Intermestic: Journal of International Studies
e-ISSN 2503-443X
Volume 1, No. 1, November 2016 (23-35) doi:10.24198/intermestic.v1n1.3

TANTANGAN INTELIJEN DALAM KONTRA-TERORISME DI INDONESIA: SUATU PANDANGAN

Emil Mahyudin

Departemen Hubungan Internasional Universitas Padjadjaran
email: emil.mahyudin@unpad.ac.id

Abstract

The September 11th 2001 attact in the United States has become the world's turning point, from how terrorism actors operate globally through networks to how states and international relations actors response towards it. This article about the challenges for intellegence in counter-terrorism in Indonesia and the preventive actions needed especially in the use of information technollogy, as the form of detection effort and early warning for the terrors. Through the literature reviews, it is found that in practice the Indonesians intellegence activities are tend to not well organized from one institution to another because of the trust-deficit, overlapping activities and accuration of intellegence, and the lack of concrete actions in eliminating the terrorism threats in cyber sphere. It can be concluded that the comprehensive and integrative efforts are needed in organizing the intelligence in Indonesia. On the other hand, the national strategy on counter-terrorism in cyber area through the comprehensive use of information technology on the cyber terrorism threats.

Keywords: *counter-terrorism, cyber security, information technology, intellegence, terrorism*

Abstrak

Serangan 11 September 2001 di Amerika Serikat menjadi titik balik bagi dunia, baik dari bagaimana aktor-aktor terorisme beroperasi secara global melalui jaringan-jaringan, hingga bagaimana negara dan aktor-aktor hubungan internasional merespons aksi-aksi teror. Tulisan ini mengenai tantangan intelijen dalam kontra-terorisme di Indonesia dan aksi preventif yang diperlukan terutama pada penggunaan teknologi informasi, sebagai suatu upaya deteksi dan peringatan dini bagi kewaspadaan terhadap aksi-aksi teror. Melalui telaah kepustakaan, ditemukan bahwa pada praktiknya kegiatan intelijen Indonesia cenderung tidak terkoordinasi dengan baik antara satu lembaga dengan lainnya yang disebabkan oleh adanya *trust-deficit*, tumpang tindih aktivitas akumulasi dan akurasi intelijen, serta ketiadaan aksi konkret untuk mengeliminasi ancaman di ranah *cyber*. Disimpulkan bahwa dibutuhkan suatu upaya komprehensif dan integratif dalam mengelola intelijen di Indonesia. Selain itu, suatu strategi nasional *counter-terrorism* dalam ranah *cyber* melalui penggunaan teknologi informasi yang menyeluruh dalam ranah *cyber*.

Kata Kunci: *counter-terrorism, cyber security*, intelijen, teknologi informasi, terorisme

Pendahuluan

Terorisme telah bertransformasi menjadi ancaman global sejak serangan 11 September 2001 di Amerika Serikat. Bila di masa sebelumnya aksi terorisme hanya melanda beberapa negara tertentu dengan skala operasi yang terbatas, saat ini aksi terorisme berpotensi mengancam mayoritas negara di dunia lewat skala operasi global. Kemajuan teknologi informasi membuat kelompok teroris lebih mudah dalam berkomunikasi, meskipun semua sarana komunikasi yang tersedia senantiasa berada dalam pengawasan aparat keamanan. Berkecamuknya konflik di beberapa negara Arab yang dikenal sebagai *Arab Spring* turut menjadi ladang subur bagi persemaian terorisme, di mana para teroris dari berbagai penjuru dunia berdatangan ke sana untuk berjuang mencapai tujuannya (IHS, 2012).

Kini ancaman terorisme yang dihadapi oleh Indonesia telah berevolusi dibandingkan 16 tahun lampau. Para teroris telah melakukan regenerasi di mana jaringan generasi teroris terbaru kini memiliki keterkaitan yang lebih kuat dengan jaringan kelompok teroris global. Pergeseran kepemimpinan terorisme global dari Al Qaedah ke ISIS mempengaruhi pula jaringan terorisme di Indonesia (IHS, 2015). Hal tersebut menyebabkan jaringan kelompok teroris di Indonesia kini berbaiat kepada ISIS (BBC, 2016). ISIS sendiri sangat intensif melakukan penyebaran dan propaganda ajarannya lewat media sosial di internet untuk menjaring pengikut baru yang dihadapkan mampu melaksanakan serangan di wilayah masing-masing secara mandiri. (IHS Jane's Intelligence Review, 2015: 8-13).

