Aksi Cyber-Terrorism di Amerika Serikat dalam Perspektif Keamanan Global

Halida Azalea Iffa Dina

Fakultas Ilmu Sosial dan Ilmu Politik
UPN Veteran Jakarta

Email: halidaaid@upnvj.ac.id

Abstract

Acts of terrorism in the international world today have a close relationship with cyberspace. This is certainly a threat to state sovereignty, as happened in the United States in August 2020. The arrests of three terrorist groups involving the armed groups Al-Qassam, Al-Qaeda, and the Islamic State of Iraq and Syria due to campaign actions and fundraising to support the action. their terror. All of these actions relied on sophisticated cyber instruments and from their actions, these terrorist groups managed to collect millions of US dollars, using around 300 cryptocurrency accounts, 3 websites, and 4 Facebook accounts. The purpose of this study is to analyze the actions of cyber-terrorism in the United States from a global security perspective. The results of the study indicate that this act of terrorism enters into a security dilemma, which means that all efforts are made to achieve its security and will trigger feelings of insecurity for other countries.

Keywords: Cyber Crime, Terrorism, Security, USA

Tindak terorisme dalam dunia internasional saat ini memiliki keterkaitan yang erat dengan dunia maya. Hal ini tentu menjadi ancaman atas kedaulatan negara, sebagaimana yang terjadi di Amerika Serikat pada bulan Agustus 2020. Ditangkapnya tiga kelompok teroris melibatkan kelompok bersenjata Al-Qassam, Al-Qaeda, dan Islamic State Iraq and Suriah akibat tindakan kampanye serta penggalangan dana untuk mendukung aksi teror mereka. Seluruh aksi ini mengandalkan instrumen siber yang canggih dan dari aksinya, kelompok-kelompok teroris tersebut berhasil mengumpulkan jutaan dolar AS, menggunakan sekitar 300 akun mata uang kripto, 3 website, serta 4 akun Facebook. Tujuan dari penelitian ini yaitu untuk menganalisis aksi cyber-terrorism di Amerika Serikat dalam perspektif keamanan global. Hasil penelitian menunjukkan bahwa aksi terorisme ini pada dasarnya masuk ke dalam security dilemma yang berarti segala upaya yang dilakukan untuk mencapai keamanannya dan akan memicu rasa tidak aman bagi negara lain.

Kata Kunci : Kejahatan Siber, Terorisme, Keamanan, Amerika Serikat

Pendahuluan

Berbagai fenomena yang terjadi di dunia terlihat telah memberikan pengaruh positif dan negatif. Dengan berkembangnya zaman, fenomena yang terjadi dalam dunia internasional bisa saja berkaitan erat dengan dunia maya. Menilik pada hal negatif, berbagai kejahatan lintas negara yang tadinya hanya dapat dilakukan secara tradisional kini mulai menemukan cara baru. Salah satu tindak kejahatan dengan pemanfaatan teknologi informasi dan komunikasi adalah terorisme. Kemunculan dunia siber memberikan tantangan baru bagi para pelaku teror di seluruh dunia untuk menjadikannya instrumen dalam memperluas jaringan teroris. Bagi faktor ketahanan politik, terorisme menjadi ancaman atas kedaulatan sebuah negara. Kesesuaian antara kebijakan publik menjadi parameter bagi terciptanya sebuah kondisi politik yang kondusif. Di sisi lain, terorisme erat dengan negara yang rentan akan konflik dan kesenjangan sosial. Begitu pula dengan perkembangan teroris dalam dunia siber yang menjadi ancaman dan harus difokuskan demi membangun ketahanan sosial. Pasca

peristiwa terorisme yang menghancurkan gedung World Trade Center di Amerika Serikat, negara-negara di seluruh dunia mulai untuk kembali meningkatkan keamanan agar hal tersebut tidak terjadi di negaranya. Namun permasalahan semakin rumit di mana aksi kejahatan khususnya terorisme mulai menemukan cara terkini sehingga tindakannya sulit dilacak.

