karena penelitian ini lebih fokus menggali fenomena yang menjadi perhatian masyarakat luas hingga saat ini, yakni terorisme. Teknik pengumpulan data dilakukan dengan observasi dan dokumentasi. Objek penelitian yang diobservasi fokus pada video-video propaganda teroris di media online (youtube dan official situs online berita), media sosial, website, majalah online, dan game online. Sementara itu, untuk dokumentasi fokus pada berbagai jurnal yang membahas tentang new media dan *cyber-terrorism*, artikel *online* tentang global *cyber-terrorism*, dan berbagai sumber tertulis yang relevan. Analisis data dilakukan dengan analisis isi (*content analysis*) yang dimulai dari mengkategorikan hasil data baik dalam bentuk video, gambar, maupun tulisan dalam beberapa tema sesuai dengan kajian yang ditentukan yakni mulai dari aksi global *cyber-terrorism*, beragam *new media cyber-terrorism*, dan studi kasus *cyber-terrorism* di Indonesia kemudian dianalisis sesuai kajian teoritis yang digunakan.

Hasil dan pembahasan

Aksi Global Cyber-terrorism

Cyber-terrorism merupakan konvergensi dari terorisme dan *cyberspace* (Denning, dalam Gordon & Ford, 2003:3). *Cyber-terrorism* merupakan penggunaan peralatan jaringan komputer untuk mengganggu sistem infrastruktur Negara (energi, transportasi, operasional pemerintahan, dan sejenisnya) atau untuk mengintimidasi pemerintahan atau sekelompok masyarakat sipil (Lewis, 2002: 1; Tan, 2003:12). *Cyberspace* merupakan metode pengiriman pesan yang menarik untuk teroris. Akses dengan *cyberspace* lebih mudah diperoleh dibandingkan media konvensional. Hanya satu yang dibutuhkan, yakni komputer yang terhubung dengan Internet. Namun, *cyberterrorist* juga memerlukan level tinggi untuk menguasai komputer. (Brenner, 2002:150) Kemampuan *cyberspace* yang dapat ditembus juga memfasilitasi *cyber-terrorism* (David R & David G, dalam Brenner, 2002:150).

Cyberspace dapat digunakan untuk mengalahkan sistem dan menghindari inspeksi.

Teroris di beberapa Negara dapat bertukar *e-mail* dengan sedikit ketakutan akan diawasi. Teroris bisa bertemu secara *online* dan menghindari pengecekan imigrasi dengan menggunakan *cyberspace*. Jadi, *cyberspace* menawarkan para teroris keamanan yang lebih kuat dan fleksibilitas operasional. Mereka dapat melancarkan serangan dari hampir semua tempat di dunia tanpa secara langsung mengekspos diri mereka yang membahayakan diri mereka secara fisik. (Brenner, 2002: 150). Mereka tidak terhambat oleh regulasi lagi. Bahkan, pada tahun 2002 menurut peneliti *Microsoft*, mereka memiliki taktik dengan sering kali menghilang begitu saja secara cepat dan mengganti situs mereka dengan alamat yang berbeda lagi dengan tujuan menghindari pengawasan dari pihak pemerintah maupun intelejen tapi konten tetap sama (Seib&Janbek, 2011: 59).

Selain itu, *cyberspace* juga menawarkan teroris kemampuan untuk menyerang secara struktur dengan ketepatan yang tinggi. Penggunaan Internet oleh teroris memberikan cara yang murah untuk mereka menyebarkan propaganda mereka tanpa mempermasalahakan faktor geografis yang jauh maupun sulit dijangkau (Takwani, 2002:146). Adanya Internet, video-video aksi terorisme mereka dapat dilihat jutaan orang, berbagai gambar dan perkataan mampu tersebar secara bebas tanpa ada *gatekeeper* yang harus mereka lalui seperti media massa. Al-Qaeda mengadopsi Internet sebagai medium yang terbaik untuk mengirim dan menerima pesan pada audiens yang tersebar di beragam tempat di dunia. (Seib & Janbek, 2011:26).