Konflik di Arab yang berimbas pada munculnya ISIS berimplikasi pada kian besar dan kompleknya upaya Indonesia untuk melaksanakan *counter-terrorism*. Aksi penegakan hukum terhadap para teroris di Indonesia dianggap belum diimbangi dengan keberhasilan program deradikalisasi (Kompas, 2016). Selain itu, dari aspek hukum peraturan perundang-undangan Indonesia yang terkait dengan terorisme dinilai belum mampu mencakup semua aspek kegiatan terorisme (Antara, 2016). Atau dengan kata lain, masih ada celah dalam undang-undang terorisme yang dapat dimanfaatkan oleh para teroris guna lolos dari jeratan hukum.

Begitu pula dengan peran intelijen dalam *counter-terrorism*, di mana masih kuat pandangan bahwa komunitas intelijen Indonesia selalu mengalami *intelligence failure* dalam kasus terorisme (Setyawan, 2016). Pandangan demikian selalu muncul apabila terjadi aksi terorisme, termasuk dalam kasus di kawasan M.H. Thamrin, Jakarta pada 14 Januari 2016. Makalah ini akan mengulas tentang pandangan tentang tantangan intelijen dalam *counter-*

terrorism di Indonesia, di mana pembahasan dibatasi pada kapasitas dan kapabilitas organisasi intelijen itu sendiri.

Terorisme

Dewasa ini dunia tengah menghadapi ancaman terorisme, termasuk Indonesia. Kelompok teroris telah melancarkan sejumlah serangan mematikan dengan jumlah korban besar untuk menegaskan tujuan politik mereka. Serangan itu terjadi baik di negara maju seperti Amerika Serikat, Inggris dan Spanyol, maupun di negara berkembang termasuk di Indonesia. Selain serangan 11 September 2001 di Washington DC dan New York, juga terjadi serangan teroris di Madrid pada 11 Maret 2004 dan London pada 7 Juli 2005. Begitu pula serangan teror di Indonesia yang terjadi di beberapa tempat sejak 2000 hingga kini dengan jumlah korban yang cukup signifikan.

Terorisme sesungguhnya adalah bagian dari perang. Seberapa buruk pun itu, perang adalah bagian dari peradaban manusia. Perang merupakan upaya terakhir manusia untuk mempertahankan hidup mereka melalui tindakan kekerasan secara massal yang melibatkan kekuatan militer dalam jumlah tertentu. Terorisme mempunyai karakteristik utama, yaitu penggunaan kekerasan yang meliputi pembajakan, penculikan, bom bunuh diri, dan lain sebagainya (Winarno, 2011:171).

Lindemann (2010) dalam *Causes of War: The Struggle for Recognition*, mengungkapkan bahwa dalam perang, pihak militer berperan sangat penting dalam menentukan tujuan, arah, strategi, operasi, taktik, dan itu merupakan arena yang dilakukan dalam menunjang apa yang dinamakan keamanan nasional. Bagaimanapun juga, tujuan dari kerja keras dan perjuangan dalam perang adalah untuk mendapatkan pengakuan, terutama pengakuan secara politik, baik dengan alasan keberlanjutan maupun keamanan nasional.

Terorisme yang kini berkembang merupakan salah satu bentuk perang yang bersifat asimetris, di mana pihak teroris yang secara kuantitas dan kualitas lemah dihadapkan pada aktor negara dengan berbagai cara mencoba mengeksploitasi kelemahan aktor negara agar posisi mereka lebih kuat lagi guna mencapai tujuan yang telah ditetapkan. Terorisme merupakan fenomena yang kompleks dan karenanya tidak ada penjelasan tunggal yang bisa menjawab motif tindakan terorisme secara memuaskan (Winarno, 2011:175).

