POTENSI PENGGUNA INTERNET INDONESIA DALAM *COUNTER-CYBER RADICALIZATION*

INDONESIA'S NETIZEN POTENTIAL ON COUNTER-CYBER RADICALIZATION

Rizky Reza Lubis [1]

Alumni Universitas Pertahanan Indonesia
(rizkyrezalubis@gmail.com)

Abstrak – tulisan ini menjelaskan proses radikalisasi yang terjadi di dunia maya, dengan melihat bagaimana dan mengapa masyarakat Indonesia rentan menjadi target organisasi teroris khususnya dalam hal perekrutan melalui dunia maya. Teroris tidak hanya memanfaatkan akses internet sebagai sarana komunikasi, tetapi juga memanfaatkannya sebagai sarana dalam menyembunyikan identitas dan lokasi saat menyebarkan ideologi radikal. Konsep yang digunakan dalam tulisan ini adalah *cyber radicalization*, yang merupakan konsep baru yang terbentuk dari konsep ancaman cyber dan radikalisasi. Adapun hasil dari tulisan ini menunjukkan bahwa pengguna internet Indonesia memliliki potensi yang besar untuk melawan radikaslisasi di dunia maya dan memilki kapasitas dalam mendukung agenda *counter terrorism* di dunia maya. Namun, hal tersebut masih menghadapi beberapa tantangan, sehingga diperlukan pemanfaatan pengguna internet oleh pemerintah secara maksimum dalam agenda *counter-cyber radicalization.*

Kata Kunci : *cyber*, radikalisasi, terorisme, Indonesia

Abstract – *This paper discusses the process of radicalization in cyberspace. It will look at how and why Indonesia are vulnerable in society and targeted by terrorist organizations in an attempt to recruit them, especially in cyberspace. The terrorists have become expert, not only using the latest tools of internet communications, but to do it in a way that can shield their identities and even their locations when spreading the radical ideology. The concept that used in this paper is cyber-radicalization, which is the new concept that merged from cyber threat and radicalization. The result from this paper shown that Indonesia netizens (internet users) had great potency to fight radicalization in the cyberspace and thecapacity for supporting government counter-cyber radicalization agenda. However, fighting cyber radicalization in that way faced several challenges. Therefore Indonesia's government should benefited the netizens to reach the optimum point on counter-cyber radicalization agenda.*

Keywords: *cyber, radicalization, terrorism, Indonesia*

[1] Alumni Universitas Pertahanan Indonesia, Program Studi Diplomasi Pertahanan Cohort 2.

Pendahuluan

Awalnya internet diciptakan untuk memudahkan komunikasi antar kalangan akademik dan militer yang terhubung dalam jaringan *The Advanced Research Projects Agency Network (ARPANET)* pada tahun 1969.[2] Seiring dengan perkembangan Teknologi, Informasi (TIK), internet dapat digunakan secara bebas sebagai layanan publik untuk berkomunikasi. Namun, hal tersebut juga mengalami pergeseran fungsi, internet juga digunakan sebagai media dalam melakukan tindak criminal, salah satunya adalah aksiterorisme. Aksi teror yang dilaksanakandengan instrumen internet disepakati sebagai tindakan*cyber terrorism. Cyber terrorism* merupakan ancaman bagi pertahanan dan keamanan negara karena mampu melakukan perusakan *(destruction),* pengubahan (*alteration*)*,* dan akuisisi dan retransmisi (*acquisition* dan *retransmission)* pada objek nyata maupun jaringan *cyber*.[3]

Menurut Dorothy E. Denning, frasa *cyber terrorism* pertama kali tercipta pada tahun 1982 oleh Barry Collin yang menekankan definisinya pada situasi ketika bertemunya *physic world* (dunia fisik) dan *cyberspace*[4] (dunia maya), maka saat kejahatan atau tindak teror terjadi pada situasi tersebut dikatakan sebagai *cyber terrorism.*[5] Collin menegaskan bahwa pada *cyber warfare* (peperangan siber) masa depan akan melibatkan teroris yang menggunakan *cyberspace* untuk melakukan penyerangan terhadap infrastruktur penting. Dengan pesatnya perkembangan teknologi saat ini, sangat memungkinkan untuk terjadinya serangan hanya melalui sekali tekan tombol di komputer untuk merusak dan meledakkan infrastruktur yang memakan korban jiwa, kerugian materil dan dampak *disruptive* pada stabilitas negara.[6] Terkait dengan proses berdiri dan berjalannya suatu organisasi terorisme, cenderung tidak bisa dilepaskan dari perkembangan teknologi khususnya internet. Telah banyak terjadi kejahatan terorisme didalam *cyberspace*, titik awalnya pada tahun 1998 dimana setengah dari tiga puluh organisasi teroris yang ditetapkan oleh *U.S Antiterrorism and Effective Death Penalty Act of 1996* menggunakan situs internet untuk melakukan tindak terorisme.[7]

Pemanfaatan *cyberspace* dalam melakukan aksi teror merupakan ancaman yang nyata dan baru bagi beberapa negara.[8] Skenario terburuk dari hal tersebut adalah ketika suatu

[2] Petrus Reinhard Golose, *Seputar Kejahatan Hacking: Teori dan Studi Kasus*, (Jakarta: Yayasan Pengembangan Kajian Kepolisian Indonesia, 2008).

[3] Dorothy E. Denning, *Terror's Web: How the Internet Is Transforming Terrorism, Handbook on Internet Crime*, (New York: Willan Publishing, 2009).

[4] Kata *cyberspace* biasa juga disebut dengan *cyber world* yang berarti berada pada ranah dunia maya.

[5] Dorothy E. Denning, *op. cit.,* hlm. 194-212

[6] Clay Wilson, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress", *Focus on Terrorism*, Vol. 9, 2003, hlm. 1-42.

[7] Petrus Reinhard Golose, Invasi terorisme ke cyberspace. (Jakarta: YPKIK/Yayasan Pengembangan Kajian Ilmu Kepolisian, 2015).

