DAMPAK SERANGAN VIRTUAL ISIS *CYBER-CALIPHATE* TERHADAP AMERIKA SERIKAT

Bayu Widiyanto
Program Studi Ilmu Hubungan Internasional
Universitas Paramadina
Jl. Jend. Gatot Subroto Kav. 97, Jakarta Selatan
widiyantosawyer@gmail.com

Abstrak

Saat ini, ada perdebatan tentang apakah *cyberterrorism* menimbulkan ancaman serius bagi masyarakat meskipun banyak yang telah didramatisasi di media populer. Karena istilah *cyberterrorism* telah digunakan secara tidak layak dan telah digunakan secara berlebihan, pemahaman yang jelas tentang bahaya *cyberterrorism* harus dimulai dengan definisi yang jelas. Saat ini, jaringan komputer diserang setiap hari karena ketidakmampuan keamanan dalam mengimbangi pertumbuhan konektivitas dan karena telah tersedianya peralatan dan teknik *hacking*. Karena infrastruktur yang terpenting adalah jaringan, hal itu berisiko. Meskipun dalam banyak invasi harian, para *hacker* mencoba untuk mengetahui apakah mereka bisa, dengan tindakan vandalisme atau *denial-of-service attacks*, individu bisa mendapatkan akses terhadap informasi sensitif. Bahaya nyata dari *cyberterrorism*, bagaimanapun juga, terletak pada penggunaan komputer baik sebagai taktik teroris maupun sebagai pengganda kekuatan.

Kata kunci: ISIS, *Cyber-Caliphate*, serangan virtual, *cyberterrorism*, teknologi informasi, Amerika Serikat

Abstract

Currently, there is a considerable debate about whether cyberterrorism poses a serious threat to society, although much has been dramatized in the popular media. Because the term cyberterrorism has been improperly used and overused, a clear understanding of the danger of cyberterrorism must begin with a clear definition. Currently, computer networks are attacked daily because of the security's inability to keep pace with the growth of connectivity and because of readily available hacking tools and techniques. Because the most critical infrastructure is the network, it is at risk. Although many of the daily invasions are hackers trying to get in just to see if they can, by acts of vandalism or denial-of-service attacks, individuals are gaining access to sensitive information. The real danger of cyberterrorism, however, lies in the computer's use as both a terrorist tactic and a force multiplier.

Keywords: ISIS, Cyber-Caliphate, virtual attacks, cyberterrorism, information technology, United States

Pendahuluan

Pada abad ke-21 ini, perkembangan ilmu pengetahuan dan teknologi (IPTEK) berlangsung sangat cepat dan semakin tidak rasional. Prosesnya sangat radikal dan hampir menyentuh setiap lapisan manusia di lintas negara sehingga semua orang dapat memiliki kemudahan akses, bahkan di lokasi yang sangat jauh dari tempat tinggal berada. Namun, teknologi ini juga datang dengan efek samping yang cukup signifikan. Kalau kita melihat kemajuan IPTEK, tepatnya dalam bidang *information technology* (teknologi informasi/IT), kemajuannya dapat membuat orang-orang menjadi lebih dekat. Akan tetapi, mereka hanya didekatkan secara virtual dalam sebuah ruang yang semu, dan ruang tersebut sangat rentan terhadap serangan asing. Sejak IPTEK dalam bidang IT maju, sistem keamanan sebuah negara pun semakin maju. Demikian pula metode peperangan. Saat ini telah muncul metode perang baru yang disebut sebagai teknik *asymmetrical war* (perang asimetris). Dalam metode perang ini, bentuk pertempurannya tidak lagi hanya dilakukan secara fisik, tetapi juga secara virtual.