Penggunaan *cyberspace* juga membiarkan teroris mengirimkan sebuah serangan yang mencakup beberapa serangan yang berurutan hanya dari satu tempat. Teroris bisa melaksanakan aksinya dari jarak yang sangat jauh, bahkan beda benua atau Negara dengan Internet. Bahkan juga jika mereka menggunakan komputer dekat dengan area sasarannya, teroris tidak perlu ada ditempat lokasi sehingga penggunaan *cyberspace* berarti aksinya tidak perlu mengorbankan anggota mereka. (Brenner, 2008:153). Di Timur Tengah, *website* dari kelompok militan Islam, Hezbollah, diciptakan oleh para pendukung Hamas untuk mengumumkan pembunuhan mereka terhadap sekelompok Yahudi. *Cyber war* terjadi antara pihak Arab dengan Yahudi. (Takwani, 2002:146). Selain itu, serangan secara *cyber* terjadi

pada komputer militer Amerika Serikat ketika berada di Kosovo dalam rangka melindungi Negara tersebut dari serangan Serbia untuk meninggalkan Negara tersebut. (Lewis, 2002:8). Bahkan, secara lebih detail bukan hanya propaganda saja, Internet digunakan sebagai media publikasi untuk penggalangan dana, membicarakan target, dan koordinasi melakukan serangan. (Banez, 2010:3). Para teroris pun semakin pintar menggunakan fasilitas perpustakaan *online* dimana banyak informasi didalamnya tentang material maupun cara membuat bom (Seib & Janbek, 2011:26). Bahkan, kemungkinan mereka bisa membuat perpustakaan *online* sendiri yang terselubung dan menjadi sumber berbagai anggota kelompok teroris untuk melakukan aktivitas terorismenya. Kelompok teroris di seluruh dunia bisa mengaksesnya dengan mudah.

Pada tahun 1996, kelompok Hamas Palestina dilaporkan melakukan “chat room dan e-mail” untuk merencanakan dan berkoordinasi dalam operasinya di Gaza dan Lebanon. Selama periode yang sama, Hezbollah Lebanon membangun sejumlah situs untuk melaporkan keberhasilan serangannya melawan Israel. Internet menguntungkan untuk komunikasi dan operasional mereka. Kelompok Al-Qaeda memiliki situs salah satunya *www.alneda.com*, akan tetapi setelah terjadi peristiwa 9/11 situs tidak terdeteksi lagi, tidak terdapat gambar Al-Qaeda (Weimann, dalam Banez, 2010: 18). Maka, terjadi pergerakan teroris secara *online (terrorism movement)* dari satu alamat situs ke alamat lain, dari satu sistem *online* ke sistem lain. Mereka bisa mengganti sistem mereka dengan mudah ketika mereka mulai terdeteksi oleh pihak pemerintah, khususnya pihak pemerintah dan militer Amerika Serikat.

Berdasarkan temuan Seib dan Janbek (2011:31) dalam bukunya “Global terrorism and New Media” menyatakan bahwa Al-Qaeda memiliki produksi operasional sendiri untuk konten *online* yang disembarkannya, yang bernama As Sahab (*The Clouds*) yang berfungsi dengan dibawah keamanan yang sangat ketat. Video Osama Bin Laden, Zawahiri, atau juru bicara Al-Qaeda lainnya yang tertembak di lokasi yang terisolasi dibawa menuju tempat yang aman untuk di-*upload* di Internet dan kemudian video dikirimkan ke fasilitas produksi terakhir Al Sahab, dimana video tersebut di-*edit* secara grafis dan tambahan *subtitle*-nya. As Sahab menggunakan

peralatan seperti Laptop Sony Vaio dan *software* yang sangat tinggi kualitasnya dalam melindungi data mereka. Produk video tahap akhirnya adalah video dibawa oleh seorang kurir ke warnet dan di-*upload* pada beragam situs afiliasi Al-Qaeda. Alamat-alamat Internet tersebut di-*publish* melalui berbagai forum dan ruang *chatting*. Kemudian pengikut Al-Qaeda meng-*copy*-nya dan mendistribusikannya. Sistem ini sudah digunakan sejak tahun 2005, yakni sejak Al-Qaeda berhenti mengirimkan videonya pada stasiun televisi Al-Jazeera dan organisasi pemberitaan lainnya, yang suka meng-*edit* tidak sesuai faktanya, bahkan menghilangkan video yang dikirimkan oleh Al-Qaeda.

Sebenarnya pemanfaatan Internet oleh teroris bukan hanya dari kelompok teroris Al-Qaeda saja, akan tetapi kelompok lain juga menggunakan seperti Taliban dan Hizbut Tahrir. Namun, keberadaan media *online* mereka tidak semahir, sekuat dan sebanyak Al-Qaeda (Seib & Janbek, 2011: 39). Dengan demikian, seperti yang disimpulkan oleh pihak *United Nations Office on Drugs and Crime* bahwa penggunaan Internet oleh teroris didasari beberapa tujuan yang mereka harus capai, mencakup penyebaran propaganda (termasuk rekrutmen, radikalisasi, penghasutan), mencari dana, pelatihan, perencanaan (melalui komunikasi rahasia dan informasi terbuka), eksekusi, dan *cyberattack* (2012: 3). Penggunaan media berbasis Internet ini menunjukkan bahwa para teroris memahami media sebagai alat strategi dan taktik dalam aktivitas teroris mereka. Penggunaan Internet oleh teroris dalam berbagai bentuk pesan baik secara audio visual, gambar, maupun kata-kata secara simultan dan kontinu bertujuan agar masyarakat dunia tetap sadar akan eksistensi para teroris.