[8] James Andrew Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, (Washington, DC: Center for Strategic & International Studies, 2002).

negara tidak hanya akan mengambil langkah yang sudah dikuasai mayoritas negara, yaitu pendekatan tradisional; militer menghadapi militer atau negara menghadapi negara. Namun musuh akan memiliki pola baru yang belum pernah terjadi sebelumnya, yaitu pemanfaatan *non-state actor* yang memicu peperangan asimetris, salah satunya adalah memanfaatkan kelompok teroris.[9] Teroris yang melakukan aksi di *cyberspace* dan mendapatkan dukungan dari suatu negara akan menjadi ancaman global. Negara yang diuntungkan dalam konteks ini adalah negara-negara yang memilki kemampuan teknologi yang unggul (didominasi negara-negara maju) dan mau secara serius memanfaatkan potensi yang terdapat di *cyberspace* sebagai elemen pertahanan dan keamanan negara.[10]

Menariknya, selain melakukan aksi-aksi teror, jaringan teroris memanfaatkan *cyberspace* sebagai media dalam menyebarkan paham-paham radikal atau yang disebut dengan radikalisasi. Terlepas dari banyaknya hal positif dari Internet, namun internet dengan segala fitur dan kebebebasan aksesnya (khususnya di negara demokrasi) menyediakan peluang untuk terjadi atau setidaknya mendukung radikalisasi secara efektif dan efisien. Adapun peluang tersebut mengacu pada penelitian Von Bher, Anais Reding, dan Edward Gribbon mengenai "radikalisasi di era digital" yang dielaborasi dengan analisa penulis, sebagai berikut:[11]

1. Internet yang menghubungkan masyarakat tanpa mengenal batas teritorial negara membuka peluang untuk menyebarkan dan menanamkan ideologi dan pemahaman radikal pada seluruh pengguna internet di dunia.
2. Internet sebagai *"echo-chamber"*, dimana internet menyediakan akses dengan mudah untuk memeperoleh beragam informasi, termasuk informasi mengenai terorisme. Informasi yang diperoleh tersebut akan terus berkembang dan menyebar ke media lainnya.
3. Internet menjadi akselerator radikalisasi. Pengguna internet yang memiliki pemahaman yang mengarahkan ke ideologi radikal dan ekstrem cenderung mendapat keteguhan hati untuk bergabung dengan jaringan teroris setelah mendapat materi-materi radikal di internet.
4. Internet memberikan jaminan keamanan yang lebih tinggi ketimbang radikalisasi di dunia nyata. Mengingat pengajaran ideologi radikal dapat dilakukan tanpa harus melakukan pertemuan langung. Hal ini akan memberi jaminan kerahasiaan pada identitas dan lokasi.

[9] David J. Kilcullen, "Three Pillars of Counter-insurgency", Pidato pada *the U.S Government Counterinsurgency Conference*, Washington D.C, 28 September 2006, dalam https://www.research-gate.net/publication/237538249_Three_Pillars_of_Counterinsurgency.

[10] James Andrew Lewis, *op.cit,* hlm. 4.

[11] Von Bher et. al., *Radicalization in the Digital Era*, (Santa Monica: RAND Corporation, 2013).

Dengan segala bentuk keuntungan yang disediakan internet dalam konteks radikalisasi di *cyberspace*, maka penanganan yang dilakukan pemerintah juga perlu berada ditataran *cyberspace.* Menariknya, bagi negara-negara demokrasi yang memilki tuntutuan untuk menjamin kebebasan berekspresi dan berserikat mengalami dilema ketika mengimplementasikan program *counter-cyber radicalization* atau upaya melawan radikalisasi di *cyberspace.* Negara tersebut tidak bisa secara brutal melakukan pemblokiran pada situs web dan media sosial mengingat akan melanggar beberapa hak warga negaranya. Selain itu, penilaian "teroris" dan "radikal" merupakan subjektivitas dari penilainya. Sehingga diperlukan proses penyaringan situs web dan akun media sosial secara sangat selektif. Pemerintah memerlukan cara kreatif untuk melakukan *counter-cyber radicalization* tanpa melanggar hak-hak warga negaranya.

Cyber Radicalization

Sebelum berangkat lebih jauh dalam membicarakan radikalisasi di *cyberspace*, pada dasarnya radikalisasi perlu dipahami bukan sebagai bentuk penyebaran teror, namun sebagai "proses" dalam mengembangkan ideologi dan kepercayaan ekstrimis. Mengacu pada Oxford Dictionary, radikalisasi merupakan aksi atau proses yang menyebabkan individu berada dalam posisi radikal dalam isu politik dan sosial.[12] Hal tersebut senada dengan definisi radikalisasi milik Wilner dan Dubouloz:[13]

> "Radicalization is a personal process in which individuals adopt extreme political, social, and/or religious ideals and aspirations, and where the attainment of particular goals justifies the use of indiscriminate violence. It is both a mental and emotional process that prepares and motivates an individual to pursue violent behavior".

Maka, dari definisi tersebut dapat dipahami bahwa radikalisasi sebagai sebuah "proses" dalam membuat individu mengadopsi pemikiran radikal yang berkonsekuensi menjadi aksi terorisme dan ekstremisme. Seiring dengan perkembangan teknologi, radikalisasi atau cara menyebarkan paham radikal juga mengalami perkembangan pada *cyberspace,* seperti yang telah disebutkan sebelumnya, yaitu *cyber radicalization*. Berikut fase-fase radikalisasi seiring dengan perkembangan teknologi:[14]

- Fase 1: tahun 1984, radikalisasi dimulai melalui khotbah/ceramah, koran/majalah yang diprint, dan rekaman video ceramah atau "perjuangan" dengan kekerasan.
- Fase 2: pertengahan tahun 1990an, situs-situs internet, contohnya seperti Al-Neda dan Azzam

[12] "Radicalization", Oxford Dictionary, dalam https://en.oxforddictionaries.com/definition/radicalization, 19 Juli 2017, diakses pada 19 Juli 2017

[13] Alex S. Wilner dan Claire-Jehanne Dubouloz,Homegrown terrorism and transformative learning: an interdisciplinary approach to understanding radicalization", *Global Change, Peace & Security*, Vol. 22, No. 1, 2010, hlm.33-51.

[14] Aaron Y. Zelin, Richard Borow Fellow, "The State of Global Jihad Online: A Qualitative, Quantitative, and Cross-Lingual Analysis",Washington Institute for Near East Policy, January 2013.

Publications.