Contohnya sebagaimana yang terjadi di Washington, Amerika Serikat dimana pada 13 Agustus 2020 Departemen Kehakiman, Departemen Keamanan dalam Negeri, dan Departemen Keuangan AS mengumumkan adanya tiga kampanye yang dilakukan tiga kelompok teroris untuk meminta dukungan atas teror di AS melalui dunia maya. Ketiga departemen tersebut menilai bahwa aksi ini melibatkan kelompok bersenjata Al-Qassam, Al-Qaeda, dan Islamic State Iraq and Suriah ("ISIS"). Seluruh aksi ini mengandalkan instrumen siber yang canggih dan dari aksinya, kelompok-kelompok teroris tersebut berhasil mengumpulkan jutaan dolar AS, menggunakan sekitar 300 akun mata uang kripto, 3 *website*, serta 4 akun Facebook yang telah disita oleh otoritas AS. Menurut berita tertulis, ketiga kelompok teroris ini melakukan tindakan yang berbeda dalam melakukan kampanye dan penggalangan dana dan beroperasi secara anonim di ruang digital(ICE.GOV, 2020).

Dalam tulisan ini, penulis handak membahas terkait aksi *cyber-terrorism* dalam kajian keamanan global melalui studi kasus "*Global Disruption of 3 terror Finance Cyber-enabled Campaigns*" yang terjadi di Amerika Serikat Agustus 2020 lalu.

Definisi Cyber-terrorism

Cyber-terrorism adalah sebuah penggabungan kata dari terorisme dan *cyberspace*(Gordon, 2003). *Cyber-terrorism* dapat diartikan sebagai penggunaan peralatan jaringan komputer untuk memberi gangguan pada sistem yang dimiliki negara, bisa pula bertujuan untuk mengintimidasi pertahanan dan kelompok sipil tertentu. Bagi para teroris, cyberspace merupakan cara yang menarik dalam pengiriman informasi, serta dinilai lebih mudah dibanding cara konvensional. Hanya dengan perangkat komputer dan akses internet, aksi ini dapat dilakukan, namun diperlukan juga penguasaan komputer tingkat tinggi (Brenner, 2002, p. 150). Cyberspace bisa juga dimanfaatkan untuk menyelesaikan masalah pada sistem dan menghindari inspeksi mendadak. Para teroris dari berbagai negara bisa saling bertukar informasi dan dapat bertemu secara online dengan leluasa tanpa takut diawasi. Intinya, cyberspace ini memberikan penawaran pada teroris sebuah keleluasaan dan fleksibilitas dalam beroperasi (Brenner, 2002).

Penggunaan *cyberspace* juga memberikan manfaat bagi teroris seperti kemampuan dalam menyerang sesuatu dari jarak yang sangat jauh. Bahkan dari negara dan benua yang berbeda serta hanya menggunakan internet. Beragam platform lain juga masih bisa digunakan para teroris untuk mencari cara dalam menjalankan aksinya. Media seperti YouTube, Facebook, Majalah Online, dan Website dapat disesuaikan demi menargetkan audiens yang mereka ingin manfaatkan. Contohnya pada *website,* informasi disiarkan pada halaman web oleh kelompok teroris bisa memiliki tujuan tertentu. Seperti pada halaman *jehad.net* dan *aloswa.org* dirancang oleh para anggota Al-Qaeda demi membuktikan dukungan pada Osama Bin Laden(K.L.G. Tan, 2003). Manfaat dari situs-situs ini merupakan bentuk dari publikasi sejarah, misi, ideologi, dan tujuan keseluruhan untuk menghancurkan musuh. Selain itu, digunakan pula untuk situs penggalangan dana, dengan harapan uang yang terkumpul dari individu bisa mendukung gerak mereka.