Beragam New Media Cyber-terrorism: Online Game, Website, Youtube, Social Media, dan Majalah Online

Terorisme global menggunakan berbagai jenis new media dalam beberapa cara untuk menghasilkan publisitas dan menarik perhatian publik. (CBC News, 2012). Keberagaman media yang digunakan tersebut disesuaikan dengan target audiens yang mereka ingin komunikasikan. (Lumbaca&Gray, 2011: 46). Tokoh Al-Qaeda yang sangat aktif menggunakan aplikasi Internet dalam aktivitas terorismenya adalah Al-Awlaki, yang lahir di *New Mexico* dan mendapatkan

gelarnya dari Universitas Colorado dan Universitas San Diego (Seib & Janbek, 2011: 38). Penggunaan media Internet yang sangat tampak jelas digunakan secara terang-terangan dan bisa diakses seluruh warga dunia secara bebas adalah *Website, Youtube, social media* dan majalah *online*. Ditambah *online game* diduga oleh para intelejen juga sebagai media mereka berkoordinasi dalam menyusun strategi. Beragamnya aplikasi media *online* digunakan secara maksimal oleh para teroris untuk aktivitas mereka.

Youtube

Pertama, *Youtube*. *Youtube* menjadi satu bagian media *online* yang paling efektif mereka karena selain mampu mencapai publik secara luas, *youtube* juga mampu menyampaikan pesan mereka secara audio visual tanpa dimanipulasi oleh media massa. Para kelompok teroris sering menggunakan *Youtube* untuk memberitakan aktivitas mereka. Jika bisa di-*browsing* banyak sekali video terorisme yang muncul. Seperti kabar terakhir bahwa kelompok Al-Qaeda meng-*upload* video di *Youtube* yang memperlihatkan Al-Qaeda menyelenggarakan sebuah pertemuan akbar di Yaman baru-baru ini (Patnistik, 2014). Para analis tengah memeriksa mobil putih dalam video itu, yang memimpin konvoi. Video tersebut awalnya muncul di beberapa situs jihad yang kemudian diunggah di Youtube. Wajah beberapa anggota Al-Qaeda dalam video itu dibuat kabur. Hal itu menunjukkan kekhawatiran akan adanya

rencana serangan baru. Alasan Al-Qaeda merilis video tersebut, menurut Bergen, analis keamanan nasional Amerika, berspekulasi bahwa kelompok itu melakukannya untuk tujuan propaganda, untuk menunjukkan bahwa mereka masih beroperasi meskipun Osama Bin Laden meninggal.



Gambar 1. Gambar dari sebuah video yang memperlihatkan Al Qaeda menyelenggarakan sebuah pertemuan akbar di Yaman baru-baru ini.
Sumber: Patnistik, 2014

Website

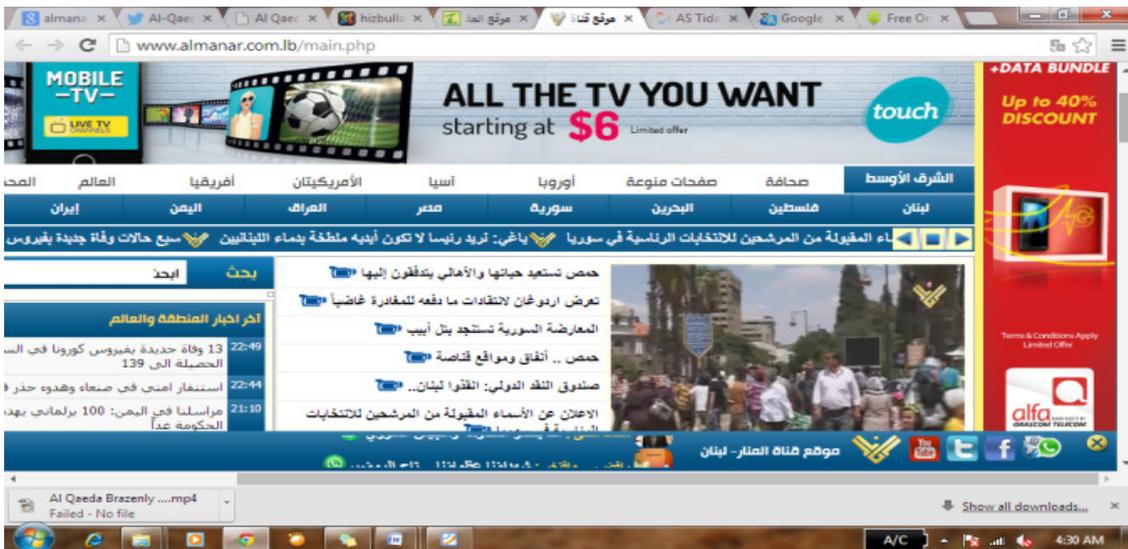
Kedua, *Website*. *Website* di-*posting* oleh berbagai kelompok teroris dengan tujuan-tujuan tertentu. Beberapa seperti *jihad.net* dan *alotswa.org* yang dibuat oleh pendukung Al-Qaeda untuk menunjukkan dukungannya pada Osama Bin Laden, sementara seperti *7hj.7hj.com* mengajari penggunaan *hacking* untuk melayani organisasi Islam (Ashley, dalam Tan, 2003:3). Namun, untuk saat ini ketiga situs tersebut tidak bisa diakses kembali. Sedangkan, Hizbullah