- Fase 3: Pertengahan tahun 2000an, forum interaktif di *cyberspace*. Pada masa tersebut mulai bermunculan forum-forum *online* diskusi mengenai ideologi dan kepercayaan ekstrimis.
- Fase 4: akhir tahun 2000an; penyebaran paham radikal memasuki ranah media sosial seiring dengan meningkatnya pengguna media sosial. Adapun media sosial yang kerap kali digunakan adalah Facebook, Youtube dan Twitter.

Radikalisasi di *cyberspace* akan terus berlanjut mengingat proses penyebaran paham radikal dan propaganda akan lebih efektif dan efisien apabila dilakukan di *cyberspace. Cyber radicalization* akan menciptakan peluang untuk terjadinya *self-radicalization,* dimana individu menjadi teroris tanpa berafiliasi dengan kelompok radikal secara langsung namun mereka tetap mendapatkan pengaruh dari ideologi dan pesan para teroris tersebut, yang biasa disebut dengan teroris "*lone wolf*".[15]

Meski tidak bergerak secara kelompok, teroris yang tercipta dari *self-radicalization* merupakan ancaman yang serius. Terdapat kecenderungan kelompok teroris yang bergerak secara masif mendapatkan bantuan dari mereka yang melakukan *self-radicalization* dan bahkan mereka mendatangi kelompok tersebut untuk mengajukan diri sebagai anggotanya. Hal tersebut dapat terlihat darikasus Mohammed Atta dan tiga orang lainnya yang terlibat langsung pada penyerangan 9/11, menariknya, mereka sendiri berdomisili di Hamburg, Jerman yang kemudian melakukan perjalanan ke Pakistan.[16] Kemudian kasus lainnya pada bom bunuh diri di London tahun 2005 yang dilakukan oleh teroris yang merupakan warga negara Inggris sendiri. Hasil penyelidikan menunjukkan bahwa teroris tersebut mendapatkan pemahaman dari internet dan kemudian mengunjungi Al-Qaeda untuk mendapatkan pelatihan yang berujung pada aksi "Jihad" di negaranya sendiri.[17]

Adapun *cyber radicalization* memiliki beragam bentuk, pada tahap mempromosikan ideologi atau pemahaman kelompok teroris, mereka cenderung menggunakan sosial media dengan tautan yang mengarah ke situs web atau forum *online* yang memberikan informasi lebih mendetail ketimbang sosial media yang terlalu terbuka untuk umum. Situs web atau forum *online* tersebut beragam dan banyak bentuknya, serta cenderung memiliki ciri sebagai berikut;[18]

[15] "Self-Radicalization", Citizendium, dalam http://en.citizendium.org/wiki/Self-radicalization,23 September 2013, diakses pada 2 Juni 2017.

[16] Ruth Stein, *For Love of the Father: A Psychoanalytic Study of Religious Terrorism*, (Stanford: Stanford University Press, 2010).

[17] Bruce Hoffman, *Challenges for the U.S. Special Operations Command posted by the Global Terrorist Threat: al-Qaeda on the Run or on the March?*, (George Washington D.C: Middle East Policy, 2013).

[18] Anton Ali Abas, Paparan Mata Kuliah Media dan Terorisme, Program Studi Peperangan Asimetris, Universitas Pertahanan Indonesia, 13 Oktober 2015.

Tabel 1. Situs dan Forum Online Berpaham Radikal

Forum	Affiliation	Active Accounts
Shumukhal-Islam	AlQaeda	8,000
Al-Fida'	AlQaeda	10,000
Ansaral-MujahideenArabicForum	AlQaeda	5,500
Ansaral-MujahideenEnglishForum	AlQaeda	2,000
Al-Qimmah	Al-Shabaab	9,000
JamiaHafsaUrduForum	Tehrik-eTaliban Pakistan	2,100

Sumber: Anton Ali Abas, Paparan Mata Kuliah Media dan Terorisme, Program Studi Peperangan Asimetris, Universitas Pertahanan Indonesia, 13 Oktober 2015.

- Berisi konten yang bersifat persuasif dalam membenarkan kepercayaan dan ideologi teroris serta menegaskan kesalahan-kesalahan kepercayaan ideologi lain, termasuk ideologi yang dianut negara-negara sekuler.
- Terdapat berita foto, dan video yang menunjukkan penderitaan dan ketertindasan untuk menggalang simpati, namun terdapat juga yang menunjukkan "aksi" ekstremis.
- Memiliki dua atau lebih versi bahasa, hal ini menunjukkan target dari *cyber radicalization* adalah masyarakat global.
- Khusus untuk anggota/ menggunakan kata sandi *(password-protected)* agar bisa masuk dan melihat isi konten dari situs web tersebut. Hal tersebut dilakukan sebagai bentuk antisipasi dari organsasi teroris agar tidak dapat dilihat oleh pemerintah atau *cyber police.* Meskipun, *cyber police* akan sangat mudah untuk bisa memeriksa isi forum diskusi *online* yang menggunakan kata sandi atau privat namun jika tidak terbuka untuk publik, kemungkinan diketahui oleh *cyber police* akan lebih kecil.

Penggunaan situs web dan forum diskusi *online* merupakan pilihan yang efektif dalam melakukan perekrutan dan menggalang simpati. Hal ini dapat terlihat dari banyaknya anggota dari grup-grup *online* yang tertutup tersebut. Berikut adalah forum-forum diskusi secara internasional yang paling terkenal dan memilki anggota aktif yang banyak (lihat tabel 1).

Dalam mempromosikan situs-situs web dan forum diskusi *online* tersebut kelompok teroris cenderung menggunakan jaringan sosial media. Selain itu, sosial media dipahami sebagai instrumen yang cukup relevan dan efektif dalam *cyber radicalization*. Salah satu contohnya adalah kasus perekrutan

calon "jihadis" melalui Facebook untuk dikirim ke Suriah pada tahun 2014, diantaranya adalah WNI yang telah dideportasi dari Turki dan diperiksa sebagai saksi. Menurut keterangannya, mereka akan berangkat ke Suriah dengan mendapatkan akses dari pertemanan di Facebook. Awal mulanya, saksi tersebut mendapat undangan pertemanan di Facebook dengan seseorang yang tidak dikenal, saksi menerima pertemanan tersebut karena melihat tulisan-tulisan di halaman Facebook yang sangat Islami dan banyak bercerita mengenai daulah atau daerah kekuasan ISIS di Suriah. Pertemanan di Facebook tersebut berlanjut dengan memanfaatkan fasilitas *chat* secara personalyang pada akhirnya mendapatkan tawaran untuk berangkat ke Suriah.[19]

Contoh tersebut menunjukkan salah satu bentuk dalam mempromosikan ideologi radikal dan menggalang dukungan melalui sosial media. Sosial media yang paling sering digunakan adalah sosial media yang paling banyak peminatnya, dimana tiga teratas adalah Facebook, Youtube dan Twitter. Adapun karakter dari akun sosial media tersebut dalam konteks radikalisasi dapat dilihat pada tabel (lihat tabel 2).