Terorisme sebagai isu keamanan international menuntut kerjasama antar negara untuk menghadapinya. Sejumlah organisasi internasional telah mendefinisikan terorisme

sesuai dengan kepentingan bersama mereka. Misalnya dalam *The Agreement on Information Exchange and Establishment of Communication Procedures* yang ditandatangani oleh Indonesia, Malaysia dan Filipina (*The Trilateral Agreement*) pada 7 Mei 2002, terorisme didefinisikan sebagai:

> *Any act of violence of threat thereof perpetrated to carry out within the respective territories of the Parties or in the border area of any of the Parties an individual or collective criminal plan with the aim of terrorizing people of threatening to harm them or imperiling their lives, honor, freedoms, security or rights or exposing the environment or any facility or public or private property to hazards or occupying or seizing them, or endangering a national resource, or international facilities, of threatening the stability, territorial integrity, political unity or sovereignty of independent States.*

ASEAN sendiri pada 13 Januari 2007 menandatangani *The ASEAN Convention on Counter Terrorism* (ACCT). ACCT mendefinisikan teorisme pada berbagai konvensi PBB yang mengkriminalisasikan aksi terorisme, seperti *Convention for the Suppression of Unlawful Seizure of Aircraft 1970, Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation 1971* dan *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation 1988*.

Apabila diteliti lebih jauh, tidak ada definisi tunggal tentang terorisme. Sejauh ini negara-negara di dunia baru sepakat pada empat macam kriteria terorisme. Kriteria itu mencakup target, tujuan, motivasi dan legitimasi dari aksi terorisme tersebut. Sebagai contoh adalah PBB yang setidaknya memiliki dua definisi tentang terorisme.

Pertama, Resolusi Dewan Keamanan PBB No.1566 (2004) yang mendefinisikan terorisme sebagai *criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act*. (Azdema, 2015).

Kedua, Panel PBB pada 17 Maret 2005, mendeskripsikan terorisme *as any act "intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act*." (Azdema, 2015).

Begitu pula dengan sejumlah negara di dunia, mempunyai definisi masing-masing mengenai terorisme. Inggris melalui Terrorism Act 2000 mendefinisikan terorisme *to*

include an act "designed seriously to interfere with or seriously to disrupt an electronic system".[i] Adapun Amerika Serikat mempunyai lebih dari satu definisi tentang terorisme. Dalam Patriot Act 2001 aktivitas terorisme termasuk: (Azdema, 2015)

- *threatening, conspiring or attempting to hijack airplanes, boats, buses or other vehicles.*
- *threatening, conspiring or attempting to commit acts of violence on any "protected" persons, such as government officials*
- *any crime committed with "the use of any weapon or dangerous device," when the intent of the crime is determined to be the endangerment of public safety or substantial property damagerather than for "mere personal monetary gain*

Sedangkan FBI yang merupakan salah satu penegak hukum Amerika Serikat mendefinisikan terorisme sebagai *The unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives*. (Azdema, 2015).

Ketidaksepakatan tentang definisi terorisme juga melingkupi para pakar. Bahkan, ada pakar yang tidak secara khusus mendefinisikan terorisme, namun lebih mengemukakan pada jenis, tujuan dan ciri-ciri terorisme. Misalnya adalah Wilkinson (2001:59) yang membagi terorisme dalam empat bentuk. Yaitu terorisme epifenomenal, terorisme revolusioner, terorisme subrevolusioner, dan terorisme represif.

Menurut Wilkinson, terorisme epifenomenal adalah terrorisme tanpa tujuan yang jelas. Adapun terorisme revolusioner mempunyai tujuan khusus yaitu untuk mengubah secara radikal suatu keadaan atau sistem. Sedangkan terorisme subrevolusioner adalah teror yang bertujuan untuk menekan pemerintah untuk mengubah kebijakan tertentu. Selanjutnya terorisme represif adalah aksi teror yang menindas orang lain atau kelompok lain.

Intelijen dan Teknologi Informasi

Dalam membahas tentang *counter-terrorism*, salah satu titik kritis adalah bagaimana peran intelijen di dalamnya. Sudah menjadi kehendak semua pihak agar serangan intelijen dapat digagalkan sejak dari tahap perencanaan dan persiapan, akan tetapi bahkan intelijen negara maju pun yang dilengkapi dengan sumberdaya yang besar masih tetap saja mengalami *intelligence failure*. Contoh kasus mutakhir akan *intelligence failure* adalah serangan teroris di Paris pada 13 November 2015. *Intelligence failure* terjadi pada tingkat Uni Eropa walaupun organisasi itu telah mempunyai mekanisme *intelligence sharing* (IHS Jane's Intelligence Review, 2016: 8-13).

Intelijen menurut Kent (1965) adalah: *"The knowledge which our highly placed civilian and military men must have to safeguard the national warfare"*. Sedangkan menurut Laksamana William F. Raborn: "*Intelligence is refers to information which has been carefully evaluated as to its accuracy and significance"*. Perbedaan antara "intelijen" dan "informasi" terletak pada proses evaluasi terhadap akurasi dan *assessing* signifikansinya terhadap keamanan nasional (Ransom, 1971:7). Sebagaimana diketahui, intelijen memainkan peranan kunci dalam pengambilan keputusan, karena masukan dari intelijen akan menentukan warna dari keputusan yang diambil.