Gambar 2. Website Hizbullah sebagai pusat media kelompok teroris Hizbullah
Sumber: hizbulla.org.lk



Gambar 3. Website moqawama sebagai media yang menggambarkan serangannya melawan Israel
Sumber: <http://www.moqawama.org/>



Gambar 4. Website almanar sebagai media yang menyediakan berita dan informasi
Sumber: <http://www.almanar.com.lb/main.php>

diketahui mengoperasikan tiga situs sejak Februari 1998: *hizbullah.org* digunakan sebagai pusat kantor media, *moqawama.org* menggambarkan serangannya melawan Israel, dan *almanar.com.lb* menyediakan berita dan informasi (Denning, dalam Tan, 2003:9). Situs-situs tersebut berfungsi mempublikasikan sejarah, misi, ideologi, dan keseluruhan tujuan mereka dalam memusnahkan musuhnya. Ditambah, *website* tersebut digunakan sebagai situs penggalangan dana dengan harapan terkumpul dana dari individu dan pemerintahan yang bersimpati pada aksi mereka (Hoffman, dalam Lumbaca&Gray, 2011:48). Donasi

diterima secara *online* yang bisa menggunakan “Pay Pal” (Kaplan, dalam Lumbaca&Gray, 2011:48). Abu Musab al-Zarqawi’s Al-Qaeda di Iraq cukup pandai dalam menggunakan *website* yang mereka gunakan untuk mem-*posting* rekaman video mereka mengebom, mutilasi, dan menculik korban mereka. (Lumbaca&Gray, 2011:48)

Online Game

Ketiga, *Online Game*. Cara yang juga semakin populer menyamarkan pesan yang tidak berbahaya untuk para teroris berkomunikasi secara *online*



Gambar 5. Online Game World of Warcraft
Sumber: (Gross, 2013)

sebagai “gamer” dalam *game online*. Banyak forum *online* yang dienkripsi dan membutuhkan *password* untuk bergabung. Beberapa mungkin akan disusupi oleh agen-agen intelijen pemerintah yang menyamar sebagai militan *online* untuk mengetahui aksi para teroris tersebut. (Gardner, 2013). Mereka melebarkan penggunaan media mereka untuk semakin luas jangkauan atau semakin efektif komunikasi antar para anggotanya hingga membuat pihak NSA dan pemerintah Inggris menyusup secara besar-besaran ke dalam *game online multi-player role-playing* (MMORPG) seperti *World of Warcraft* dan *Second Life* untuk memata-matai komunikasi antar teroris tersebut. Fakta tersebut diungkapkan oleh mantan anggota NSA, Edward Snowden, yang dimana dokumen rahasia tersebut dia berikan pada majalah Inggris *The Guardian* dan *New York Times*. (Gross, 2013). Bahkan, tindakan militer tersebut dilindungi oleh hukum. Jika tidak diimbangi dengan kemampuan analisis yang kuat dalam permainan *game* untuk mengikuti gerakan teroris, maka mereka hanya melakukan pengawasan secara massa.