Terkait penggunaan sosial media yang fungsi utamanya adalah berbagi video, seperti Youtube, *cyber-radicalization* dilakukan dengan menyebarkan video bertema-tema khusus. Terdapat enam kategori tema yang biasanya diunggah ke internet oleh

[19] Petrus Reinhard Golose, *op.cit.*

Tabel 2. Media Sosial sebagai Instrumen *Cyber Radicalization*

Facebook	*Multiple accounts* *Private Messaging and Chat* *Closed groups*
YouTube	*Media dissemination* *Validation* *Messaging*
Twitter	*Wide broadcast* *Multiple accounts* *Direct Messaging*

Sumber: Anton Ali Abas, Paparan Mata Kuliah Media dan Terorisme, Program Studi Peperangan Asimetris, Universitas Pertahanan Indonesia, 13 Oktober 2015.

kelompok teroris:[20]

1. Video operasional (pada saat mereka melakukan penyerangan).
2. Video dengan menunjukkan sandera *(hostage video)*
3. Video yang memberikan pernyataan atau *statement* yang mewakili kelompok mereka.
4. Video persembahan *(tribute video).*
5. Video ketika melaksanakan latihan bersenjata *(internal training video)*
6. Video yang memberikan instruksi kepada publik.

Cyber-radicalization melalui sosial media tersebut merupakan hal yang perlu diwaspadai karena paling mudah menyebar dan popular. Selain itu, mayoritas penggunanya adalah remaja yang belum memiliki kemapanan mental sehingga rentan menjadi target radikalisasi. Meskipun *cyber-radicalization* (serta segala hal yang berkaitan dengan terorisme lainnya) cenderung

[20] Anton Ali Abas, *op.cit.*

indikriminasi terhadap targetnya.

Cyber Radicalization di Indonesia

Semenjak kejadian runtuhnya *World Trade Center* (WTC) pada September 2011 dan khususnya pada peristiwa Bom Bali I, Indonesia telah menaruh perhatian serius terhadap isu terorisme dan turut aktif dalam kebijakan "*war on terror*" yang dicanangkan Amerika Serikat. Namun hal ini menjadi dilema sendiri. Bagi negara yang masih menghadapi masalah pengangguran dan kemiskinan seperti Indonesia, akan semakin rumit jika harus memilih mana yang didahulukan antara menangani masalah ekonomi atau menangani terorisme. Belum lagi bagi negara yang mayoritas muslim, seringkali pemerintahnya harus berhadapan dengan masyarakatnya sendiri. Pada dasarnya tidak semua muslim di Indonesia memiliki paham radikal dan mengarah pada gerakan terorisme, namun berdasarkan dari keberagaman agama di Indonesia, aksi teroris kerap kali dilakukan oleh pihak yang mengklaim bahwa dirinya sebagai muslim dan hal tersebut merupakan resiko bagi agama mayoritas.[21] Dilema semacam inilah yang kadangkala memicu ketegangan-ketegangan dalam negeri yang dapat memicu disintegrasi bangsa. Dengan kondisi tersebut, dapat dipahami bahwa terorisme telah menjadi ancaman nyata bagi Indonesia.[22]

Indonesia merupakan negara yang rentan akan ancaman terorisme, hal ini dapat terlihat dari banyaknya aksi terror di Indonesia, seperti pada kasus-kasus besar: Bom Bali I pada Oktober 2002, Bom Bali II pada Oktober 2005, Hotel JW Marriot dan Hotel Ritz Calton pada Juli 2009, Kedutaan Besar Australia pada September 2004.[23] Plaza Sarinah pada Januari 2016, hingga Terminal Kampung Melayu pada Mei 2017. Selain itu, terdapat juga perlibatan warga negara Indonesia (WNI) dalam jaringan terorisme internasional seperti ISIS, Al-Qaeda, Jamaah Islamiyah, Abu Sayyaf dan sebagainya.[24] Sedangkan untuk ancaman teror yang terjadi di *cyberspace*, mengacu pada data statistik Kementerian Komunikasi dan Informatika, Indonesia menduduki posisi teratas akan kerentanan dalam serangan *cyber.* Hal tersebut menjadikan Indonesia kerap kali menjadi target penyerangan di *cyberspace* apabila dibandingkan dengan negara-negara lainya. Seperti yang tergambarkan pada grafik (lihat grafik 1).

Salah satu kasus terorisme dengan pemanfaatan *cyberspace* di Indonesia yang mendapat sorotan adalah kasus Imam Samudra, seorang terpidana mati atas kasus Bom Bali I. Saat itu, Imam Samudra dapat melakukan kontrol terhadap jaringan teroris dari dalam sel penjaranya dengan menggunakan

