CYBERTERRORISM: SUATU TANTANGAN KOMUNIKASI ASIMETRIS BAGI KETAHANAN NASIONAL

[1]Aa Bambang A.S., [2]Idealisa Fitriana

Abstrak.*Cyberterrorism merupakan aktivitas dan/atau metode yang digunakan oleh sejumlah jaringan atau kelompok teroris. Tidak dapat dipungkiri bahwa dunia maya dan kemajuan teknologi mudah menjadi wadah bagi mereka dalam melakukan aksinya. Dalam mewujudkan ketahanan nasional, diperlukan penanggulangan yang menyeluruh atas ancaman penyalahgunaan teknologi informasi dan komunikasi (cyber threat/asymmetric threat untuk kepentingan aksi teror. Cyberterrorism constitutes an activity and/or a method used by any linkages or terrorism groups. It is almost undeniable for cyber realm and technology development could become such media to do their acts. To make a kind of national resilience into the real one, it is necessary to form counter-measures as a whole over the misused of communication and information technology, yet its threat (cyber threat/asymmetric threat for terrorism purposes.*

Kata kunci: Cyberterrorism, komunikasi asimetris, ketahanan nasional.

1. Pendahuluan

Secara harfiah, Indonesia memiliki pandangan atau perspektif atas diri dan lingkungannya. Perspektif ini didasarkan pada UUD 1945 dan Pancasila. Hal tersebut terangkum dalam konsep Wawasan Nusantara. Wawasan bangsa Indonesia yaitu wawasan nusantara yang mengarah pada proses pembangunan menuju tujuan nasional. Pemahaman mengenai wawasan nusantara tidak akan terlepas dari pembahasan mengenai ketahanan nasional. Ketahanan nasional menjadi suatu kondisi yang harus diwujudkan dalam mencapai tujuan nasional. Ketahanan nasional berkaitan dengan keamanan komprehensif (menyeluruh) yang meliputi aspek pertahanan dan keamanan, ideologi, politik, ekonomi, sosial, dan budaya. Produk dari aspek-aspek ini adalah tujuan nasional yang dicapai melalui wawasan nusantara. Wawasan nusantara dipengaruhi oleh beberapa faktor, yaitu wilayah, geopolitik-geostrategi, serta perkembangan wilayah Indonesia. (*www.academia.edu/7049399/ANALISIS KETERKAITAN WAWASAN NUSANTARA DENGAN KETAHANAN NASIONAL*)

Indonesia tengah mengalami peningkatan pada isu geopolitiknya. Hal ini tentu menjadi masalah yang patut dipertimbangkan terkait dengan pembangunan ketahanan nasional. Isu geopolitik biasanya mengutamakan strategi yang berkenaan dengan pemahaman mengenai bagaimana isu-isu di suatu wilayah dipengaruhi dan mempengaruhi sistem politik suatu negara. Salah satu isu geopolitik yang marak hingga saat ini adalah isu terorisme. Jika dikaitkan dengan aspek kemasyarakatan dalam unsur kehidupan nasional, isu terorisme juga menyinggung masalah ketahanan ideologi, politik, dan pertahanan keamanan. (Hendropriyono, 2009:350)

Terorisme menjadi ancaman terhadap ketahanan ideologi Indonesia. Percaturan politik internasional menuntun Indonesia untuk dapat menghadapi berbagai kepentingan ideologi yang berbeda. Untuk dapat

mewujudkan ketahanan nasional, Indonesia diharapkan kembali pada filsafat bangsa yang meliputi keseluruhan ideologi, yaitu demokratis, nasionalis, religius, humanis serta berkeadilan sosial. Dalam menghadapi isu terorisme, Indonesia digiring untuk mempertahankan ideologi pancasila dari maraknya fundamentalitas terhadap agama. Agama bersifat universal dan seharusnya dipandang secara inklusif, bukan secara tekstual dan eksklusif. Sementara itu, doktrin radikal adalah hal inti dalam permasalahan terorisme yang memberikan tantangan bagi kekuatan Indonesia untuk membangun ketahanan nasionalnya.

Pada aspek ketahanan politik, terorisme menjadi satu ancaman atas kedaulatan Negara Kesatuan Republik Indonesia. Ketahanan politik berbasis pada kehidupan dan sistem politik. Keselarasan kebijakan publik dengan kepentingan masyarakat menjadi tolak ukur bagi terciptanya kondisi politik yang kondusif. Sementara itu, terorisme tumbuh pesat di daerah yang rentan akan konflik dan kesenjangan sosial. Rasa tidak puas dan ketidakadilan memberikan peluang bagi suatu kelompok dalam melakukan aksi terorisme. Ketidakstabilan keamanan akibat aksi pengeboman dan aktivitas terorisme lainnya jelas mengancam ketahanan di bidang keamanan dan pertahanan.

Saat ini, terorisme tidak hanya sekedar berbentuk fisik. Terorisme telah hidup dan berkembang melalui pemanfaatan teknologi informasi dan komunikasi (*cyberterrorism*). Kerumitan dunia *cyber* memberi inspirasi bagi pelaku teror di Indonesia untuk menjadikannya sebagai media dalam mengembangkan jaringan teroris. Terorisme yang tumbuh dan berkembang melalui dunia *cyber* adalah salah satu ancaman yang perlu menjadi fokus utama dalam membangun ketahanan nasional. Berdasarkan fenomena ini, masalah dirumuskan: 1) Bagaimana *cyberterrorism* menjadi ancaman asimetris bagi pembangunan ketahanan nasional?, 2) Seperti apa penanggulangan *cyberterrorism* yang dapat dilaksanakan?