Studi kasus Global Disruption of 3 terror Finance Cyber-enabled Campaigns

Pada Agustus 2020 lalu, Departemen Kehakiman, Departemen Keamanan Dalam Negeri, dan Departemen Keuangan mengumumkan pembongkaran tiga kampanye yang bertujuan untuk penggalangan dana teroris melalui dunia maya, dalang dari aktivitas tersebut adalah kelompok bersenjata Al-Qassam, Al-Qaeda, dan Islamic State Iraq and Suriah (ISIS). Ketiga kampanye pendanaan teror ini diakui menggunakan alat siber yang canggih, termasuk pada permintaan sumbangan dalam bentuk uang kripto dari seluruh dunia. Otoritas yang bertugas menilai aktivitas teror ini berujung pada penyitaan ratusan dolar mata uang kripto dan ini menjadi yang terbesar yang pernah dilakukan pemerintah dalam konteks terorisme di AS. tindakan ini menunjukkan bagaimana organisasi teroris yang berbeda menyesuaikan kegiatan pendanaan teroris dengan cara yang selaras yaitu menggunakan kemampuan siber dan *cryptocurrency* untuk menarik perhatian dan mengumpulkan dana untuk kegiatan teroris mereka.

Kampanye pertama dilakukan oleh Brigade Al-Qassam yang berupaya melakukan penggalangan dana c*ryptocurrency* pada awal 2019. Dimulai dengan Brigade al-Qassam memposting panggilan di halaman media sosialnya untuk sumbangan bitcoin untuk mendanai kampanye terornya pada awal 2019. Brigade al-Qassam kemudian memindahkan permintaan ini ke situs resminya, *alqassam.net*, *alqassam.ps*, dan *qassam.ps*. Kelompok Al-Qassam melakukan penipuan apabila donasi bitcoin tidak mampu diselidiki dan akan dimanfaatkan untuk kekerasan. Halaman web para teroris bisa menampilkan video tentang cara ber donasi tanpa mencantumkan identitas. Namun, sumbangan tersebut tidak anonim. Bekerja sama, agen IRS, HSI, dan FBI melacak dan menyita semua 150 akun cryptocurrency yang mencuci dana ke dan dari akun Brigade Al-Qassam.

Berikutnya, kampanye Al-Qaeda dan kelompok teroris yang berafiliasi, sebagian besar berbasis di Suriah. Sebagai rincian pengaduan penyitaan, organisasi teroris ini melakukan pencucian uang dalam bentuk bitcoin melaui saluran Telegram dan sosial media lain agar bisa mendapatkan dana berupa *cryptocurrency* guna melanjutkan tindakan teroris mereka. Beberapa kasus, kelompok tersebut berlaku sebagai badan amal tapi, pada kenyataannya, mereka secara jelas menggalang dana untuk aktivitas terorisme.

Terakhir, kampanye yang dilakukan ISIS dengan cara menggabungkan inisiatif Departemen memerangi pengelabuan yang berhubungan COVID-19. Keluhan itu menyoroti skema Murat Cakar, seorang fasilitator ISIS yang memiliki tanggung jawab dalam mengelola operasi peretasan ISIS, dan menjual APD palsu lewat situs FaceMaskCenter.com. Halaman web tersebut mengklaim menjual masker respirator N95 yang disetujui FDA, padahal barang tersebut tidak disetujui FDA. Administrator situs mengklaim memiliki persediaan masker yang hampir tidak terbatas, meskipun barang-barang tersebut secara resmi ditetapkan sebagai barang langka.

Cyber-terrorism dalam Perspektif Keamanan Global

Menganalisis permasalahan *Cyber-terrorism* menggunakan sudut pandang keamanan global maka hal ini berkaitan dengan *security dilemma*. Dilema keamanan dapat didefinisikan sebagai serangkaian tindakan dan tanggapan dari segi keamanan negara lain (pengembangan senjata). Segala upaya yang dilakukan suatu negara untuk mencapai keamanannya (terutama dengan memperkuat kemampuan militernya) akan memicu rasa tidak aman di negara lain. Faktor-faktor dilema keamanan adalah: (1) komunikasi yang buruk antara kedua pihak, (2) faktor sejarah atau kondisi kontemporer, (3) kemajuan teknologi senjata, dan sulit untuk membedakan apakah itu ofensif atau defensif. Selain itu, dilema keamanan dalam keamanan global merupakan ide terstruktur yang di dalamnya terdapat usaha atau langkah yang diambil oleh negara demi menjaga kebutuhan keamanannya sendiri. Dibalik niat yang dimiliki,

biasanya hal tersebut cenderung menimbulkan rasa tidak nyaman terhadap negara lain. Karena setiap negara berpendapat bahwa aktivitas yang dilakukannya hanya bersifat defensif dan aktivitas negara lain bersifat mengancam (Herz, 1950).