Intelijen sangat identik dengan kerahasiaan, termasuk sumber informasinya. Akan tetapi menurut Laksamana Ellies M. Zacharias: "*95 per cent of peacetime intelligence came from open source, 4 per cent from semi-open sources, and only 1 per cent, sometimes less, from secret agents"*. (Ransom, 1971:19). Sedangkan Letnan Jenderal Samuel Wilson menyatakan bahwa: "*ninety percent of intelligence come from open sources. The other ten percent, the clandestine work, is just the more dramatic"*. (Friedman, 2004:285).

Tidak berlebihan untuk menyatakan bahwa intelijen adalah pengetahuan mengenai ancaman, di mana ancaman adalah hasil dari perkalian antara *intention*, *capability* dan *circumstance*. Apabila salah satu dari tiga elemen itu bernilai nol, berarti ancaman tidak ada. Dalam konteks *counter-terrorism*, kerjasama intelijen merupakan suatu spektrum yang telah berlangsung lama. Dewasa ini, kerjasama intelijen cakupannya telah diperluas sehingga bukan saja untuk menghadapi aktor negara, tetapi pula aktor non negara. Melalui kerjasama intelijen, diharapkan pihak-pihak yang terlibat kerjasama dapat secara dini mendeteksi munculnya ancaman sehingga dapat mengambil langkah-langkah pencegahan sebelum ancaman itu terwujud, termasuk di dalamnya ancaman terorisme.

Salah satu kegiatan dalam kerjasama intelijen antar negara adalah *intelligence sharing*. *Sharing* dalam kerjasama intelijen merupakan sebuah tantangan tersendiri, sebab hal itu hanya dapat dilaksanakan apabila telah tercipta *trust*. Masalah tentang *trust* dalam kerjasama intelijen, pada dasarnya merupakan masalah klasik yang selalu muncul dari waktu ke waktu. Sparago (2006) menyatakan bahwa, "*In order for intelligence cooperation to work, there must be an established trust between the governments and intelligence services*". Selanjutnya, Sparago menambahkan, dalam kerjasama intelijen, terdapat *cost* yang harus ditanggung oleh semua pihak yang terlibat dalam kerjasama itu. Salah satu *cost* itu adalah,

"*In order for intelligence cooperation to be mutually beneficial to all involved, there must be equal levels of sharing*". (Sparago, 2006).

Adapun Walsh (2009:7) mendeskripsikan dengan baik menyangkut *trust* dalam *information sharing*. Walsh melihat intelijen sebagai komoditas, di mana *states share out of mutual interest or to extract things like foreign aid and security assurances.* Selanjutnya Walsh berargumen bahwa: "*The secret nature of intelligence gives rise to two key problems*. *The "sellers" of intelligence can't be sure that "buyers" will adequately protect what they receive, and "buyers" cannot be sure of the veracity of the intelligence they get from "sellers"*. (Walsh, 2009:13).

Intelijen tidak bekerja dalam ruang yang vakum, di mana kini salah satu tantangan intelijen adalah bagaimana merespon terhadap kemajuan teknologi informasi. Dewasa ini mayoritas lembaga intelijen memberikan perhatian khusus terhadap dunia teknologi informasi, karena banyak informasi yang dapat digali dari domain *cyber*. Tak dapat dipungkiri, kelompok teroris pun memanfaatkan domain *cyber* untuk mencapai tujuannya sebagaimana terlihat dalam kasus ISIS yang mengeksploitasi domain *cyber*.

Teknologi informasi pada dasarnya merupakan teknologi yang berhubungan dengan pembuatan (*generation*), pencatatan (*recording*), distribusi (*distribution*), penyimpanan (*storage*), representasi (*representation*), pengambilan (*retrival*), dan penyebaran (*dissemination*) informasi (William dan Sawyer, 2011). Perkembangan teknologi informasi sebagian berasal dari kegiatan-kegiatan penemuan bagi kepentingan pertahanan dan militer, seperti komputer yang sejarahnya terkait dengan upaya Sekutu memecahkan kode-kode mesin sandi Enigma Jerman atau internet yang pada awalnya merupakan jaringan komunikasi internal Departemen Pertahanan Amerika Serikat.