Game online Second Life digunakan untuk memata-matai adanya pencucian uang oleh para teroris tersebut yang tanpa bank mereka dapat memperoleh dana. Menurut Jeff Hermes, Direktur Hukum Proyek Digital Media dan Jaringan Hukum Media Online Berkman Harvard Center

untuk Internet dan Masyarakat mengungkapkan bahwa mereka berusaha menjual uang yang mereka peroleh dari permainan *games* tersebut. (Lejacq, 2013). Sedangkan, untuk *game online World of Warcraft* digunakan sebagai media untuk membicarakan strategi penyerangan. Adanya *game online* tersebut mereka bisa memanipulasi pemerintah dan pihak intelejen dengan identitas palsu. Pihak intelejen Amerika tersebut ingin mengetahui rencana aksi terorisme terbaru mereka. Setelah diketahui rahasia tersebut, perusahaan IT dunia seperti *Microsoft, Google, Facebook, Yahoo, Apple, Twitter* dan *LinkedIn* menyampaikan pernyataan publik meminta agar pemerintah dunia memberhentikan pengawasan secara *online* tersebut. Menurut mereka, tindakan mata-mata pemerintah tersebut mengganggu privasi konsumen *game* dan kenyamanan mereka dalam bermain *game online*. (Gross, 2013).

Selain itu, ditemukan oleh The Sun (*Foxnews*, 2012) teroris menggunakan *game online* seperti *Call of Duty* untuk *plot* dan mendiskusikan serangan selanjutnya secara pribadi. *Online game* memungkinkan pemainnya untuk *log in* dalam sebuah grup untuk saling menyerang maupun berdiskusi. Mereka biasanya masuk dalam sebuah grup *game online* dan mendiskusikan *plot* aksi teror yang akan mereka lakukan. Beragam gaya dan misi terdapat dalam permainan *games* tersebut mulai dari menanam bom hingga bertarung satu lawan satu.



Gambar 6. Salah satu scene Online Game Call of Duty
Sumber: (The Sun, 2012)

Social Media

Keempat, *Social Media*. Teroris berusaha menggunakan beragam jenis *social media* yang



Gambar 7. Facebook Kelompok Hizbullah
Sumber: www.facebook.com/Hizbullahorglk

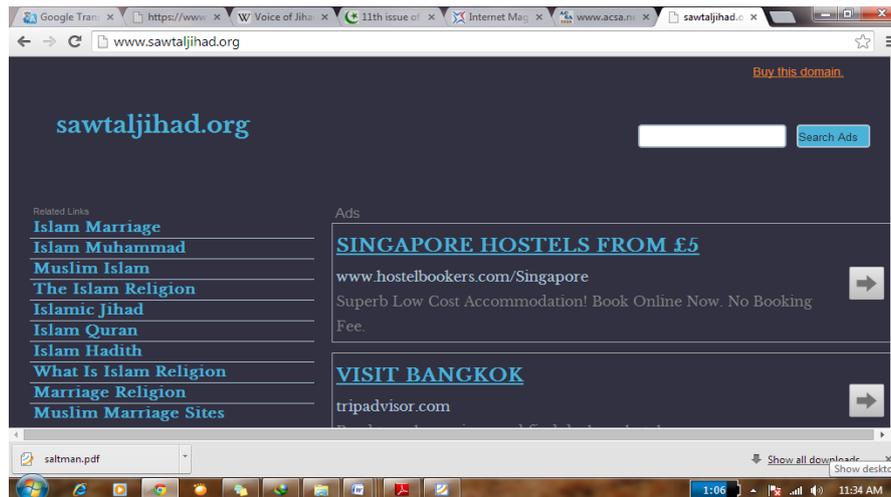


Gambar 8. Twitter AQIM dari hanya 5.000 follower hingga 37.800 follower
Sumber: <https://twitter.com/AkimSalatak>

mencakup *twitter* dan *facebook*. Berdasarkan penelitian terbaru, kelompok teroris internasional yang menantang Negara Barat, seperti Al-Qaeda, Hamas, dan Hezbollah bergantian melakukan perekrutan melalui jaringan sosial seperti *facebook* dan *twitter* untuk menarik berbagai kalangan dan mengumpulkan intelejen. Saat ini menurut Gabriel Weimann dari Universitas Haifa mengungkapkan bahwa hampir 90% organisasi teroris menggunakan Internet melalui *social media*. Dengan menggunakan alat tersebut, organisasi dapat secara aktif melakukan *recruitment* tanpa batasan geografis. *Social media* memungkinkan mereka mengambil inisiatif membuat permintaan untuk menjadi “teman”, meng-*upload* video, dan mereka tidak lagi menggunakan

alat pasif lagi seperti di *website*. (CBC News, 2012). Hal ini karena memang *Website* cenderung satu arah dibandingkan dengan *social media* yang bersifat interaktif atau sudah berbasis *Web 2.0* bahkan *Web 3.0* karena sudah masuk dalam ideologi mereka. *Facebook* dan *twitter* dijadikan forum oleh mereka dalam berkomunikasi antar anggotanya, *recruitment*, dan bahkan kita bisa melihat intruksi mereka dalam membuat bom.