Kasus yang ingin penulis ambil dalam hal ini adalah kemunculan C*yber-Caliphate*, sub-divisi yang dikembangkan oleh ISIS yang mendorong upaya mereka memerangi Barat. Menurut Dewan Riset Nasional dalam *Suatu Pemikiran tentang Perang Asimetris* (2008), perang asimetris adalah suatu model peperangan yang dikembangkan dari cara berpikir yang tidak lazim dan di luar aturan peperangan yang berlaku, dengan spektrum perang yang sangat luas dan mencakup aspek-aspek *astagatra* (perpaduan antara *trigatra*: geografi, demografi, dan sumber daya alam (SDA); dan *pancagatra*: ideologi, politik, ekonomi, sosial, dan budaya).

Perang asimetris selalu melibatkan peperangan antara dua aktor atau lebih, dengan ciri menonjol dari kekuatan yang tidak seimbang. Di sini, ISIS berusaha menyamakan kapasitas bertempur mereka dengan negara-negara Barat, seperti Amerika Serikat (AS), dan negara-negara lain yang berusaha menggempur ISIS. Namun, karena kapasitasnya tidak sebanding, mereka menggunakan teknik perang asimetris, yakni dengan membentuk *Cyber-Caliphate* dan menggunakannya untuk menyerang infrastruktur-infrastruktur virtual, seperti *website The United States Central Command* (CENTCOM), *website* Mountain View Telegraph, dan infrastruktur-infrastruktur virtual AS yang cukup vital.

Tema ini berusaha menunjukkan betapa bahayanya teknologi ketika digunakan untuk kepentingan yang tidak baik. Penulis juga ingin meneliti lebih jauh lagi mengapa ISIS sampai harus meretas beberapa *website* penting AS, serta mempelajari perkembangannya dari awal terbentuk sampai sekarang..

Human Security

> *Human security is the combination of threats associated with war, genocide, and the displacement of populations. At a minimum, human security means freedom from violence and from the fear of violence* (Human Security Report Project, tanpa tahun).

Konsep *human security* diangkat karena kasus yang penulis bahas sangat terkait dari segi bahwa *fear* (rasa takut) di masyarakat merupakan isu global baru yang muncul, terutama jika dikaitkan dengan kasus ekstremisme. Kelompok-kelompok ekstremis memanfaatkan rasa takut di kalangan masyarakat untuk menunjukan signifikansi mereka. Metode itu juga dijadikan sebagai alternatif bagi kelompok-kelompok tersebut dalam melakukan serangan, selain melakukan konfrontasi secara frontal dengan AS di Timur Tengah.

Social Network Theory

> *Social Network Theory is the study of how people, organizations or groups interact with others inside their network. Understanding the theory is easier when you examine the individual pieces starting with the largest element, which is networks, and working down to the smallest element, which is the actors* (Claywell, tanpa tahun).

Teori yang penulis gunakan dalam pembahasan ini adalah *social network theory* di mana teori ini mengungkapkan karakteristik subyek tertentu (individu atau kelompok/ organisasi) dan menjelaskan bagaimana subyek itu menjalankan pola kerja mereka. Dalam kaitannya dengan kasus yang diangkat, penulis ingin mengkaitkan teori ini terhadap pola kerja kelompok *hacker Cyber-Caliphate* dan kegiatan mereka terhadap kehidupan individu pengelola/pengguna struktur dunia maya tersebut.

Cyberterrorism

Cyberterrorism tidak memiliki definisi yang jelas. Organisasi/instansi hukum seperti *Federal Bureau Investigation* (FBI) di AS dan *Centre for the Protection of National Infrastructure* (CPNI) di Inggris dan politisi hanya dapat memberikan entitas *cyberterrorism*

ini sebatas definisi umum yang masih tidak terlalu jelas. Menurut Verton (2003), *cyberterrorist* merupakan sekumpulan orang yang melakukan serangan mendadak dengan menggunakan komputer dan internet untuk melumpuhkan infrastruktur negara. Namun, Denning berpendapat lain. Menurutnya, *cyberterrorism* merupakan aksi penyerangan menggunakan komputer sebagai alat bertempur. Di sisi lain, Bronskill (2001) dan Weimann (2004) berargumen bahwa *cyberterrorism* digunakan untuk merekrut, mencari dukungan, dan melancarkan propaganda melalui *website* (Awan, 2014).