Seperti yang kita tahu bahwa sistem internasional memiliki sifat anarki dan setiap negara memerlukan kekuatan dan keamanan yang stabil. Instrumen seperti persenjataan, militer, kemampuan teknologi yang canggih akan membuktikan bahwa negara tersebut cukup kuat dan berbagai instrumen tersebut merupakan bentuk pertahanan dari ancaman negara lain. Tidak hanya negara, dilema keamanan juga bisa muncul akibat faktor eksternal seperti ancaman radikalisme yang akan ada di masa depan dan negara bukan sebagai faktor pendorongnya (Mitzen, 2006).

Cyber-terrorism sebagai kejahatan cara baru memberikan ancaman bagi negara yang diserang, dalam kasus ini adalah Amerika Serikat. Upaya yang dilakukan sekelompok teroris ini memicu rasa tidak aman bagi AS. Amerika Serikat tidak jarang mendapatkan ancaman dari beberapa kelompok terorisme dan dalam beberapa kasus sampai memakan korban jiwa. Faktor munculnya dilema keamanan ini tentunya komunikasi yang buruk dari AS dan negara asal kelompok teroris ini. Atau bahkan hanya kebencian kelompok tersebut terhadap negara adidaya tersebut. Masih banyak kemungkinan lain yang mendukung geraknya aktivitas para teroris dalam melakukan penyerangan.

Kesimpulan

Cyber-terrorism merupakan penggunaan peralatan jaringan komputer untuk memberi gangguan pada sistem yang dimiliki negara, bisa pula bertujuan untuk mengintimidasi pertahanan dan kelompok sipil tertentu. *Global Disruption of 3 terror Finance Cyber-enabled Campaigns* sebagai contoh nyata tindakan terorisme menggunakan instrumen siber. Dalam kasus ini, adanya kampanye yang mendukung pendanaan teroris melalui dunia maya melibatkan tiga kelompok terorisme dari Timur Tengah. Ketiga kelompok tersebut melakukan pengelabuan dengan cara berbeda namun dengan tujuan yang sama. Perspektif keamanan global memandang tindakan iniberhubungan dengan *security dilemma*. *Security dilemma* sendiri memiliki definisi segala upaya yang dilakukan suatu negara untuk mencapai keamanannya (terutama dengan memperkuat kemampuan militernya) akan memicu rasa tidak aman di negara lain. Maka dari itu, dengan adanya sistem internasional yang bersifat anarki ini, setiap negara perlu memiliki sistem keamanan yang kuat meliputi berbagai macam instrumen. Baik yang tradisional maupun kontemporer. Dalam menyelesaikan permasalahan ini, AS mencerminkan tekad untuk menargetkan dan membongkar pelaku terorisme dunia maya dan pencucian uang yang canggih ini di seluruh dunia, serta terus menjaga keamanan negaranya dengan baik.

Daftar Pustaka

Brenner, S. W. (2002, may 20). *Cyber-terrorism: How real*. Diambil dari Media Asia: https://doi.org/10.1080/01296612.2002.

Gordon, S. F. (2003, - -). *Cyber-terrorism?* Diambil dari symantec: www.symantec.com

Herz, J. H. (1950). Internationalism and the Security Dilemma. *Cambridge University press*, 157.

ICE.GOV. (2020, August 13). *Global disruption of 3 terror finance cyber-enabled campaigns*. Diambil dari U.S Immigration and Costoms Enforcement: https://www.ice.gov/news/releases/global-disruption-3-terror-finance-cyber-enabled-campaigns

K.L.G. Tan. (2003). Confronting Cyberterrorism with Cyber Deception. *Naval Postgraduate School, California*, 3.

Mitzen, J. (2006). Ontological Security in World Politics:. *Ohio State University, USA*, 347.