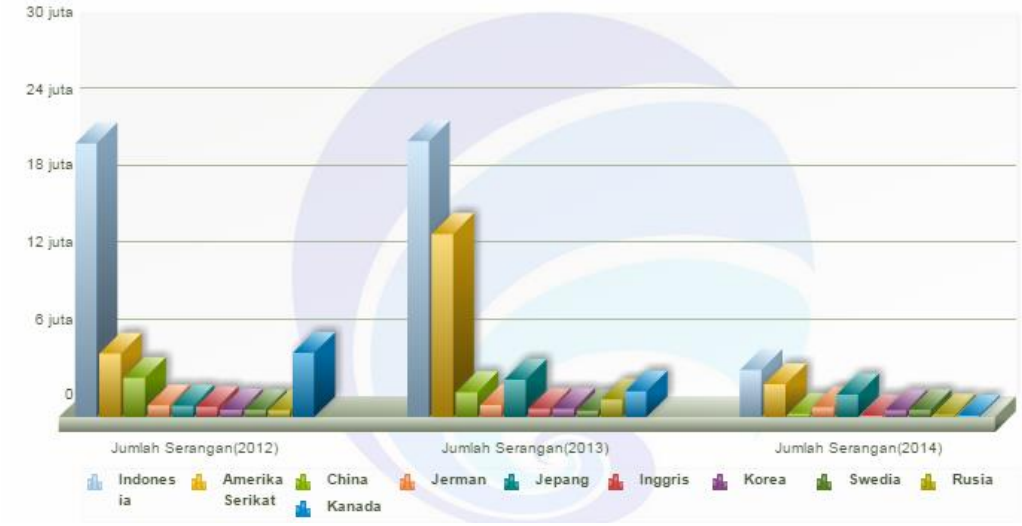
[21] "Terorisme Dikaitkan Islam, BNPT: Itu Resiko Agama Mayoritas", Republika, 15 April 2016, dalam http://nasional.republika.co.id/berita/nasional/umum/16/04/15/o5neyu377-terorisme-dikaitkan-islam-bnpt-itu-resiko-agama-mayoritas, diakses pada 17 Juli 2017.

[22] "Terorisme masih jadi ancaman nyata tahun 2016", Rappler, 29 Desember 2015, dalamhttp://www.rappler.com/indonesia/117434-terorisme-masih-jadi-ancaman-nyata-tahun-2016, diakses pada 13 Agustus 2016.

[23] Jeneman Iskandar, "Perubahan Pola Serangan Teorisme di Indonesia: Studi Kasus Tahun 2000-2013", (Jakarta: Dapur Buku, 2014).

[24] Golose, *op.cit.*

Grafik 1. Negara Target *Cyberattack* dan *Cyberterror* Tahun 2012-2014



Sumber: Kementerian Komunikasi dan Informatika, 2017, Data dan Statistik; Cyber Security and Governance (Ditjen PPI), dalamhttps://statistik.kominfo.go.id/site/searchKonten?iddoc=1370, diakses pada 2 Juni 2017.

internet.[25] Selain itu, ancaman paling sering dalam *cyberspace* di Indonesia adalah penggunaan situs internet dalam melakukan propaganda dan *brain washing* guna menyebarkan ideologi radikal atau yang biasa disebut dengan *cyber radicalization*.[26]

Pemerintah Indonesia sendiri dalam menilai beberapa kasus penggunaan internet sebagai media *cyber radicalization* masih bersifat subjektif, apakah tindakan tersebut mengarah ke tindakan teror atau tidak. Adapun kasus yang secara jelas menyatakan *cyber radicalization* dan dilanjutkan dengan aksi teror di Indonesia adalah situs *Al-Kitabatul Maut Al Alamiya* atau *the international death brigade* yang mengklaim bertanggungjawab pada kasus Bom Bali I pada tahun 2002.[27] Selain itu, terdapat kasus Santoso yang disebut memimpin jaringan Kelompok Mujahidin Indonesia Timur yang menyampaikan dukungannya terhadap pimpinan ISIS Abu Bakar Al Bahgdadi melalui video di YouTube. Aksinya berujung dengan diikuti sejumlah orang Indonesia yang mengaku berada di wilayah kekuasaan ISIS, Irak serta Suriah, dan mengajak masyarakat untuk ikut 'berjihad' bersama ISIS di negara tersebut.[28]

Sebagai tindakan pencegahan atas terulangnya aksi-aksi teror dan radikalisasi tersebut dan membatasi pergerakan jaringan teroris di *cyberspace* Indonesia, maka pemerintah Indonesia dengan

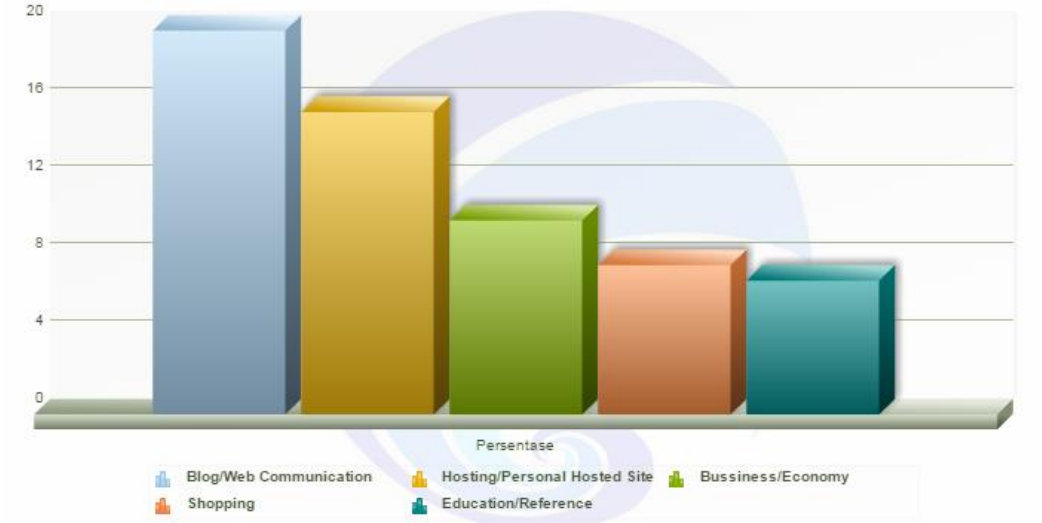
[25] Imam Samudra berhasil menyelundupkan laptop ke dalam sel dengan bantuan seorang Sipir Lembaga Pemasyarakatan (Lapas) Kerobokan, yang sebelumnya telah direkrut menjadi anggota teroris di dalam Lapas. Berdasarkan Laporan International Growth Centre dalam Petrus Reinhard Golose, *Invasi Terorisme ke Cyberspace*, (Jakarta: YPKIK/Yayasan Pengembangan Kajian Ilmu Kepolisian, 2015), hlm. 18-19.

[26] Von Bher, *op.cit.*

[27] "We Bombed Bali", dalam http://www.theage.com.au/articles/2002/12/12/1039656175179.html,13 Desember 2002, diakses pada 6 Juni 2017.