Pada Bulan Maret 2013, *Al Qaeda in the Islamic Magreb* (AQIM) meluncurkan akun *Twitter* yang mendapatkan lebih dari 5.500 *follower*, dan akun AQIM yang *following* tujuh orang termasuk kelompok teroris akun *twitter* resmi Somalia Al Shabaab dan



Gambar 9: Tampilan situs majalah online milik Al-Qaeda *Sawt al-Jihad (Voice of Jihad)*
Sumber: <http://www.sawtaljihad.org/>

al Nusra di Suriah, yang pada gilirannya mengikuti kelompok pemberontak lain di Aleppo. Jean Paul Rouiller dari *the Geneva Centre* untuk *the Training and Analysis of Terrorism* mengatakan bahwa *social media* merupakan media yang vital untuk organisasi teroris modern. Pihak intelejen Inggris seperti MI5, dan organisasi mata-matanya GCHQ dan MI6 selalu memonitor berbagai akun *social media* termasuk *facebook* dan *twitter* yang diduga sebagai akun milik kelompok teroris. Mereka bertukar informasi dan taktik melalui akun *social media* mereka. (Rivers, 2013).

Selain rekrutmen, menurut Weimann, *facebook* digunakan untuk mengumpulkan informasi tentang inteligen miter dan politik. Terkadang banyak orang yang tidak memperdulikan identitas seseorang yang mereka terima sebagai teman *social media* dan para teroris bisa menggunakan profil palsu untuk mendekati kelompok atau individu yang potensial untuk mendukung aksi dan menambah kekuatan mereka dalam keterampilan maupun pengetahuan yang relevan dengan tujuan mereka. Sebagai contohnya, Weimann mengatakan bahwa terdapat pernyataan dari Lebanon bahwa Hezbollah mencari bahan tentang aktivitas militer Israel dalam *facebook*. Negara-negara seperti Amerika Serikat, Kanada, Inggris telah mengintruksikan anggota militernya untuk menghapus informasi pribadi mereka yang terdapat dalam *facebook* jika tidak, maka Al-Qaeda akan mengawasinya (CBC News, 2012).

Majalah Online

Selain keempat media tersebut, mereka juga memiliki *Sawt al-Jihad (Voice of Jihad)* adalah sebuah majalah *online* yang pertama kali muncul pada tahun 2004 untuk mempromosikan pencapaian mujahidin. (Seib & Janbek, 2011: 27). Alamat situs majalah ini adalah <http://www.sawtaljihad.org/> dan dikelola oleh Komite Al-Qaeda di Saudi Arabia dalam Bahasa Inggris. Isinya berbagai isu yang berkaitan dengan aksi jihad mereka mulai dari posting tulisan hingga link “Islamic Video” dan “Jihad Video”. (Saltman, 2008:6). Namun, jika diakses saat ini, tampilan situsnya tidak lagi seperti sebuah majalah *online* seperti yang tampak dibawah ini. *Link* yang disediakan pun jika diakses seperti “Islamic Jihad” juga tidak masuk pada konten yang berkaitan dengan jihad, tapi menuju konten yang diluar konteks Islam dan Jihad.

Meskipun demikian, adanya majalah *online* ini membuktikan bahwa Al-Qaeda sebagai kelompok teroris yang memiliki beragam media *online* dalam mengkomunikasikan komunitasnya pada dunia. Mereka berusaha menyebarkan ideologi mereka dari segala arah dan segala segmentasi media. Berbagai cara teroris melalui penggunaan beragam media Internet ini mendorong pembaca atau *user* lebih *concern* pada *cybersecurity*.

Fenomena Cyber-terrorism di Indonesia

Indonesia menjadi salah satu Negara yang selalu diidentikkan dengan sarang teroris oleh dunia.

Hal ini tidak mengherankan karena telah banyak aksi teroris yang terjadi di Indonesia selama beberapa tahun. Indonesia memiliki banyak kemungkinan *cyber-terrorism* bisa dilakukan dengan bebas dan meluas. Hal ini disebabkan dengan regulasi tentang *cyber crime* tidak terlalu kuat. Bahkan, belum ada regulasi khusus yang mengatur tentang *cyber-terrorism*. Pemerintah Indonesia dengan anggota intelegennya juga belum kuat dalam penguasaan perangkat teknologi jaringan komputer dalam mendeteksi *cyber-terrorism*. Meskipun mereka berhasil menemukannya, mereka masih tidak mampu mengatasinya sehingga aksi terorisme di Indonesia hingga kini terus bertambah. Indonesia sangat lemah dalam perlindungan data Internet.