Seiring dengan perjalanan waktu, kemajuan teknologi informasi itu dipergunakan secara luas pada sektor-sektor sipil. Penggunaan teknologi informasi pada berbagai macam sektor kehidupan manusia pada tingkatan tertentu ternyata berdampak negatif, khususnya menyangkut penyalahgunaan teknologi informasi untuk kepentingan kriminal maupun kepentingan politik yang berbasis kekerasan. Dengan kata lain, teknologi informasi kini telah menjadi *weapon of choice* bagi aktor-aktor yang lebih lemah guna melancarkan serangan asimetris, termasuk teroris di dalamnya.

Selain aksi *hacking*, teknologi informasi khususnya internet saat ini dimanfaatkan pula untuk membangun kekuatan kelompok teroris. Sebagai contoh adalah penyebaran

tulisan-tulisan keagamaan yang menyerukan penggunaan kekerasan kepada pihak lain yang dianggap tidak sepaham dalam situs-situs internet. Hal itu dipandang dapat melahirkan *self radicalization* yang melahirkan *lone wolf* yang sangat berpotensi mengancam keamanan nasional. (IHS Jane's Intelligence Review, 2013). Begitu pula dengan penyebaran tulisan-tulisan tentang bagaimana membuat bom dari bahan-bahan yang tersedia di sekitar.

Dalam konteks kelompok teroris, ancaman yang ditimbulkan olehnya melalui penggunaan teknologi seperti teknologi informasi tidak dapat dipandang remeh. Bisa jadi dalam aksi mereka, korban yang jatuh tidak banyak. Akan tetapi aksi itu telah menimbulkan ketakutan yang menyebar di kalangan masyarakat dan ketakutan itulah yang menjadi tujuan dari aksi yang dilaksanakan.

Serangan *cyber* kini telah berubah menjadi ancaman lain bukan saja terhadap keamanan internasional, tetapi juga ekonomi dunia. Berbeda dengan serangan teroris yang bersifat fisik, serangan *cyber* ditujukan untuk mencuri dan atau merusak sistem data yang dimiliki oleh aktor negara dan non negara seperti perusahaan. Motif dari serangan *cyber* dapat berupa politik, dapat pula berupa ekonomi yaitu ingin mencuri rahasia bisnis kompetitor. (IHS, 2015). Sebagai contoh dari serangan *cyber* terhadap berbagai sasaran pemerintah dan perusahaan Amerika Serikat yang menurut Mandiant dilakukan oleh entitas *hacker* di Cina yang tergabung dalam Unit 61398 yang berada People's Liberation Army (PLA) General Staff Department's 3rd Department. (IHS, 2013).

Dihadapkan pada ancaman dan tantangan yang berasal dari domain *cyber*, institusi-institusi intelijen dunia telah membentuk satuan kerja khusus di bidang *cyber*. Fungsi satuan itu adalah untuk melaksanakan ofensif dan defensif sekaligus. Dikaitkan dengan konteks *counter-terrorism*, salah satu tugas unit *cyber* adalah mengawasi secara terus menerus aktivitas kelompok teroris dan para simpatisannya pada dunia maya. Sebagai contoh, media sosial seperti Twitter, Facebook dan Youtube telah menjadi media efektif bagi kelompok teroris untuk merekrut anggota baru sekaligus mendorong serangan teror yang dilaksanakan oleh para simpatisan secara mandiri/*lone wolf*.

Dalam rangka *counter-terrorism*, telah menjadi kesepakatan bahwa institusi intelijen harus mempunyai pemahaman yang mendalam terhadap kemajuan teknologi informasi dan sekaligus memanfaatkannya guna mencapai tujuan yang telah ditetapkan. Upaya *counter-terrorism* yang mengabaikan atau setidaknya tidak memberikan perhatian yang proporsional terhadap domain *cyber* justru akan berkontribusi pada *intelligence failure*.

Tantangan Intelijen Indonesia

Negara-negara di kawasan Asia Tenggara telah memiliki kerjasama intensif di bidang intelijen dalam rangka *counter-terrorism*. Efektivitas kerjasama itu cukup signifikan, karena tidak sedikit rencana aksi serangan teror berhasil dicegah karena adanya *intelligence sharing* antar negara. Namun masalahnya adalah keberhasilan kerjasama intelijen antar negara tidak selalu berbanding lurus dengan kerjasama intelijen intra-negara. Maksudnya adalah kerjasama antar institusi intelijen yang berbeda dalam satu negara yang sama. Inilah salah satu tantangan kritis yang dihadapi oleh Indonesia dalam melaksanakan *counter-terrorism* saat ini dan ke depan.