Pada hakikatnya, tulisan ini ingin memperkenalkan ancaman asimetris kepada khalayak masyarakat. Dengan begitu, masyarakat atau pembaca dapat memahami dan waspada terhadap keberadaan tantangan asimetris seperti *cyberterrorism*. Melalui rumusan masalah, tulisan ini juga bertujuan untuk menjelaskan urjensi dari keberadaan *cyberterrorism* serta signifikansi penanggulangan *cyberterrorism* dalam mewujudkan pembangunan ketahanan nasional.

2. Pembahasan

Terorisme dan Asas Ketahanan Nasional

Ketahanan nasional mempunyai prasyarat dalam hal perwujudannya, yaitu asas-asas:

1. Kesejahteraan dan Keamanan
2. Komprehensif (terintegrasi)
3. Mawas diri ke dalam dan ke luar
4. Kekeluargaan

(www.dosenpendidikan.com/pengertian-azas-ketahanan-indonesia-menurut-uud/)

Keempat asas ini berkaitan dengan isu terorisme sebagai tantangan asimetris bagi pembangunan ketahanan nasional. Pada hakikatnya penanggulangan terorisme juga mengutamakan asas-asas ketahanan nasional.

Kesejahteraan dan keamanan merupakan tolak ukur pencapaian ketahanan nasional. Ketika berbicara mengenai terorisme, maka terdapat *root of causes* (penyebab) dari adanya aksi

terorisme itu sendiri. *greed* (ketidakpuasan) dan *grievance* (keluhan) muncul karena mereka merasa mengalami ketidakadilan atas distribusi kesejahteraan yang tidak merata (motif ekonomi) atau kebijakan dari segala aspek kehidupan.

Dalam mencegah atau menanggulangi terorisme dibutuhkan elemen penopang dalam mencapai kesuksesannya. Salah satu elemennya adalah legislasi atau kepercayaan publik. Hal ini didukung oleh beberapa faktor seperti konsesi politik, indikator ekonomi, dan pertahanan dalam membangun legislasi yang dapat dipercaya oleh khalayak atau masyarakat umum.

Kesejahteraan yang terjamin merupakan indikator ekonomi bagi tiap warga dalam suatu negara. Untuk konteks terorisme, negara sebagai subjek keamanan diharapkan mampu mengeliminasi kemungkinan adanya tindak atau aksi terorisme yang berbasis motif ekonomi. Salah satunya dengan menyediakan sumber-sumber daya (pemberian lahan/sawah, lapangan pekerjaan) yang dapat dimanfaatkan oleh mantan narapidana maupun keluarga atau kerabatnya. Melalui hal tersebut, legislasi yang baik terhadap kebijakan dan segala tindakan yang diambil oleh pemerintah akan terbangun.

Dalam menanggulangi terorisme, suatu negara memerlukan usaha yang terintegrasi (*unity of effort*). Usaha ini melibatkan masyarakat sipil, polisi, dan aparat militer. Jika *unity of effort* sebagai wujud mawas diri suatu negara terhadap lingkungannya sendiri, maka kerjasama atau kolaborasi luar negeri adalah wujud mawas diri ke luar bagi negara dan sebagai salah satu elemen penopang keberhasilan dari penanggulangan tersebut. Agar suatu negara berhasil dalam memberantas terorisme, dibutuhkan kerjasama lintas batas negara untuk dapat memfasilitasi proses diseminasi dan pertukaran pengetahuan dalam melakukan diseminasi. Kolaborasi luar negeri juga nantinya akan mendorong terciptanya perjanjian ekstradisi sebagai dasar legislasi dalam menindak teroris dari luar negara yang tertangkap di dalam negeri.

Signifikansi kerjasama dan kolaborasi luar negeri dikonfirmasi oleh teori liberal institusionalisme. Menurut R. Jackson dan G. Sorensen (1999), teori ini berpersepsi bahwa institusi menolong dalam memajukan kerjasama antar negara-negara. (Jackson & Sorensen 2005, 155). Dengan adanya kerjasama atau kolaborasi antar negara, maka badan atau lembaga kerjasama akan memaksimalkan kapabilitas dirinya dengan turut melibatkan partisipasi bersama aktor non-negara dalam suatu sistem; membuat legislasi atau konsensus bersama atas hukum terkait masalah pemberantasan terorisme.

Salah satu prinsip penanggulangan terorisme adalah peningkatan *core value* (nilai pokok). Hal ini berkaitan dengan asas kekeluargaan dalam ketahanan nasional yang mengutamakan prinsip perbedaan dan tanggung jawab bersama. Implementasi aktivitas kerjasama ini contohnya adalah *neighbourhood watch group*. Aktivitas ini melibatkan masyarakat atau warga dalam melakukan tindakan *pre-emptive* seperti pengawasan dan pengamanan secara bersama terhadap potensi kejahatan atau aksi teror di lingkungan sekitar.

Cyberterrorism: Tantangan Komunikasi Asimetris bagi Pembangunan Ketahanan Nasional

Menurut Rod Thornton, peperangan asimetris adalah aksi atau tindak kekerasan yang dilakukan oleh

'si tidak punya' terhadap 'si empunya' dimana 'si tidak punya' yang meliputi aktor negara atau non-negara menerapkan taktik dan strateginya dengan memanfaatkan kerentanan (kelemahan) dari lawannya yang lebih kuat. Disini konteksnya adalah 'si empunya'. Peperangan asimetris melalui jejaring (terutama internet), sesungguhnya merupakan komunikasi asimetris karena bobot utamanya ada pada "media baru yang sangat efisien (bahkan efektif dalam kasus terorisme) dalam penyebarluasan (*diseminasi*) pesan berupa sasus, rumors, hoax, bahkan kebohongan dan fitnah yang dianggap sebagai kelemahan perentah. Dengan demikian, komunikasi asimetris adalah komunikasi peperangan yang dilakukan oleh sempalan/kelompok/oganisasi tertentu terhadap negara (cq.Pemerintah) dengan menggunakan media jejaring terutama internet dengan bahan baku sasus, rumors, hoax, bahkan kebohongan dan fitnah.