FBI secara resmi mengindikasikan bahwa kelompok ekstremis atau garis keras menggunakan identitas untuk mencuri dan melakukan penipuan kartu kredit untuk mendukung aktivitas terorisme mereka. Berdasarkan laporan media, kepolisian Indonesia meyakini bahwa pengeboman Bali tahun 2002 oleh sekelompok teroris sebagian didanai melalui penipuan kartu kredit secara *online*. (Rollins&Wilson, 2007:5). Serangan di Bali dan beberapa Negara juga kemungkinan didanai melalui pencurian kartu kredit. (Rollins&Wilson, 2007:18). Imam Samudra dinyatakan bersalah dan dihukum eksekusi mati untuk kejadian pemboman dua kali di Bali pada tahun 2002 menulis buku "Aku Melawan Terroris!" yang dilaporkan juga di-*translate*-kan dalam bahasa Inggris "Me Against the Terrorist". Samudra mendorong remaja Muslim secara aktif mengembangkan kemampuan *hacking*-nya untuk menyerang jaringan komputer Amerika Serikat. Samudra menyebutkan beberapa situs dan *chat room* sebagai sumber-sumber mereka untuk meningkatkan kemampuan *hacking* mereka. Samudra mendesak remaja Muslim untuk mendapatkan angka pin kartu kreditnya dan menggunakannya untuk mendanai perjuangannya melawan Amerika Serikat dan sekutunya.

Menurut tim penyidik, Samudra menggunakan laptop untuk berkomunikasi dengan kelompok ekstremis beberapa bulan sebelum melakukan pemboman. Pembicaraan mereka termasuk bagaimana secara curang menggunakan kartu kredit *online* untuk transfer uang yang digunakan sebagai dana serangan. Kepala unit kejahatan Indonesia, Kolonel Petrus

Golose, menyatakan Agung Prabowo, yang juga merupakan pembantu Imam Samudra, sebagai *hacker professional*. Agung Prabowo menciptakan sebuah situs yang digunakan untuk membunuh para warga Asing tanpa berada di lokasi serangan. (Voanews, 2009).

Situs garis keras atau ekstremis lainnya juga seringkali menyediakan *link* antara satu sama lain untuk meyakinkan rasa partisipasi dalam perjuangannya di seluruh dunia. Situs seperti itu digunakan oleh kelompok Laskar Jihad Indonesia, contohnya mereka telah terhubung dengan berbagai situs jihad yang berhubungan dengan Palestina, Afganistan, Chechya, dan tempat lainnya. (Seib & Janbek, 2011:41). Pada Mei 2001, Laskar Jihad melakukan aksi *cyber-terrorism* dengan meng-*hack* situs kedutaan besar Australia dan kepolisian Indonesia di Jakarta sebagai bentuk protes tertangkapnya pemimpin mereka, Ja'far Umar Thalib. Setiap akses situs keduanya, mereka mengarahkannya pada situs lainnya yang berisi peringatan kepada kepolisian Indonesia untuk membebaskan pemimpin mereka (Irwin, 2004: 83). Semua ini membuktikan bahwa teroris di Indonesia juga telah masuk era *new media*.

KESIMPULAN

Berdasarkan pembahasan yang telah diuraikan maka dapat diambil beberapa kesimpulan. Pertama, aksi global cyber-berterrorism seiring dengan kecanggihan teknologi era digital semakin menguat dan semakin beragam aksi yang bisa dilakukannya. Sejauh ini, aksi *cyber-terrorism* dilakukan mulai dengan mengintimidasi pemerintah dan masyarakat sipil dengan mengganggu sistem jaringan infrastruktur; melakukan serangan, pembunuhan, dan propaganda dengan akurasi yang tinggi tanpa terdeteksi tempat dan media yang digunakan; mengumumkan berbagai aksi radikal pembunuhan dan terror melalui video maupun gambar secara *online* yang disebarakan melalui akun pribadi mereka; pembuatan online library untuk anggota teroris dalam berbagi ilmu pembuatan bom dan berbagai senjata ilegal; dan melakukan *hack* terhadap beberapa jalur pendanaan. Secara teknologi, jaringan teroris Al-Qaeda dalam aksi *cyber-terrorism* lebih mahir, kuat dan banyak jumlahnya dibandingkan dengan jaringan teroris lainnya.

Kedua, beragam New Media digunakan dalam aksi *cyber-terrorism* yang sejauh ini terdeteksi

digunakan oleh mereka diantaranya *youtube, website, online game, facebook, twitter*, dan majalah *online*. Ketiga, Indonesia merupakan salah satu Negara yang sering diidentikan dengan aksi radikal terorismenya. Aksi *cyber-terrorism* di Indonesia terdiri dari pencurian dan penipuan kartu kredit untuk mendukung pendanaan dalam aksi terorismenya; penyerangan jaringan komputer atau hacking situs-situs asing khususnya yang berbau Amerika Serikat; dan penciptaan situs *online* untuk melakukan pembunuhan tanpa berada dilokasi.