[28] "ISIS Sebar Pemahaman Radikal melalui Media Digital", dalamhttp://www.bbc.com/indonesia/berita_indonesia/2015/03/150301_radikalisme_anakmuda_sosmed,2 Maret 2015, diakses pada 6 Juni 2017.

Grafik 2. Kategori Website Berbahaya di Indonesia



Sumber: Kementerian Komunikasi dan Informatika, 2017, Data dan Statistik; Cyber Security and Governance (Ditjen PPI), dalam https://statistik.kominfo.go.id/site/searchKonten?iddoc=1370, diakses pada 2 Juni 2017.

legitimasi yang diberikan pada Badan Nasional Pengawasan Terorisme (BNPT) telah melakukan pemblokiran terhadap situs-situs yang dianggap menyebarkan pemahaman radikal dan ekstrem. Berikut daftar sebelas situs yang populer dan mendapatkan pemblokiran:[29]

1. voa-islam.com
2. nahimunkar.com
3. kiblat.net
4. bisyarah.com
5. dakwahtangerang.com
6. islampos.com
7. suaranews.com
8. izzamedia.com
9. gensyiah.com
10. muqawamah.com
11. abuzubair.net.

[29] "11 Situs terbaru yang diblokir pemerintah",dalamhttp://megapolitan.kompas.com/read/2017/01/04/10150067/ini.dia.11.situs.yang.terbaru.diblokir.pemerintah,1 April 2017, diakses pada6 Juni 2017.

Selain itu, BNPT juga telah melakukan beberapa pemblokiran pada situs-situs pribadi seperti *blogspot* dan *wordpress* yang berisi konten-konten radikal. Tantangan yang dihadapi adalah banyaknya pengguna situs pribadi di Indonesia (lihat Grafik 2), sehingga upaya pemblokiran membutuhkan waktu yang cukup berlarut, mengingat ketika situs tersebut diblokir atau dihapus oleh pemerintah, akan bermunculan situs-situs baru karena situs tersebut tidak berbayar dan prosedur pembuatan akun baru atau akun ganda sangat mudah (lihat grafik 2).

Potensi Pengguna Internet Indonesia dalam *Counter-Cyber Radicalization*

Penanganan *cyber radicalization* tidak bisa serupa dengan penanganan radikalisasi konvensional (yang terjadi melalui dunia nyata), diperlukan pendekatan khusus di ranah *cyberspace.* Pemerintah dapat dengan mudah melakukan

pemblokiran atau penghapusan situs, *blog* pribadi, dan akun-akun media sosial yang dinilai mememiliki konten radikal. Permasalahannya, situs dan media sosial tersebut akan terus ada dan beregenerasi dengan akun-akun barunya. Selain itu, pemblokiran dan penghapusan secara brutal akan menimbulkan nilai negatif bagi negara demokrasi yang mendukung kebebasan berekspresi.

Dalam konteks ini, model penanganan yang difokuskan adalah *counter-cyber radicalization* yang berangkat dari konsep keamanan *cyber* dan *counter-radicalization. Counter radicalization* pada dasarnya merupakan upaya selain de-radikalisasi dalam mencegah tendensi ekstremis yang tumbuh di masyarakat. Apabila diimplementasikan secara bijak, *counter-radicalization* akan lebih efektif kertimbang de-radikalisasi karena *Counter-radicalization* merupakan perlawanan pada proses penyebaran paham-paham radikal dan berfokus pada embrio radikalisasi, sedangkan de-radikalisasi berfokus pada upaya merubah pemahaman (yang sudah) radikal kembali normal.[30]

Pemanfaatan instrumen *cyberspace,* khususnya dalam konteks sosial media untuk melakukan *counter-radicalization* dapat dikategorikan sebagai *counter-cyber radicalization. Counter-cyber radicalization* perlu dilakukan karena saat ini peneror lebih banyak berada di dunia maya dalam penyebaran pesan, propaganda permusuhan dan promosi tindakan kekerasan. Beberapa temuan pemanfaatan dunia maya oleh kelompok teroris di Indonesia bahwa dunia maya digunakan untuk merilis manifesto, propaganda, dan statemen agitatif, menggalang dukungan, dan penguatan jaringan, mengkomunikasikan antar-jaringan dan merekrut anggota baru.[31]

Menurut catatan penulis, terdapat beberapa potensi pengguna internet Indonesia dalam menangkal atau menajadi bagian dari agenda *counter-radicalization* yang tidak hanya berada ditataran normatif, namun berfokus pada embrio radikalisasi di *cyberspace* tersebut. *Pertama,* banyaknya jumlah pengguna internet di Indonesia dan cenderung sangat aktif di media sosial menjadikan Indonesia mudah mengangkat sesuatu isu menjadi viral hanya dengan bermodalkan tanda pagar *(hashtag).*[32] *Cyber-radicalization* yang dilakukan melalui sosial media akan tidak efektf apabila mayoritas pengguna sosial media tersebut ikut menyebarkan konten-konten yang bertentangan dengan ideologi radikal. Maka tugas pemerintah adalah mengeluarkan konten-

[30] Farhan Zahid, "Analyzing the Counter-Radicalization and De-Radicalization Models" dalam http://www.cf2r.org/fr/foreign-analyzes/analyzing-the-counter-radicalization-and-de-radicalization-models.php, 13 Desember 2016, diakses 19 Juli 2017.

[31] Petrus Reinhard Golose, *op.cit.*

[32] Hashtag adalah kata atau frase tanpa spasi yang diawali dengan simbol hash ("#"). Hashtag difungsikan untuk menggolongkan tema atau topik yang lebih spesifik dalam media sosial, dan di sisi lain hashtag juga mempermudah orang lain untuk mencari topik yang saling berhubungan. Lihat, "Definisi Hashtag pada Sosial Media", dalam http://organixdigital.com/blog/read/definisidan-fungsihashtagpadasosialmedia, 11 April 2014, diakses pada 3 Juni 2017.