Terdapat beberapa tantangan kerjasama intelijen intra-negara di Indonesia dalam *counter-terrorism*. Setidaknya terdapat tiga tantangan dalam kerjasama tersebut. Tantangan demikian sesungguhnya bukan hal baru, akan tetapi selama bertahun-tahun tidak pernah ada penyelesaian yang sesuai dengan kepentingan nasional Indonesia.

Pertama, *trust* antar lembaga. Tingkat *trust* antar lembaga intelijen Indonesia tidak berada dalam kondisi yang baik. Bahkan dapat dikatakan terjadinya *trust deficit*. Persaingan antar institusi intelijen adalah sebuah fakta, walaupun tidak muncul ke permukaan secara terang benderang karena sifat intelijen yang memang bekerja di ruang gelap.

Terjadinya *trust deficit* antar institusi intelijen Indonesia tidak lepas dari rivalitas antar lembaga dan residu masa lalu. Rivalitas antar institusi intelijen seolah sudah given dalam dunia intelijen di setiap negara, akan tetapi hal demikian dapat diminimalkan apabila terdapat direktif politik yang kuat dari pucuk tertinggi kepemimpinan nasional. Dalam konteks ini, rivalitas khususnya terjadi antara BIN, BAIS dan Intelijen Polri sebagaimana tersirat pasca serangan teror di Jakarta akhir Januari 2016 lalu.

Upaya *counter-terrorism* di Indonesia masih belum optimal karena rivalitas demikian, di mana ditengarai setiap institusi intelijen terkait belum sepenuhnya kooperatif dalam intelligence sharing. Hal ini memang sulit untuk dibuktikan pada tingkat publik, akan tetapi atmosfir demikian terasa apabila kita “menyelam ke dalam komunitas intelijen“. Karena dalam *intelijen knowledge is power*, setiap institusi ditengarai menjaga informasi yang bersifat high value untuk tidak dibagikan kepada institusi lainnya karena berbagai alasan.

Trust deficit antar institusi intelijen diperburuk dengan residu masa lalu, di mana dalam sistem politik Orde Baru peran institusi militer sangat kuat dan dominan, termasuk di dalamnya intelijen militer. Sementara dalam era demokrasi saat ini, *counter-terrorism* dikategorikan dalam tindakan penegakan hukum yang mengacu pada KUHAP (Kitab Undang-undang Hukum Acara Pidana). Artinya, institusi intelijen militer tidak dapat berperan signifikan dalam hal tersebut. Sebaliknya, Polri tentu saja tidak ingin kewenangan penindakan dalam *counter-terrorism* terbagi dengan lembaga lain.

Kedua, peran BIN (Badan Intelijen Negara). Sesuai Undang-undang No.17 Tahun 2011 tentang Intelijen Negara, salah satu fungsi BIN adalah menyelenggarakan koordinasi intelijen negara. Dalam konteks ini, Kepala BIN berfungsi layaknya Director, *National Intelligence (DNI)* dalam komunitas intelijen Amerika Serikat. Dikaitkan dengan *counter-terrorism*, BIN memiliki kewenangan untuk mengkoordinasikan kegiatan intelijen dengan institusi intelijen lainnya.

Namun dalam prakteknya, masih menjadi pertanyaan tentang bagaimana peran BIN dalam melaksanakan fungsi tersebut. Memang betul bahwa BIN memiliki kerjasama *intelligence sharing* dengan mitranya di negara-negara lain, akan tetapi bagaimana koordinasi *intelligence sharing* antar lembaga intelijen di Indonesia yang semuanya berada di bawah koordinasi BIN. Dalam arti bukan saja BIN melakukan *intelligence sharing* kepada lembaga intelijen lain di dalam negeri, tetapi lembaga intelijen yang berada di bawah koordinasi BIN pun melakukan *intelligence sharing* kepada BIN.

Secara hukum berdasarkan Undang-undang No.17 Tahun 2011, BIN mempunyai kewenangan memaksa kepada lembaga intelijen yang berada di bawah koordinasinya untuk melaksanakan *information sharing*. Akan tetapi menjadi pertanyaan apakah kewenangan itu dapat dilaksanakan secara efektif di tengah masih kuatnya ego institusi intelijen sekaligus rivalitas antar mereka. Masalah klasik ini bukan khas Indonesia, tetapi juga terjadi di negara maju seperti Amerika Serikat yang baru dapat diminimalisasi setelah negara itu mengalami *strategic surprise* melalui serangan 11 September 2001.