Cyberterrorism merupakan gabungan dari *cyberspace* dengan *terrorism* (terorisme). Hal ini merujuk pada serangan yang tidak terduga dan juga ancaman terhadap komputer, jaringan, dan informasi yang tersimpan dalam perangkat tersebut yang jika informasi itu berhasil dikuasai oleh kelompok ini, mereka dapat mengancam pemerintahan suatu negara bahkan rakyatnya. Serangan virtual tersebut yang dilakukan oleh kelompok tersebut untuk mendapatkan tujuan mereka secara politik maupun sosial (Weimann, 2004).

Cyberspace sendiri merupakan entitas yang berupa tempat virtual yang biasanya digunakan untuk menyimpan data dan sebuah tempat di mana semua orang dapat mengakses. Karena adanya terorisme yang juga menjadi virtual, *cyberspace* dimanipulasi oleh terorisme menjadi senjata yang kemudian digunakan untuk menyerang infrastruktur di dunia nyata. Menurut beberapa penulis yang saya kutip, *cyberspace* adalah perangkat yang dependen pada waktu, terdiri dari interkoneksi sistem informasi dan pengguna manusia yang berinteraksi dengan sistem ini (Ottis dan Lorents, 2010).

Dengan demikian, dapat ditarik garis tengah bahwa *cyberterrorism* merupakan kegiatan yang melibatkan tindak aktif maupun pasif. Aktif berarti menggunakan komputer untuk melakukan infiltrasi terhadap infrastruktur penting dalam negara, seperti listrik, layanan darurat, telekomunikasi, suplai air, ekonomi, militer, dan institusi finansial sebuah negara yang bisa berakibat fatal. Sisi pasif menunjukkan bahwa *cyberterrorism* juga dapat melakukan rekrutmen, mencari dukungan, dan melancarkan propaganda yang bertujuan untuk menyebarkan rasa takut terhadap masyarakat global di dunia maya.

Sejarah *Cyberterrorism*

Akar *cyberterrorism* berawal dari tahun 1990, ketika penggunaan internet mulai dikenal secara luas dan muncul perdebatan tentang munculnya "*information society*" yang berakhir pada munculnya beberapa pengkaji tentang potensi resiko yang akan dihadapi negara yang berjaringan tinggi dan sangat bergantung terhadap teknologi tinggi seperti AS. Karena ini semua, AS sangat bergantung terhadap komputer. Tujuan utama dari kegiatan ini adalah untuk melakukan disrupsi atau gangguan, namun tidak sampai memberikan dampak yang fatal dan biasanya dilakukan untuk kepentingan politik (Weimann, 2005).

Teroris menggunakan *cyberspace* untuk menciptakan sebuah ketidakpastian. Mereka sendiri melakukan hal-hal ini karena alasan tersendiri seperti melawan otoritas negara dan pemerintahan dan menggunakan cara apapun untuk mencapai tujuan mereka. Kasus-kasus sebelum ISIS *Cyber-Caliphate* yang pernah muncul dan merupakan isu *cyberterrorism* adalah sebagai berikut:

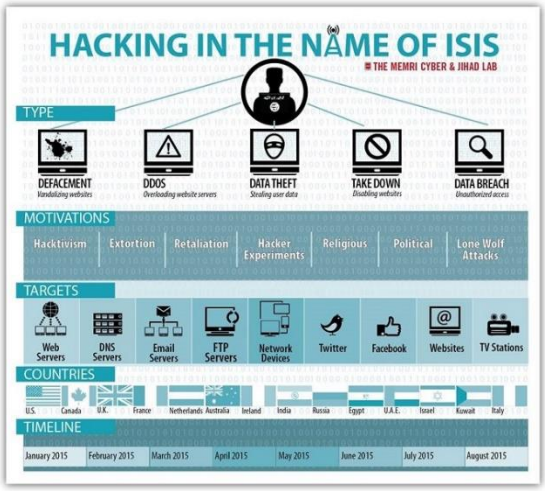
1. Pada tahun 1997, Kedutaan Besar Sri Lanka dibanjiri oleh hampir 800 email yang semua berisi tentang ancaman terhadap kedutaan besar tersebut. Kelompok yang mengancam kedutaan besar tersebut menyebut diri mereka sebagai *Black Tigers*. Alasan mereka melakukan kejahatan ini adalah untuk mengganggu komunikasi kedutaan tersebut dengan cara menyerang sistem pemerintahan.
2. Pada bulan Juli 1997, sekelompok *hacker* China mematikan satelit China dan mengumumkan bahwa mereka membangun organisasi global untuk memprotes dan mencegah datangnya investasi asing dari Barat di China.
3. Sabotase internet yang terjadi tahun 1998 di *Bhabha Atomic Research Centre*, India. Pelakunya melakukan hal ini karena memprotes program riset nuklir India.
4. Pada bulan April dan Oktober 2007, infrastruktur informasi di Estonia diserang dengan menggunakan komputer yang ber-*server* di Rusia. Kemudian pada Oktober 2007, *website* Presiden Ukraina diserang oleh gerakan muda Rusia, *The Eurasian Youth Movement*.
5. Adapun kasus yang dapat menyebar kepanikan secara global adalah *cyber attack* pada

akhir tahun 2008 ketika kelompok *hacker* yang bernama *Greek Security Team* dan *Intrude* berhasil menyerang sistem komputer *European Organization for Nuclear Research* (CERN) sangat dalam dan hampir memiliki kendali penuh terhadap salah satu pelacak di *Large Hadron Collider* (LHC), partikel nuklir paling besar di dunia. Kelompok tersebut meretas sistemnya ketika LHC pertama kali dijalankan. Mereka juga memasang halaman palsu di *website* resmi CERN dan berusaha mempromosikan diri mereka di *website* tersebut. Serangan kelompok ini memang tidak memunculkan kerusakan serius, namun karena kelompok ini berhasil mengendalikan salah satu pelacak di LHC dan alat-alat penting lainnya, mereka berhasil membuat kepanikan di hampir seluruh Eropa dan ketidaknyamanan banyak pihak.

Semua hal di atas menunjukan bahwa kegiatan *cyberterrorism* telah ada jauh sebelum ISIS muncul. Faktor pendorong suatu entitas melakukan itu didasari berbagai alasan, namun yang paling signifikan adalah ingin melawan sistem yang sekarang berjalan di dunia dan mencoba untuk menunjukan signifikansi entitas tersebut sehingga entitas tersebut dikenal oleh seluruh masyarakat dan sekaligus menyebarkan kepanikan di tengah masyarakat (Bogdanoski dan Petreski, 2014).

Ancaman *Cyber-Caliphate* terhadap Amerika Serikat

Dalam beberapa tahun terakhir, ancaman *cyber attack* sudah mulai memiliki signifikansi yang hampir dominan di antara kegiatan teroris ISIS dan kelompok ekstremis lain yang berafiliasi dengan ISIS. Hal ini menjadi semakin serius ketika ISIS memiliki tujuan baru. ISIS kemudian tidak hanya merekrut orang-orang yang ahli IT, tetapi juga sudah mempunyai kapasitas untuk mengakses *cyber weapons*. Terlebih lagi ketika *cyber weapons* semacam *virus* dan *software* perusak serta alat-alat lain yang digunakan oleh ISIS untuk melakukan serangan sudah sangat mudah diakses dan bahkan bisa dibeli secara *online*, seperti di eBay dan juga di pasar gelap yang menyediakan alat-alat serupa yang kemungkinan terburuknya digunakan untuk menyerang negara atau perusahaan (Platov, 2016).



Gambar 1
Kegiatan Ekstremis dalam *Internet Cyberspace*
Sumber: Steven Stalinsky dan R. Sosnow, "Hacking In The Name Of The Islamic State (ISIS)", *The Middle East Media Research Institute*, 21 Agustus 2015, http://www.memrijttm.org/hacking-in-the-name-of-the-islamic-state-isis.html (diakses pada tanggal 19 Juni 2016).