Dalam bukunya yang berjudul "*Asymmetric Warfare*", definisi konseptual peperangan asimetris ini muncul dari adanya kasus yang bermula (*entry case*) di Amerika, yaitu serangan pada 11 September terhadap menara *World Trade Center* (*WTC*) (Thornton 2007, 1-2). *Entry case* ini mengarahkan pada pengkategorian terorisme sebagai salah satu bentuk peperangan asimetris.

Terorisme melibatkan pihak 'si tidak punya' atau aktor non-negara dalam melawan 'si empunya' atau pihak otoritas pemerintah dengan mengeksploitasi kelemahan. Beberapa contohnya adalah melakukan upaya serangan-serangan teror dan publisitas untuk menggalang dukungan masyarakat atas tindakannya dalam mencapai tujuan politis (mendorong pemerintah untuk mengubah kebijakan dan mengakomodasi ketidakpuasan mereka terhadap negara). Berdasarkan konsep yang dijabarkan di atas, terorisme merupakan salah satu manifestasi peperangan asimetris.

Pada era kontemporer saat ini, ancaman asimetris tidak hanya berasal dari keberadaan terorisme itu sendiri, tetapi juga dari ruang *cyber* (*cyberspace*). Teknologi digital yang melibatkan *cyberspace* seperti internet memberikan keleluasaan bagi semua pihak termasuk aktor non-negara seperti individu, kelompok atau organisasi terorisme. Internet seringkali digunakan oleh kelompok atau organisasi terorisme sebagai alat (tool) dalam melaksanakan aktivitas terornya (*cyberterrorism*) untuk menggalang dukungan, seperti propaganda dan indoktrinasi. Ruang cyber menjadi suatu media yang dimanfaatkan karena pelaku teror tidak akan segera teridentifikasi saat itu juga oleh 'si empunya' atau aktor negara. Kelemahan tersebut yang pada akhirnya dieksploitasi oleh 'si tidak punya' atau aktor non-negara.

Dorothy Denning (seorang profesor ilmu komputer USA) mendefinisikan *cyberterrorism* di depan Komite Representatif Pelayanan Angkatan Bersenjata pada bulan Mei tahun 2000 sebagai perluasan *cyberspace* dan terorisme. Menurutnya, jika diartikan, *cyberterrorism* merujuk pada serangan dan ancaman atas serangan terhadap komputer, jaringan dan informasi dengan tujuan mengintimidasi, menekan pemerintah dan rakyatnya serta memiliki kepentingan politik atau sosial. Serangan ini memberikan hasil yaitu tindak kekerasan terhadap orang atau properti. Tujuannya adalah menyebabkan ketakutan. Sementara itu, serangan terhadap infrastruktur juga dapat dikatakan aksi terorisme (www.usip.org, hal 4). *Cyberterrorism* memberikan tantangan bagi pemerintah

Indonesia untuk berperan signifikan dalam melawan teroris yang melakukan manuever nya di ruang *cyber*. Aktivitas *cyberterrorism* menjadi pilihan yang menarik bagi teroris dalam mencapai tujuannya, dengan alasan (www.usip.org, hal 6) :

1. Metode ini lebih murah daripada metode tradisional yang biasa dilakukan oleh kelompok atau organisasi teroris. Individu atau kelompok teroris hanya membutuhkan komputer dan sambungan internet. Mereka tidak lagi perlu membeli senjata atau peledak. Justru dengan adanya internet mereka berharap dapat menciptakan virus dan melepaskannya melalui sambungan internet.
2. *Cyberterrorism* dapat menjadi metode atau cara yang lebih rahasia daripada metode konvensional yang biasa digunakan. Individu atau kelompok teroris dapat menggunakan *user name* atau kode identitas yang bukan sebenarnya ketika masuk ke website tertentu. Hal ini dapat memanipulasi aparat keamanan atau polisi untuk mencari identitas teroris yang sebenarnya. Melalui *cyberspace*, pelaku terorisme tidak dibatasi pergerakannya.
3. Jumlah target yang dihasilkan dari aktivitas *cyberterrorism* itu lebih besar. *Cyberterrorist* mampu menarget jaringan komputer milik individu, pemerintah, masyarakat, maskapai swasta, dan sebagainya. Kompleksitas dari pemilihan target atau sasaran-sasaran ini membuat pelaku terorisme dapat menemukan kelemahan yang dapat mereka eksploitasi.
4. Aktivitas *cyberterrorism* dapat dilaksanakan secara berpindah-pindah. *Cyberterrorism* tidak membutuhkan pelatihan fisik dan psikologis. Keberadaannya yang berpindah dari satu tempat ke tempat lain membuatnya lebih leluasa melakukan aksinya seperti merekrut ataupun menggalang dukungan.
5. *Cyberterrorism* selalu dianggap menghasilkan dampak yang lebih besar terhadap orang banyak. Oleh karenanya, metode ini menggalang media yang lebih besar pula dalam rangka publisitas mereka.