Ketiga, teknologi informasi. Kelompok teroris masa kini mengeksploitasi secara luas penggunaan teknologi informasi, baik untuk propaganda, perekrutan maupun perencanaan aksi teror. Guna menghadapi hal tersebut, secara teori dibutuhkan strategi eksploitasi teknologi informasi dalam rangka *counter-terrorism*. Namun nyatanya hal demikian belum ada, di mana pendekatan yang diadopsi lebih banyak bersifat *ad-hoc* dan sekaligus reaktif.

Di Indonesia, kelompok teroris telah menggunakan teknologi internet dalam melancarkan aksinya. Penggunaan itu mulai dari mulai menyusun rencana teror, pelatihan, pembiayaan, rekrutmen hingga eksekusi. Hal itu berdasarkan temuan aparat keamanan dalam beberapa tahun terakhir, yang memperkuat keyakinan bahwa kemampuan kelompok itu tidak dapat dipandang sebelah mata.

Di sisi lain, institusi intelijen nampaknya baru belakangan mulai memberikan perhatian khusus dan tersendiri terhadap domain *cyber* dalam menghadapi terorisme. Sebagai ilustrasi, sampai saat ini belum ada pengawasan khusus terhadap media sosial dan situs internet yang berafiliasi atau bersimpati kepada kelompok teroris yang dilaksanakan oleh institusi intelijen. Penutupan akun media sosial dan situs internet yang berafiliasi atau bersimpati kepada kelompok itu dilakukan oleh Kementerian Komunikasi dan Informatika mayoritas bukan berdasarkan laporan dari institusi intelijen, akan tetapi hasil pengawasan dari kementerian itu sendiri. Dengan kata lain, institusi intelijen Indonesia terlambat merespon kemajuan teknologi informasi, khususnya domain *cyber*.

Di samping itu, sistem perbankan, telekomunikasi, pembangkit listrik dan lain sebagainya juga rentan terhadap serangan *cyber*. Kemampuan kelompok teroris dalam melancarkan serangan terhadap sasaran-sasaran itu tidak perlu diragukan lagi, sehingga dibutuhkan adanya pemahaman terhadap karakteristik ancaman demikian dan bagaimana strategi untuk menangkalnya. Bukan tidak mungkin sistem-sistem yang telah disebutkan itu suatu saat akan menjadi sasaran di Indonesia, di mana kerugian material atas serangan *cyber* tidak kalah dahsyatnya dibandingkan serangan kinetik.

Baru beberapa waktu silam beberapa institusi intelijen telah membentuk satuan *cyber* sendiri yang hingga kini masih mencari bentuk. Di antara tantangan satuan tersebut adalah mereka harus beroperasi tanpa adanya strategi nasional tentang bagaimana melaksanakan *counter-terrorism* pada domain *cyber*. Bahkan pada hirarki yang lebih tinggi, Indonesia belum merumuskan strategi nasional pada domain *cyber*. Melihat besarnya cakupan domain *cyber* yang harus dilindungi, instituasi intelijen tidak dapat sendirian bekerja untuk menangkalnya.

Langkah ke Depan

Sejumlah tantangan yang dihadapi oleh Indonesia dalam melaksanakan *counter-terrorism*, khususnya pada institusi intelijen, tentu saja memiliki solusi. Solusi pertama dan utama

adalah harus adanya kemauan dari kepemimpinan nasional untuk membenahi institusi intelijen Indonesia, khususnya dari aspek kerjasama dan koordinasi. Dalam konteks ini, kepemimpinan nasional harus *hands on* dan tidak dapat begitu saja mendelegasikan kepada BIN sebagai lembaga intelijen negara yang berwenang menyusun kebijakan nasional di bidang intelijen sekaligus koordinator intelijen negara. Belajar dari kasus penataan ulang komunitas intelijen Amerika Serikat pasca serangan 11 September 2001 yang di antaranya melahirkan jabatan DNI yang berpisah dari jabatan Direktur CIA, penataan sukses dilaksanakan karena Presiden Amerika Serikat langsung *hands on*.