Kelompok ekstremis ISIS, yang sekarang dijuluki dengan nama *Cyber-Caliphate*, tersebut muncul pada 24 Desember 2014 melakukan *cyber attack* terhadap *Albuquerque Journal* dan ke *domain* yang bernama *US Official Network Communications*. Setelah insiden tersebut, *cyber attack* yang dilancarkan kelompok ini mulai semakin gencar, terutama dalam bentuk *defacement* atau perusukan sebuah *website*. Contoh jelasnya adalah ketika kelompok tersebut melakukan *defacement* terhadap *website* WBOC TV di Maryland. Serangan sejenis juga bermunculan dan menimbulkan banyak kerusakan, seperti gangguan penyiaran; pembobolan data-data penting; serangan virtual terhadap perusahaan koran dan layanan berita di AS, termasuk *Newsweek Magazine*; dan serangan virtual terhadap perusahaan *non-profit* seperti *US Military Spouse Organization*; *website* militer AS, termasuk *The United States Central Command* (CENTCOM); dan akun-akun sosial media (di antaranya facebook dan twitter).

Pada Maret 2015, *Cyber-Caliphate* juga mengumpulkan beberapa data yang mereka ambil dari berbagai sumber di internet dan mengelaborasikan data tersebut. Kemudian, mereka membuat *hit list* atau daftar target yang akan diserang secara eksplisit dan membuat 100 data tentang personel militer AS, termasuk foto, fisik, alamat email, dan nomor telepon genggam mereka masing-masing. Semua data ini diperoleh dengan *hacking* (meretas) beberapa *server* militer, *database*, dan email setiap personel militer AS di Angkatan Darat, Angkatan laut, dan Angkatan Udara. Mereka juga mengirim email kepada korbannya, berisikan bahwa ISIS akan menyerang individu warga negara AS tersebut jika diketahui bahwa mereka terlibat dalam perlawanan terhadap ISIS maupun perlawanan terhadap propaganda ISIS di dunia maya.

Berikut adalah potongan isi email yang dikirim oleh *Cyber-Caliphate* kepada targetnya yang terlibat:

> *O Kuffar in America, O You who worship the cross, O You crusaders that fight the Islamic State, we say to you: "DIE IN YOUR RAGE!", die in your rage because with the grace of Allah, The Islamic State Hacking Division (ISHD) has hacked several military servers, databases and emails and with all this access we have successfully obtained personal information related to military personnel in the U.S. Air Force, NAVY & Army... With the huge amount of data we have from various different servers and databases, we have decided to leak 100 addresses so that our brothers residing in America can deal with you* (Stalinsky dan Sosnow, 2015).

Hal ini semua memberi peringatan keras terhadap seluruh AS, dari personel militer sampai masyarakatnya. Oleh karena itu, Presiden Obama mengeluarkan *Executive Order* (Perintah Eksekutif) yang berisikan perintah dan kebijakan baru terkait dalam melawan ancaman *online*. Lebih tepatnya, langkah untuk melawan c*yber actor* yang melakukan serangan di luar garis yuridiksi AS sendiri (Lohrmann, 2015).

Perintah ini mengizinkan Departemen Keuangan AS berkonsultasi dengan *Attorney General* (Jaksa Agung) dan menteri negara untuk memberi sanksi kepada individu atau entitas yang melakukan *cybercrime* (kejahatan *cyber*) yang mengancam AS dari segi keamanan nasional, kebijakan luar negeri, keberlangsungan ekonomi, dan stabilitas finasial. Kebijakan ini berlaku jika melakukan hal yang dapat mempengaruhi:

1. Menyerang atau membobol sektor infrastruktur penting AS.
2. Melakukan disrupsi terhadap jaringan komputer, seperti *denial-of-service attacks*.
3. Mengganggu, merusak, atau menyalahgunakan dana/sumber ekonomi, perdagangan secara rahasia, pengenalan/pemetaan individu, atau informasi finansial untuk bersaing. Contoh di antaranya informasi *credit card* (kartu kredit), rahasia dagang, dan informasi sensitif lainnya.