Grafik 3. Aktivitas menggunakan internet oleh Individu di Indonesia

Sumber: Kementerian Komunikasi dan Informatika, 2017, Data dan Statistik; *Cyber Security and Governance (Ditjen PPI)*, tersedia di *https://statistik.kominfo.go.id/site/searchKonten?iddoc=1370*, diakses pada 2 Juni 2017.

konten (yang bersifat propaganda) dan mengkampanyekan untuk melawan radikalisasi di internet, yang paling efektif adalah menggunakan *hashtag*. Pengguna internet yang menangkap pesan tersebut kemungkinan akan menyebarkan konten tersebut dan menjadikannya *trend*. Menurut penulis, dari sekian banyak konteks di *cyberspace*, sosial media merupakan hal yang paling perlu untuk diperhatikan karena sebuah isu cenderung popular dan menyebar dengan cepat melalui sosial media. Terlebih, penggunaan internet di Indonesia didominasi untuk tujuan sosial media, seperti yang tergambarkan dalam grafik (lihat grafik 3).

Kedua, Masyarakat Indonesia mampu meproduksi produk lelucon dengan sangat cepat dan membuatnya populer dengan hitungan menit di *cybersapce*. Selera humor masyarakat Indonesia tersebut telah diakui masyarakat dunia. Hal ini terlihat dari kasus Bom di area Sarinah Thamrin pada 14 Januari 2016, setelah kejadian tersebut dalam hitungan menit trenddi sosial media dunia langsung berubah menjadi isu pengeboman tersebut. Menariknya, tidak seperti kasus terorisme di Paris, Perancis[33], mayoritas respons masyarakat Indonesia (khususnya Jakarta) di sosial media tidak menunjukkan rasa takut akan teror yang tercipta; justru menjadikan aksi terorisme tersebut menjadi bahan lelucon dan satir terhadap ideologi-ideologi radikal. Hal tersebut ditunjukkan dengan banyaknya produksi meme (gambar dengan tulisan) dan status sosial media yang bersifat satir. Pada saat itu, respons pengguna internet di Indonesia tersebut menjadi simbol bahwa terorisme tidak membuat masyarakat Indonesia takut yang ditandai dengan *hastag* "#KamiTidakTakut" yang

[33] "Paris Massacre: At least 128 die in attacks", dalam http://edition.cnn.com/2015/11/13/world/parisshooting/index.html, 14 November 2015, diakses pada 4 Juni 2017.

menyebar diseluruh dunia. Hal tersebut menunjukkan aksi terorisme yang bertujuan untuk menyebarkan teror dan rasa takut telah gagal dilakukan atau dapat ditangkal oleh respon pengguna internet Indonesia.[34]

Selain itu, dalam kasus peledekan di Terminal Kampung Melayu pada bulan Mei 2017, *hastag* "#KamiTidakTakut" kembali menjadi *trend* dunia. Ini merupakan responserentak pengguna internet Indonesia tanpa koordinasi pihak manapun. Oleh karena itu, apabila pemerintah mampu memanfaatkan potensi-potensi tersebut dengan menjadikannya bagian dari agenda *counter-cyber radicalization*, maka hal ini akan menjadi cara paling efisien dan efektif. Karena bagaimanapun juga suasana teror dan opini publik yang tercipta hanya dapat dikontrol oleh publik itu sendiri.[35] Secara teknisnya, pemerintah dapat memanfaatkan tokoh-tokoh publik yang terkenal dan aktif di *cyberspace* sebagai agen dalam mengendalikan opini publik. Status di Facebook, kicauan di Twitter dan Video di Youtube oleh tokoh-tokoh tersebut cenderung lebih cepat diterima dan menyebar di *cyberspace.*

Perlibatan pengguna internet Indonesia dalam agenda *counter-cyber radicalization* akan berdampak pada dua fase: *pertama*, saat *cyber radicalization* berlangsung dimana pengguna internet yang menjadi bagian dari agenda akan menangkal ideologi dan pemahaman radikal dengan merubahnya menjadi bahan lelucon yang pada akhirnya membuat ideologi dan pemahaman tersebut tidak populer. *Kedua,* pada saat terjadi aksi teror seperti peledakan dan bom bunuh diri. Aksi teror tersebut akan menimbulkan dampak takut dan panik yang merupakan tujuan utama teroris, yang dianggap juga sebagai keberhasilan teroris dalam menyampaikan pesan kepada calon "teroris" selanjutnya. Namun dengan banyaknya akun media sosial yang menentang dan menggambarkan tindakan tersebut sebagai tindakan konyol, maka hal tersebut akan menunjukkan bahwa upaya teroris dalam menyampaikan pesan melalui aksi teror telah gagal dilaksanakan.

Tantangan *Counter-Cyber Radicalization* di Indonesia

Indonesia dengan potensi pengguna internetnya dalam melakukan *counter-cyber radicalization* memilikitiga tantangan yang periu diperhatikan: *pertama*, kurangnya kewaspadaaan masyarakat terhadap hal-hal yang berbau "terorisme". Apabila masyarakat mampu merubah budaya populer bahwa paham radikal dan tindakan teror merupakan lelucon sehingga peminat paham tersebut atau korban dari radikalisasi akan menurun, maka konsekuensinya akan mengurangi kewaspadaan yang selama ini terbangun karena rasa "takut" terhadap aksi terorisme. Bagaimanapun

[34] Rizky Reza Lubis, "Fight Radicalization with 'Ridicoulization'", Essay for FPCI International Internship Program 2016 on Germany, Theme: The Role of Young Generation in Counter Terrorism, FPCI.
[35] *Ibid.*

juga kurangnya peminat paham radikal di *cyberspace* bukan berarti menghentikan aksi dari jaringan terorisme. Hal ini menjadikan upaya *counter-radicalization* melalui pemanfaatan pengguna internet di *cyberspace* efektif namun akan menciptakan *blind spot* baru. Pemerintah harus mampu menutup *blindspot*tersebutdengan tetap memberikan himbauan secara terus-menerus tanpa menimbulkan kepanikan dan rasa takut.

Kedua, mendiskreditkan kelompok tertentu. Menggiring opini publik untuk menganggap suatu ideologi atau pemahaman adalah radikal dan ekstrem memiliki konsekuensi akan mendiskreditkan dan menciptakan *stereotype* di masyarakat dengan kelompok (dalam konteks ini ajaran agama) yang dijadikan logika dasar dalam aksi terortersebut. Seperti halnya di Indonesia, mayoritas teroris megklaim dirinya sebagai muslim, meskipun tidak sesuai dengan ajaran agama Islam yang asli, namun ini akan menggiring opini publik bahwa agama dasar atau murni yang diklaim teroris tersebut merupakan bagian dari lelucon. Hal ini berpotensi menjadi salah satu faktor disintegrasi bangsa.