Pelaku teror melakukan manuver di ruang *cyber*, yaitu serangan cyber (*cyberattack*) terhadap target yang diinginkannya. Menurut Sieber dan Brunst, *cyberattack* sebagai *cyberterror* menyasar infrastruktur melalui internet dengan virus dan spyware di dalam jaringan komputer. Salah satu contoh kasus serangan oleh virus terhadap jaringan komputer adalah kasus serangan virus I Love You pada tahun 1999 yang dilepas dari Filipina kepada Kementerian Keuangan Romania (Golose 2015, 26). Virus ini disinyalir merubah nilai mata uang Romania dan memberikan dampak yang merugikan bagi Romania saat itu. *Cyberterror* tidak hanya menyerang infrastruktur vital negara, tetapi juga aspek kehidupan manusia dalam bentuk peretasan terhadap jaringan komunikasi, kendali pesawat, dan sebagainya.

Petrus R. Golose pada bukunya yang berjudul "*Invasi Terorisme Ke CyberSpace*" menyebutkan 9 Aktivitas Terorisme (9P) yang dilaksanakan dengan memanfaatkan teknologi informasi atau internet. 9 aktivitas tersebut adalah propaganda, perekrutan, penyediaan logistik, pelatihan, pembentukan paramiliter secara melawan hukum, perencanaan,

pelaksanaan serangan teroris, persembunyian, dan pendanaan. (Golose 2015, 35-38).

A. Bentuk-bentuk Komunikasi, Perencanaan, dan Serangan *Cyberterrorism*

Perencanaan dan pelaksanaan *cyber terorisme* sebenarnya merupakan bentuk komunikasi juga, karena dilaksanakan melalui media (bahkan lokus) komunikasi kontemporer yakni komunikasi jejaring dengan *backbone*-nya internet. Dengan demikian situasi ini penulis kelompokkan ke bentuk-bentuk komunikasi saja.

1) Propaganda

Menurut Thackrah (2004),

"Propaganda can be defined as any information, ideas doctrines or special appeals disseminated to influence the opinion, emotions, attitudes or behavior of any specified group in order to benefit the sponsor either directly or indirectly". (dalam Slide Perkuliahan *Dynamics of Terrorism.*)

Jadi, dapat diartikan bahwa propaganda adalah gagasan atau informasi yang ditujukan untuk mempengaruhi pendapat, tindakan maupun tingkah laku dari kelompok tertentu. Penyampaian propaganda dapat secara langsung atau tidak langsung. Propaganda dilakukan teroris untuk menyampaikan pesan dengan tujuan meyakinkan, mengajak ikut untuk bergabung, atau menyebarkan rasa takut. Target penyampaian pesan itu sendiri seperti pelaku teroris lainnya, target rekrutmen atau kader, dan simpatisan.

Propaganda terorisme banyak ditemukan di berbagai media termasuk internet. Internet menjadi media yang memberikan peluang bagi pelaku atau kelompok terorisme dalam melaksanakan aktivitas propagandanya. Beberapa peluang-peluang tersebut diantaranya adalah:

1. Internet memberi peluang bagi khalayak untuk menerima ideologi radikal. Jangkauan yang luas menjadi keuntungan bagi pelaku, kelompok atau organisasi terorisme
2. Internet mampu mempercepat radikalisasi. Video yang berisi paham radikal dapat secara cepat terakses oleh khalayak melalui *youtube* ataupun website umum.

Internet mendukung khalayak untuk melakukan radikalisasi mandiri. Khalayak akan mampu terpapar paham radikal tanpa harus berinteraksi langsung dengan pelaku utama teror ataupun pelaku radikalisasi (*radicalizer)* nya (Golose 2015, 48-49). Propaganda terorisme yang banyak dilakukan adalah dengan tehnik *propaganda by deed* (propaganda yang dilakukan melalui tindak kekerasan), dehumanisasi bahkan tehnik menyalahi untuk meyakini. Bentuk propaganda terorisme, menurut *United Nations on Drugs and Crime* (2012), diantaranya adalah (dalam Slide Perkuliahan *Dynamic of Terrorism*):

2) Presentasi perspektif

Bentuk propaganda ini adalah dengan menampilkan perspektif atau idealisme pelaku teror ke depan khalayak ramai. Perspektif ini disampaikan sebagai pesan atau wasiat terhadap khalayak yang disebarkan dalam rangka memperkuat kekuatannya dengan cara menciptakan rasa takut (*fear*) dan panik. Hal ini pernah dilakukan oleh Mujahidin Indonesia Timur (suatu jaringan terorisme, populer di Poso) yang pesannya dipublikasikan melalui youtube setelah melakukan aksi bom di Poso.

3) Indoktrinasi

Indoktrinasi dilakukan untuk mencapai keberhasilan kelompok atau organisasi terorisme dalam memprovokasi masyarakat untuk ikut serta atau setidaknya mendukung aksi terorisme yang dilakukan mereka. Indoktrinasi dilaksanakan seiring dengan presentasi perspektif yang dilakukan oleh teroris sebelum atau sesudah melakukan aksi teror di dunia nyata.

4) Radikalisasi

Radikalisasi dipahami mengarah pada proses indoktrinasi. Ketika seseorang telah terpapar oleh ideologi atau paham radikal, maka suatu individu akan lebih mudah diindoktrinasi untuk percaya, yakin, dan mau melakukan tindakan yang sesuai dengan keinginan *radicalizer* nya. Bisa berupa tindakan kekerasan, turut melakukan aksi bom, dan sebagainya.