DAFTAR PUSTAKA

- Banez, Justin D. (2010). The Internet and The Homegrown Jihadist Terrorism: Assessing U.S. Detection Techniques (Thesis, Naval Postgraduate School, California). Retrieved from <https://www.hsdl.org/?view&did=11245>
- Brenner, Susan W. (2002). *Cyber-terrorism: How real is the Threat?*. *Media Asia*, 29 (3), 149-154. doi: <https://doi.org/10.1080/01296612.2002.11726680>
- CBC News. (2012, January 10). Terrorist groups recruiting through social media. Retrieved from <http://www.cbc.ca/news/technology/terrorist-groups-recruiting-through-social-media-1.1131053>
- Ganor, Boaz. (2002). Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?. *Police Practice and Research: An International Journal*, 3 (4), 287-304. doi: <https://doi.org/10.1080/1561426022000032060>
- Gardner, Frank. (2013, November 2). How Do Terrorists Communicate?. Retrieved from <http://www.bbc.com/news/world-24784756>
- Gordon, S. & Ford, R. (2003). *Cyber-terrorism?*. Retrieved from www.symantec.com
- Gross, Daug. (2013, December 10). Leak: Government spies snooped in 'Warcraft,' other games. Retrieved from <http://edition.cnn.com/2013/12/09/tech/web/nsa-spying-video-games/>
- Hendropriyono, A.M. (2009). *Terorisme: Fundamentalisme, Yahudi, Islam*. Jakarta: PT Kompas Media Nusantara.
- Irwin, Jones. (2004). *War and Virtual War: The Challenges to Communities*. Amsterdam: Rodopi.
- Lejacq, Yannick. (2013, December 12). NSA's virtual waste of time? Spying in 'World of Warcraft' is harder than you think. Accessed from <http://www.nbcnews.com/tech/video-games/nsa-virtual-waste-time-spying-world-warcraft-harder-you-think-f2D11724106>
- Lewis, J. A. (2002, December). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic and International Studies*, 1-12.
- Lumbaca, S. & Gray, D.G. (2011). The Media As An Enabler For Acts Of Terrorism. *Global Security Studies*, 2 (1), 46-54.
- Patnistik, Egidius. (2014, April 17). AS Tidak Tahu Pertemuan Puncak Al Qaeda di Yaman?. Retrieved from <http://internasional.kompas.com/read/2014/04/17/1027450/AS.Tidak.Tahu.Pertemuan.Puncak.Al.Qaeda.di.Yaman>.
- Rivers, Dan. (2013, April 28). Terrorists use Twitter as a tool. Retrieved from <http://edition.cnn.com/2013/04/27/world/rivers-social-media-terror/>
- Rollins, J. & Wilson, C. (2007, January 22). Terrorist Capabilities for Cyberattack: Overview and Policy Issues. Retrieved from <http://www.fas.org/sgp/crs/terror/RL33123.pdf>
- Saltman, Samuel S. (2008). The Global Jihad Network: Why and How al-Qaeda Uses Computer Technology to Wage Jihad. *Journal of Global Change and Governance*, 1(3), 1-10.
- Seib, P. & Janbek, D.M. (2011). *Global Terrorism and New Media: The post-Al Qaeda generation*. New York: Routledge Taylor & Francis Group
- Soriano, Manuel R.T. (2008). Terrorism and the Mass Media after Al Qaeda: A Change of Course?. *Athena Intelligence Journal*, 3 (2), 1-20.
- Sukarno, Adam W. (2011). Dilema Peliputan Terorisme dan Pergeseran Pola *Framing* Berita Terorisme di Media Massa. *Jurnal Ilmu Sosial dan Ilmu Politik*, 14(3), 333-348. doi: 10.22146/jsp.10932

- Tan, K.L.G. (2003, December). *Confronting Cyber-terrorism with Cyber Deception* (Thesis, Naval Postgraduate School, California). Retrieved from <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-017.pdf>
- The Sun. (2012, March 20). Terrorists use online games like 'Call of Duty' to plot attacks. Retrieved from <http://www.foxnews.com/tech/2012/03/20/terrorists-use-online-games-like-call-duty-to-plot-attacks/>
- United Nations Office on Drugs and Crime. (2012). The use of the Internet for terrorist purpose. Retrieved from https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
- Voanews. (2009, October 31). Indonesian Police Charge Two Suspects with Cyber-Terrorism. Retrieved from <http://www.voanews.com/content/a-13-2006-08-23-voa32/400055.html>