Kesimpulan

Cyber radicalization merupakan ancaman nyata bagi suatu negara dan Indonesia merupakan salah satu negara yang paling potensial menjadi target teroris dan radikalisasi (termasuk di *cyberspace*-nya). Upaya dalam menangani radikalisasi di *cyberspace* tidak akan sama efektifnya dengan penanganan di dunia nyata. Terlebih, Indonesia merupakan negara demokrasi yang menjaga kebebesan berekspresi masyarakatnya, sehingga tidak bisa secara semena-mena melakukan pemblokiran terhadap situs dan akun-akun media sosial.

Diperlukan cara-cara kreatif dan efektif dalam *counter-cyber radicalization*, salah satunya adalah dengan memanfaatkan potensi masyarakat Indonesia yang menggunakan internet. Pengguna internet Indonesia yang banyak dan dengan keaktifannya mampu dengan mudah mengangkat suatu isu menjadi viral, dapat digunakan sebagai agenda *counter-cyber radicalization* dalam mengendalikan opini publik bahwa pemahaman radikal merupakan hal yang negatif. Selain itu, saat terjadi aksi teror pengguna internet dengan sendirinya akan melawan kepanikan dan rasa takut yang ditimbulkan dengan sosial medianya. Hal tersebut akan mereduksi peminat ideologi radikal. Namun pada pelaksanaannya, pemerintah harus memperhatikan tingkat "*awareness*" masyarakat dan posisi penganut agama tertentu agar tidak terdiskreditkan, mengingat akan banyaknya kampanye di *cyberspace* yang menentang paham-paham radikal.

Daftar Pustaka

Buku

Denning, Dorothy E. 2009. *Terror's Web: How the Internet Is Transforming Terrorism, Handbook on Internet Crime.* New York: Willan Publishing.

Golose, Petrus R. 2008. *Seputar Kejahatan Hacking: Teori dan Studi Kasus*. Jakarta: Yayasan Pengembangan Kajian Kepolisian Indonesia.

Golose, Petrus R. 2015. *Invasi Terorisme ke Cyberspace*. Jakarta : Yayasan Pengembangan Kajian Ilmu Kepolisian.

Hoffman,Bruce. 2013. *Challenges for the U.S. Special Operations Command posted by the Global Terrorist Threat: Al-Qaeda on the Run or On the March?*. George Washington D.C.: Middle East Policy.

Iskandar, Jeneman. 2014. *Perubahan Pola Serangan Teorisme di Indonesia: Studi Kasus Tahun 2000-2013*. Jakarta: Dapur Buku.

Lewis, James A.2002. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, DC: Center for Strategic & International Studies.

Stein, Ruth. 2010. *For Love of the Father: A Psychoanalytic Study of Religious Terrorism*. Stanford: Stanford University Press.

Von Bher et. al. 2013. *Radicalization in the Digital Era*. Santa Monica: RAND Corporation.

Zelin, Aaron Y dan Richard Borow Fellow. 2013. *The State of Global Jihad Online: A Qualitative, Quantitative, and Cross-Lingual Analysis.* Washington : Washington Institute for Near East Policy.

Jurnal

Jackson, Richard. 2007. *Constructing Enemies: 'Islamic terrorism'in political and academic discourse.* Government and Opposition. Vol. 42. No. 3.

Wilner, Alex S.dan Claire-Jehanne Dubouloz. 2010."Homegrown terrorism and transformative learning: an interdisciplinary approach to understanding radicalization". *Global Change, Peace & Security.* Vol. 22 No. 1.

Wilson, Clay. 2003. *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. Focus on Terrorism*. Vol. 9.

Website

"Definisi Hashtag pada Sosial Media", dalam http://organixdigital.com/blog/read/definisidanfungsihashtagpadasosial-media, 11 April 2014, diakses pada 3 Juni 2017.

"ISIS Sebar Pemahaman Radikal melalui Media Digital", dalamhttp://www.bbc.com/indonesia/berita_indonesia/2015/03/150301_radikalisme_anakmuda_sosmed2 Maret 2015, diakses pada 6 Juni 2017.

Kilcullen, David J, "Three Pillars of Counterinsurgency", Pidato pada *the U.S Government Counterinsurgency Conference*, Washington D.C, 28 September 2006, dalam https://www.researchgate.net/publication/237538249_Three_Pillars_of_Counterinsurgency.

"Paris Massacre: At least 128 die in attacks", dalam http://edition.cnn.com/2015/11/13/world/parisshooting/index.html, 14 November 2015, diakses pada 4 Juni 2017.

"Radicalization", Oxford Dictionary, dalam https://en.oxforddictionaries.com/definition/radicalization, diakses pada 19 Juli 2017.

"*Self-Radicalization*", dalam http://en.citizendium.org/wiki/Self-radicalization,23 September 2013, diakses pada 2 Juni 2017.

"Situs terbaru yang diblokir pemerintah",dalamhttp://megapolitan.kompas.com/read/2017/01/04/10150067/ini.dia.11.situs.yang.terbaru.diblokir.pemerintah,

1 April 2017, diakses pada 6 Juni 2017.

"Terorisme masih jadi ancaman nyata tahun 2016", dalamhttp://www.rappler.com/indonesia/117434-terorisme-masih-jadi-ancaman-nyata-tahun-2016 29 Desember 2015, diakses pada 13 Agustus 2016.

"We Bombed Bali", dalamhttp://www.theage.com.au/articles/2002/12/12/1039656175179.html,13 Desember 2002, diakses pada 6 Juni 2017.

Zahid, Farhan, "Analyzing the Counter-Radicalization and De-Radicalization Models" dalam http://www.cf2r.org/fr/foreign-analyzes/analyzing-the-counter-radicalization-and-de-radicalization-models.php, 13 Desember 2016, diakses pada 19 Juli 2017.

Lain-lain

Abas, Anton A. 13 Oktober 2015, Paparan Mata Kuliah Media dan Terorisme, Program Studi Peperangan Asimetris, Universitas Pertahanan Indonesia.

Lubis,Rizky Reza. 2016."Fight Radicalization with "Ridiculization".*Essay for FPCI International Internship Program 2016 on Germany. Theme: The Role of Young Generation in Counter Terrorism,* FPCI.