5) Propaganda Rekrutmen

Rekrutmen adalah capaian yang diinginkan oleh teroris setelah melakukan radikalisasi dan indoktrinasi. Saat ini rekrutmen justru lebih gencar dilakukan melalui internet. Contoh propaganda dalam rangka rekrutmen adalah kasus pengrekrutan calon martir atau bom bunuh diri oleh militan Iran melalui situs *Insight Online Magazine*. Tujuannya yaitu untuk melakukan serangan bom bunuh diri terhadap warga masyarakat Amerika Serikat dan Israel.

6) Rekrutmen

Rekrutmen dilakukan dalam rangka menyebar ideologi dan mencari dukungan atau simpatisan di tengah-tengah khalayak publik. Intensitas pengunjung situs dan informasi online menjadi target bagi teroris dan hal ini dimainkan melalui interaksi dengan calon anggota melalui chat, email, dan sebagainya.

Rekrutmen adalah agenda teroris dalam menggalang dukungan populasi atau masyarakat yang menjadi targetnya. Seperti halnya bentuk propaganda, rekrutmen ditujukan untuk menarik simpatisan dalam bergabung dengan jaringan atau organisasi terorisme nya. Kemudian diharapkan juga kader teroris dapat melakukan pelatihan dan persiapan dengan materi-materi yang disebarluaskan melalui internet.

Metode pengrekrutan dilakukan oleh teroris dengan memanfaatkan internet. Media sosial seperti Facebook digunakan untuk merekrut orang-orang. Salah satu kasus terhangat adalah tahun 2014, dimana seorang saksi diperiksa setelah sebelumnya direkrut dan dikirim ke Suriah. Saksi ini mengaku menjalin pertemanan melalui wall-wall Facebook serta chat Facebook dan diimingi fasilitas untuk berangkat ke Suriah (Golose 2015, 69).

7) Penyediaan Logistik

Jaringan terorisme biasanya menggunakan *cyberspace* sebagai sarana dalam mengakses kebutuhan logistik seperti bahan peledak, senjata, ataupun bom yang dipublikasikan. Biasanya jaringan teroris menggunakan *cyberspace* sebagai *tool* untuk menyusun akomodasi keberangkatan, terutama jika jaringan teroris telah berhasil merekrut calon kadernya melalui media sosial.

8) Pelatihan

Kelompok teroris menggunakan *cyberspace* sebagai media dalam melakukan tujuannya, yaitu pelatihan. Model pelatihan terorisme secara garis besar dapat dikategorikan menjadi dua, yaitu pengunggahan konten melalui e-book, tutorial melalui video, dan blog. Sementara model komunikasi antar calon ataupun mentor kelompok teroris adalah melalui forum dan *instant*

messenger. (Slide Perkuliahan *Dynamic of Terrorism)*

Teroris menggunakan *instant messenger* serta forum-forum untuk mempromosikan materi-materi pelatihan yang dapat diakses oleh khalayak atau netizen. Forum internet biasanya dieksploitasi dan menampilkan link yang bertautan dengan situs paparan materi penelitian.

Selain forum dan melalui *instant messenger*, teroris juga menggunakan blog dan E-book yang dapat diunduh melalui file sharing seperti 4shared dan Hotfile. Kemudian melalui situs video broadcast seperti Youtube, teroris juga bebas mengunggah video yang berisi tutorial pembuatan detonator bom atau rakitan bom untuk keperluan aksi terorisme. (Golose 2015, 161)

Selain itu, teroris menciptakan blog untuk kepentingan penyediaan materi mengenai I'dad. I'dad merupakan persiapan yang dilakukan sebelum melakukan aksi terorisme. Berdasarkan penyidikan kasus-kasus pada tahun 2000, dikatakan bahwa kemampuan teroris atau kelompoknya dalam membuat bom adalah diturunkan oleh mereka yang pernah menjalani perang di Afganistan. Mereka belajar dengan sendirinya dalam merakit bom. Posisi seperti ini cenderung membuat pelaku terorisme dapat berjalan dan bertindak berdasarkan inisiatifnya sendiri walaupun tidak ada komando yang memimpin dan mengarahkannya. (Golose 2015, 124)

Internet selain untuk memberikan bahan pengajaran mengenai pelatihan pembuatan bom juga dimanfaatkan oleh teroris dan jaringannya untuk menampilkan pelatihan pemanfaatan komputer dan internet. Hal ini dimaksudkan untuk membantu proses publikasi dan sabotase pada sejumlah jaringan komputer yang diyakini menghambat mobilisasi mereka dalam menyebar propaganda terorisme. Pemanfaatan internet tersebut dilakukan untuk menyebar materi pelatihan atau tehnik *hacking* dan penggunaan software serta prosedur komunikasi yang sifatnya rahasia (enkripsi, *anonimity*, dan *dead drop*) (dalam Petrus Golose. 2015).

9) Pembentukan Paramiliter Melawan Secara Hukum

Untuk menggalang masyarakat dalam mendukung aksi terorisme, teroris membutuhkan publisitas yang tinggi. Hal ini terkait dengan ajakan atau seruan melalui internet dan media sosial untuk melakukan mobilisasi, penggunaan senjata, dan kebutuhan dalam membentuk kelompok serang (*combat group*).