Berikutnya, Indonesia belum terlambat untuk merumuskan strategi nasional *counter-terrorism* pada domain *cyber*. Beberapa satuan *cyber* yang tersebar di sejumlah institusi intelijen harus bekerja dalam satu strategi yang sama, sehingga di situlah mendesaknya penyusunan strategi tersebut. Hendaknya menjadi kesadaran bersama bahwa dengan memanfaatkan kemajuan teknologi informasi, khususnya media sosial dan internet, kelompok teroris dapat menyebarkan propaganda sekaligus perekrutan kepada siapa saja yang mengakses domain *cyber*. Selain itu, kelompok teroris juga mempunyai sumberdaya manusia yang mampu melaksanakan serangan *cyber* pada sasaran strategis seperti perbankan, telekomunikasi, sistem pembangkit listrik dan lain sebagainya.

Daftar Pustaka

Antara. (2016). “Pemerintah Akan Percepat Revisi Undang-undang Terorisme”. Diunduh dari www.antaranews.com/berita/540664/pemerintah-akan-percepat-revisi-undang-undang-terorisme, diakses pada 17 Februari 2016.

Azdema. (2016). Diunduh dari www.azdema.gov/museum/famousbattles/pdf/Terrorism%20Definitions%20072809.pdf, diakses pada 17 Februari 2015.

BBC. (2016). “MIT dan JAT: Dua Kelompok Teror Indonesia Terkait ISIS”. Diunduh dari www.bbc.com/indonesia/berita_indonesia/2016/01/160115_indonesia_explainer_kelompok_teror”, diakses pada 17 Mei 2016.

Friedman, Richard S. (2004). “Open-Source Intelligence: A Review Essay”, dalam George, Roger Z and Kline, Robert D, *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, Washington DC: National Defense University, 2004, h. 285.

IHS Jane’s Defence Weekly. (2012). “Annual Defence Report: Middle East and Africa”, 7 December 2012.

-------. (2012). “Briefing: Cyber Espionage”, 3 November 2015.

-------. (2013). “US Company Identifies Chinese Cyber Unit”, 20 February 2013.

IHS Jane’s Intelligence Review. (2013). “Ahead of the Pack – Lone wolf terrorist attack increased”, 19 July 2013.

-------. (2015). “Cyber-mercenary industry grows worldwide”, 21 July 2015.

-------. (2015). "How Al Qaeda and Islamic State Differ in Pursuit Common Goal", 20 March 2015.
-------. (2016). "Paris Attack Focus on EU intelligence failure", January 2016, Vol 28, Issue 1, h. 8-13.
-------. (2016). "Virtual Engagement: Counter-radicalisation moves onto social media", December 2015, Vol.27, Issue 12, h. 8-13.
Lindemann, T. (2010). *Causes of War: The Struggle for Recognition*. ECPR Press
Kent, Sherman. (1965). *Strategic Intelligence for the American Policy*. Connecticut: Hamden.
Kompas. (2016). "Menteri Agama Akui Program Deradikalisasi Masih Ada Kekurangan". Diunduh dari www.nasional.kompas.com/read/2016/01/17/17255881/Menteri.Agama.Akui.Program.Deradikalisasi.Masih.Ada.Kekurangan, diakses pada 17 Februari 2016.
Ransom, Harry Howe. (1971). *The Intelligence Establishment*. Massachusetts: Harvard University Press.
Setyawan, Fery Agus. (2016). *Ledakan Bom Sarinah, Kegagalan BIN Antisipasi Teror.* Diunduh dari http://news.okezone.com/read/2016/01/15/337/1288604/ledakan-bom-sarinah-kegagalan-bin-antisipasi-teror", diakses pada 17 Februari 2016.
Sparago, Marta. (2016). "The Global Intelligence Network: Issues in International Intelligence Cooperation", dalam *Perspective in Global Issues*, Vol.1 Issue 1, Winter 2006. Diunduh dari www.perspectivesonglobalissues.com/0101/GlobalIntelligenceNetwork.html, diakses pada 16 Februari 2016.
Walsh, James Igoe. (2009). *The International Politics of Intelligence Sharing*. New York: Columbia University Press.
William, Bryan K and Stacey K Sawyer. (2011). *Using Information Technology. 9th Edition*, New York: McGraw Hill.
Wilkinson, Paul. (2001). *Terrorism Versus Democracy: The Liberal State Response*. New York: Routledge.
Winarno, Budi. (2011). *Isu-isu Global Kontemporer*. Yogyakarta: CAPS.