Otoritas ini akan digunakan terhadap hampir semua ancaman *cyber*, terutama yang berusaha menyerang infrastruktur negara, perusahaan, dan masyarakat. AS juga akan melakukan cara apapun dalam menyelesaikan ancaman *cyber* ini, termasuk menggunakan kapasitas diplomatik dan mekanisme hukum dalam melawan

ancaman ini (The White House Office of the Press Secretary, 2015).

Dari semua data yang dikumpulkan mengenai isu antara *Cyber-Caliphate* dengan AS terkait kegiatan peretasan mereka di beberapa akun sosial media instansi penting AS, pemerintah AS karena hal ini merespon dengan mengeluarkan *Executive Order* dan meningkatkan kerja dengan negara-negara Teluk, terutama dalam bidang pertahanan terhadap ancaman *cyber*, dan berusaha mengadakan semacam retaliasi terhadap tindakan ekstremis tersebut dengan cara mengintensifkan pertahanan mereka di Timur Tengah yang sekarang sedang berkonflik.

Namun, hal ini berbalik kalau kita melihat dari perspektif kelompok ekstremis tersebut. *Cyber-Caliphate* merupakan tim terbaru dari divisi peretas ISIS. Memang kerusakan yang dibuat oleh kelompok ini cenderung minim dan bukan sesuatu yang serius, tidak sampai ke infrastuktur-infrastruktur penting negara, namun dengan melakukan hal seperti peretasan akun youtube dan twitter CENTCOM, hal ini menimbulkan opini negatif di antara masyarakat AS, yaitu rasa takut. Rasa takut inilah yang digunakan oleh ISIS untuk meningkatkan kapasitas propaganda mereka sekaligus untuk merekrut anggota baru untuk bergabung, dalam arti melakukan ekspansi keanggotaannya. Belum lagi *hit list* atau daftar target personel AS yang juga membuat militer AS cukup panik. Hal itu memberikan semacam efek *deterrence* terhadap AS, menunjukan signifikansi ISIS terutama di dunia maya, dan menunjukkan bahwa ISIS mempunyai kapasitas teknologi tinggi dalam melakukan serangan terhadap musuhnya. Namun, AS tidak begitu fokus terhadap isu ini karena masih ada ancaman *cyber* yang dianggap lebih mematikan dari *Cyber-Caliphate*, yakni *cyber attack* dari China dan Rusia yang bisa dibilang lebih membutuhkan perhatian dan lebih mengancam keamanan dan kepentingan AS.

Kesimpulan

Fenomena *cyberterrorism* merupakan fenomena masa kini. Terorisme merupakan isu yang sudah muncul beberapa tahun terakhir. Namun, globalisasi dan kemajuan IPTEK yang pesat mengubah pola berpikir manusia dan sikap mereka dalam melakukan sesuatu saat ini. Munculnya *Cyber-Caliphate* cukup mengguncang negara yang memiliki IPTEK yang paling maju seperti AS di mana teknologi sudah merupakan bagian dalam kehidupan masyarakatnya sehingga privasi seseorang mulai menjadi hal yang tabu

karena semuanya sudah masuk ke dalam sebuah entitas yang disebut sistem dan menjadi satu secara keseluruhan. Hal inilah yang kemudian menjadi sebuah celah di dunia IPTEK dan kemudian dijadikan sebuah alat untuk menyebarkan informasi yang bersifat menyimpang dan alat untuk melakukan rekrutmen.

Dari sinilah *Cyber-Caliphate* melakukan serangan terhadap AS, menyebarkan rasa takut dengan cara meretas beberapa akun youtube dan twitter CENTCOM dan membentuk sebuah *hit list* atau target penyerangan terhadap personel militer AS. Adanya fenomena ini tentu saja menujukkan bahwa teknologi yang seharusnya membuat kita aman berubah menjadi alat yang bisa mengancam dan menebar rasa takut di antara masyarakat.