10) Perencanaan

Dalam melakukan perencanaan kelompok teroris menggunakan teknologi informasi untuk menetapkan strategi, taktik, maupun operasional yang akan diambil dan diterapkan. Perencanaan yang dilakukan oleh pelaku, kelompok, ataupun organisasi terorisme dimulai melalui komunikasi rahasia dan informasi bebas akses. Komunikasi rahasia diantaranya mencakup email, pesan terenskrip, dan chat room. Sedangkan informasi bebas akses seperti peta satelit, informasi pemerintah, agenda transport, dan laporan keamanan. (*Dynamic of Terrorism.*)

Penggunaan aplikasi internet pada hakikatnya merupakan suatu ancaman terkait pemanfaatan informasi untuk kepentingan penyebaran teror oleh kelompok teroris. Salah satu contoh kasusnya adalah penggunaan open source seperti *google earth* dan *google map* oleh milisi di Irak dalam melakukan perencanaan penyerangan. Aplikasi bebas akses ini tergolong murah karena dapat diakses secara

gratis. Melalui gambar satelit milisi Irak mampu mendeteksi mobilisasi tentara Inggris. Hal ini membuat serangan teroris meningkat signifikan terutama tahun 2006 ke 2007 (dalam Golose, 2015: 130):

Tahun Serangan	Jumlah Korban Tewas
2004	22 Tentara Inggris
2005	23 Tentara Inggris
2006	29 Tentara Inggris
2007	41 Tentara Inggris

Di sisi lain, perencanaan juga dapat dilakukan dari percakapan melalui email. Perencanaan melalui email dapat lebih terperinci karena sifatnya personal, sehingga pengaturan eksekusi aksi teror dapat dijabarkan secara bebas. Kemudian, kelompok teroris saat ini juga sudah menggunakan program enkripsi demi mengamankan file yang sifatnya rahasia (*confidential*).

11) Pelaksanaan Serangan

Pelaksanaan atau eksekusi dijalankan oleh kelompok teroris melalui internet sebagai perantara atau medianya. Secara umum, eksekusi memiliki pola:

1. Ancaman kekerasan yang sifatnya nyata serta meliputi penggunaan senjata dalam pelaksanaannya
2. Diseminasi melalui internet yang pada akhirnya memunculkan kegelisahan, ketakutan, dan kepanikan di tengah-tengah masyarakat
3. *Video Call* digunakan sebagai pengawas atau pengendali pelaksanaan aksi yang *real-time* atau *live* [21]

Berdasarkan pola tersebut, dapat dipahami bentuk pemanfaatan internet secara lumrah oleh kelompok teroris. Aksi kekerasan biasanya dilakukan oleh kelompok teroris dan ditunjukkan melalui situs atau *video broadcast*. Penggunaan senjata api juga diperlihatkan seolah hal tersebut dapat membangun rasa cemas dan khawatir bagi khalayak yang menontonnya. Penebaran teror ini dimaksudkan untuk mendapat perhatian dari khalayak tentang eksistensi mereka. Selain itu, memberi peringatan bagi masyarakat bahwa tak lama lagi akan dilakukan aksi terorisme yang sebenarnya.

Sementara aksi terorisme dilakukan terhadap target yang telah ditentukan, monitor dan pengendalian terhadap aksi serangan tersebut melalui *video call* juga dilaksanakan. Rancangan serangan banyak disebarluaskan melalui situs seperti anshar.net. Situs ini menjelaskan dan menjabarkan bagaimana cara melakukan aksi teror hingga urutan lokasi serta peta target yang sudah direncanakan.

12) Persembunyian

Setelah melakukan eksekusi atau pelaksanaan aksi terorisme, dilakukan tahap persembunyian. Tahap ini dimaksudkan untuk mengaburkan identitas individu atau kelompok teroris dari khalayak dan aparat penegak hukum. Adapun tempat dan lingkungan persembunyian bagi kelompok teroris adalah (Golose 2015, 142):

Keluarga

Bagi kelompok teroris, persembunyian yang tepat adalah tempat tinggal kerabat atau sanak saudara. Dengan bersembunyi di kediaman atau rumah keluarga, diharapkan kelompok teroris mampu menyamarkan langkahnya dan membuat anggota keluarga atau sanak saudaranya tersebut mengkamuflasekan tempat persembunyiannya.

Masyarakat atau publik

Bentuk persembunyian lainnya adalah penyusupan di tengah-tengah masyarakat. Salah satu contohnya adalah Noordin M. Top dan Dr. Azahari yang menyamar di Batu, Malang sebelum pada akhirnya meninggal dunia saat penangkapan.

Daerah Terpencil

Pemukiman terpencil menjadi pilihan bagi pelaku atau kelompok terorisme dalam melakukan aktivitas persembunyiannya. Contohnya seperti Nangroe Aceh Darussalam yang dijadikan basis paramiliter tahun 2010. Kemudian, daerah terpencil lain yang didukung dengan konflik kohesi sosial-politiknya adalah Poso.

Poso menjadi salah satu daerah utama bagi aktivitas terorisme jaringan Santoso semenjak intensitas konflik Poso yang sarat dengan SARA semakin meningkat. Suasana yang keruh ini dimanfaatkan teroris untuk berdiam diri dan melakukan persembunyian. Tujuannya untuk mengalihkan perhatian aparat penegak hukum dengan masalah dan kejahatan yang terjadi di sana.

Jika dikaitkan dengan penggunaan internet atau teknologi informasi, persembunyian yang dilakukan oleh pelaku individu atau kelompok terorisme dijalankan dengan menyembunyikan identitas mereka pada saat melakukan *chat*. Kemudian, terdapat tehnik *dead drop* yang membantu mengaburkan identitas mereka dengan menyimpan namun tidak mengirimkan email yang sudah mereka ketik. (Golose 2015, 142)

B. Pendanaan

Pendanaan bagi kepentingan terorisme merupakan satu aktivitas vital mengingat tahap ini memberikan kontribusi penuh atas kelancaran eksekusi atau pelaksanaan aksi terorisme. Pendanaan terorisme menunjang seluruh kebutuhan dalam melakukan aksi terorisme seperti penyediaan logistik, perencanaan, pelatihan, perekrutan, propaganda, pelarian, dan serangan teror.

Pendanaan terorisme dikategorisasikan menjadi 3 bagian (dalam Golose, 2015), yaitu berdasarkan pendana, sumber dana, dan cara memperolehnya. Sumber dana yang merupakan pemasukan bagi pendanaan berasal dari luar negeri dan dalam negeri. Sedangkan pemberi dana berasal dari negara sponsor, kelompok atau organisasi teroris, individu teroris, dan/atau masyarakat. Perolehan dana didapat dengan cara legal maupun ilegal bergantung pada subjek atau pendana tersebut.

Dalam pendanaan terorisme dikenal istilah *terror crime nexus* yang juga harus dipertimbangkan sebagai prioritas utama. Hal ini karena *crime nexus* menjadi salah satu pemicu bagi terciptanya situasi yang kondusif dan kelancaran kelompok atau organisasi terorisme dalam melakukan aktivitas dan aksi terorisme khususnya yang bersifat ilegal. *Terror crime nexus* adalah keterhubungan atau saling melengkapinya organisasi kriminal terorganisir dengan kelompok teroris.

Aksi *terror crime nexus* mencakup hal yang dimanfaatkan oleh kelompok teroris dalam memperluas, mengembangkan jaringannya dari kegiatan vital yaitu pendanaan melalui tindakan kriminal terorganisir, dukungan material dan logistik yang didapatkan melalui kegiatan kriminal transnasional seperti terorisme yang disandarkan pada penyebaran dan penjualan narkoba (*narco-terrorism*), perlindungan dan dukungan yang didapat melalui kegiatan penyelundupan dan lintas batas negara (*organ trafficking, human trafficking, illicit*

weapon smuggling), dan eksploitasi serta kesenjangan penegakan hukum. (dalam Slide Perkuliahan *Dynamic of Terrorism*).

Terorisme dan kejahatan terorganisir sendiri memiliki perbedaan yang signifikan. Kejahatan terorganisir (*organized crime*) dibangun untuk fokus khususnya pada keuntungan ekonomi dan menghasilkan pasar ilegal sebanyak mungkin. Sementara terorisme adalah tindakan yang dimotivasi oleh tujuan ideologis dan oleh hasrat untuk perubahan politik. Dikotomi biner antara kejahatan terorganisir dengan terorisme disatukan dengan kesamaan-kesamaan, yaitu:

1. Keduanya aktor yang rasional
2. Keduanya menggunakan kekerasan dan ancaman
3. Keduanya menggunakan penculikan dan pembunuhan
4. Keduanya beroperasi secara diam diam walaupun pada periode tertentu keduanya terpublikasikan di wilayah yang bersahabat bagi mereka
5. Keduanya membawa ancaman asimetris bagi negara-negara

Kategori *terror crime nexus* didasarkan pada spektrum interaksi tindak kejahatan dan teror (*terror-crime*) (dalam Slide Perkuliahan *Dynamic of Terrorism*) :

1. Kecocokan aktifitas:
2. Dimana mengadopsi metode aktivitas kejahatan yang dilakukan kelompok lain ke dalam kelompok tertentu Misalnya kelompok teroris menjiplak metode kejahatan terorganisir ataupun sebaliknya, organisasi kriminal mengadopsi cara teror demi mengancam pemerintahan. Di sini tidak terdapat hubungan kerjasama antara keduanya.
3. Nexus: dimana kerjasama kelompok teroris dan organisasi kejahatan transnasional itu ada. Kerjasamanya cenderung singkat dan transaksional tidak ada pertukaran ideologi dan bentuk kerjasama bisa berbentuk penyediaan *safe heavens* (bentuk operasional seperti dokumen yang dipalsukan ataupin melarikan diri)
4. Simbiotik: Tahap ini merupakan kelanjutan nexus. Di tahap ini, kedua belah pihak saling menguntungkan dengan membentuk struktur dan prosedur bersama hingga menimbulkan saling ketergantungan.
5. *Hybrid*: yaitu dimana keduanya mencapai puncak kerjasama dan terjadi merger. Dalam kerjasama terdapat pertukaran ideologi dan memiliki agenda politik selain melakukan kejahatan.

Dari kategori di atas dapat dinyatakan bahwa *terror crime nexus* adalah koneksi antara kejahatan terorganisir dan kelompok teroris yang mencakup spektrum interaksi dimana kegiatan yang dilakukan keduanya diindikasikan oleh adanya kerjasama untuk saling menguntungkan maupun memberikan kondisi menguntungkan bagi salah satu pihak demi berjalannya kegiatan kejahatan dan/atau terorisme.