Tindakan ISIS dalam menyebarkan ketakutan ini juga dapat direlasikan dengan konsep *human security* di mana ISIS melakukan tindakan menakuti banyak lapisan masyarakat, terlebih lagi ISIS juga melakukan rekrut kepada orang yang ingin bergabung ke ISIS sehingga jelas sekali hal ini bertentang langsung oleh konsep *human security* tersebut. Setelah itu, yang paling penting dari ini semua adalah ketika globalisasi membawa keniscayaannya dalam bentuk teknologi, di sisi lain juga membawa malapetaka karena hilangnya batasan privasi setiap individu maupun negara, dan privasi akan informasi tersebut digunakan sebagai senjata untuk memanipulasi orang maupun masyarakat dan membuktikan bahwa pada masa kini ketika berbicara mengenai perang dan strategi, hal ini sudah berkembang pesat dan canggih sehingga membunuh dan mengalahkan sudah tidak efektif lagi di abad ke-21 ini Karena ketika teroris menyerang, dalam konteks kasus yang penulis angkat ini, siapapun dapat menyerang langsung ke lapisan masyarakat yang jelas sudah berada di luar jangkauan pertahanan militer secara keseluruhan.

Daftar Pustaka

Jurnal

Awan, Imran. "Debating the Term Cyber-Terrorism: Issues and Problems". *Internet Journal of Criminology* (2014), hal. 1-14.

Bogdanoski, Mitko dan Drage Petreski. "Cyber Terrorism: Global Security Threat". *International Scientific Defence, Security and Peace Journal* (2014), hal. 59-72.

Saint-Claire, Steve. "Overview and Analysis on Cyber Terrorism". *School of Doctoral Studies*

(European Union) Journal (2011), hal. 85-98.

Weimann, Gabriel. "Cyberterrorism: The Sum of All Fears?". *Studies in Conflict & Terrorism*, Vol. 28, No. 2 (2005), hal. 129-149.

Dokumen Lain

Ottis, Rain dan Peeter Lorents. "Cyberspace: Definition and Implications". *International Conference on Information Warfare and Security*, Reading (April 2010), hal. 267.

Weimann, Gabriel. "Cyberterrorism: How Real is the Threat". *United States Institute of Peace: Special Report 119* (Desember 2004).

Internet

Claywell, Charlie R. "What is Social Network Theory". *LoveToKnow*, t.thn. http://socialnetworking.lovetoknow.com/What_is_Social_Network_Theory (diakses pada tanggal 17 Juni 2016).

Human Security Report Project. "Human Security Backgrounder". *Human Security Report Project*, t.thn. http://www.hsrgroup.org/press-room/human-security-backgrounder.aspx (diakses pada tanggal 17 Juni 2016).

Lohrmann, Dan. "Cyber Terrorism: How Dangerous is the ISIS Cyber Caliphate Threat?". *Government Technology*, 18 Mei 2015. http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html (diakses pada tanggal 19 Juni 2016).

Platov, Vladimir. "ISIS Cyber-Caliphate". *New Eastern Outlook*, 10 Februari 2016. http://journal-neo.org/2016/02/10/isis-cyber-caliphate/ (diakses pada tanggal 18 Juni 2016).

Stalinsky, Steven dan R. Sosnow. "Hacking In The Name Of The Islamic State (ISIS)". *The Middle East Media Research Institute*, 21 Agustus 2015. http://www.memrijttm.org/hacking-in-the-name-of-the-islamic-state-isis.html (diakses pada tanggal 19 Juni 2016).

The White House Office of the Press Secretary. "FACT SHEET: Executive Order Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities". *The White House*, 1 April 2015.

https://www.whitehouse.gov/the-press-office/2015/04/01/fact-sheet-executive-order-blocking-property-certain-persons-engaging-si (diakses pada tanggal 19 Juni 2016).