Salah satu kasus pendanaan terorisme melalui pemanfaatan internet yang pernah terjadi di Indonesia adalah kasus peretasan oleh Rizky Gunawan yang berkolaborasi dengan Cahya Fitrianta. Rizky Gunawan adalah salah seorang peretas situs speedline.com. tahun 2010 hingga 2012. Hasil dari peretasan tersebut dikendalikan oleh Cahya Fitrianta dengan cara pencucian uang (*money laundring*). Dana digunakan untuk mendanai pelatihan paramiliter di Poso. (dalam Golose, 2015)

Ada struktur dan prosedur yang diciptakan dari proses peretasan hingga aktivitas pencucian uang. Kedua pihak mengambil keuntungan dalam melakukan pendanaan demi aksi terorisme tersebut sehingga kasus ini dikategorikan ke dalam spektrum interaksi simbiotik. Selain melalui aktivitas ilegal seperti *terror crime nexus*, kelompok atau oganisasi terorisme juga memperoleh dana melalui aktivitas yang legal. Ada beberapa cara yang menjadi kamuflase dan digunakan oleh pelaku atau kelompok teror dalam mendapatkan dana melalui pemanfaatan internet. Menurut UNODC, beberapa di antaranya yaitu:

1. Permintaan donasi
   Melalui internet, *chat*, dan media sosial lain.
2. *E-commerce*
   Melalui fasilitas online, *PayPal*
3. Eksploitasi
   Peretasan terhadap sistem pembayaran dengan *wire fraud* (penipuan melalui keterhubungan jaringan), *auction fraud* (penipuan jual barang online yang tak kunjung datang), dan sebagainya. (dalam Slide Perkuliahan *Dynamic of Terrorism*)

Lalu, bagaimana dengan hambatan dalam melaksanakan penanggulangan *cyberterrorism*?

3. Diskusi

Regulasi Terhadap Aktivitas Pendanaan Terorisme

Penanggulangan terorisme masih sebatas pada UU Pemberantasan Terorisme (UU No. 15 Tahun 2002 Jo. Perpu No.1 Tahun 2002) yang dititikberatkan pada bentuk-bentuk serangan teroris dan regulasi yang lebih menyeluruh terangkum dalam UU No.9 Tahun 2013 tentang aktivitas pendanaan terorisme (Golose 2015, 156). Akan tetapi, Indonesia belum mengimplementasikan pembekuan aset yang membiayai aksi terorisme dan aktivitas-aktivitasnya.

Jika melihat permasalahan tersebut, maka hambatan lain yang akan muncul adalah tidak adanya regulasi atau UU yang mengatur masalah pembekuan aset atau benda yang didapat melalui aktivitas *hacking* dan di *cyberspace*. Permasalahan lain adalah *Foreign Terrorist Fighters* (FTF). FTF adalah warga negara yang berangkat atau pergi dalam rangka bergabung bersama kelompok atau jaringan terorisme di luar wilayah negaranya. Menurut Badan Intelijen Negara (2015), Indonesia belum memiliki hukum atau regulasi yang spesifik mengenai FTF. (BIN, 2015)

Ketika FTF Indonesia didapati mengalami deportasi, tidak ada regulasi yang dikenakan kepadanya sebagai FTF. FTF hanya dikenakan hukuman yang sejajar dengan hukum yang ditegakkan atas tindakan kriminal yang dilakukannya. Misalnya, FTF yang kembali ke Indonesia melakukan pemalsuan identitas pada dokumen atau passport, maka UU mengenai tindakan kriminal tersebut yang dikenakan. Sehubungan hal tersebut, muncul kekhawatiran terhadap aktivitas-aktivitas yang dilakukan oleh FTF melalui *cyberspace*, terutama ketika melakukan aktivitas pengrekrutan dan pemakaian aplikasi bebas akses yang lumrah digunakan oleh khalayak.

Penangkalan Terhadap *CyberAttack*

Indonesia masih dihadapkan pada ancaman *cyberattack* terutama *cyberattack* yang dilakukan untuk kepentingan terorisme. Belum ada sistem yang dapat menangkal serangan

cyber secara holistik ketika konsep keamanan informasi dan teknologi pada sejumlah pelayanan pemerintah terhadap masyarakat diterapkan.

Barang Milik Tahanan

Sejumlah berita di media elektronik (televisi) mengabarkan bahwa beberapa tahanan kriminal masih mengantungi ponsel. Pada hakikatnya, hal ini terdengar sepele. Namun, tidak dapat dipungkiri berbagai alat elektronik memberikan akses terhadap media sosial yang saat ini memunculkan peluang atau potensi radikalisasi pada orang yang terisolasi (baik di rumah maupun di tahanan).

Arus Informasi dan Komunikasi

Akibat arus informasi dan komunikasi yang begitu cepat dan terbukanya akses terhadap internet terdapat dampak mengalirnya konten-konten atau materi radikal di dunia maya. Belum ada sistem terintegrasi dalam mengatur mesin pencari yang mungkin menampilkan link situs radikal dan konten mengarah pada radikalisasi.

Rekomendasi: Penanggulangan *Cyberterrorism*

Cyberterrorism menjadi fokus utama permasalahan yang harus diselesaikan demi membangun ketahanan nasional Indonesia. Pada hakikatnya, aktivitas terorisme yang dilakukan dengan memanfaatkan internet merupakan gejala atau fenomena yang saat ini marak di tengah-tengah masyarakat. Keterbukaan informasi dan akses tanpa batas di dunia digital menawarkan pragmatisme masyarakat untuk mencari uang dalam memenuhi kebutuhan hidupnya.

Kejahatan *cyber* tidak luput dari isu *cyberterrorism*. *Cyberterrorism* memiliki posisi tawar yang baik di kalangan masyarakat kecil. Untuk mendapatkan uang, mereka tidak perlu mengeluarkan modal awal. Cukup dengan melakukan interaksi simbiotik dengan individu atau kelompok terorisme yang menjanjikan uang sebagai balasannya, masyarakat mampu terdoktrin untuk melakukan tindakan pendanaan atau pelancaran aktivitas terorisme.

Ketahanan nasional sebaiknya dibangun dengan *local awareness* yang tinggi untuk memberantas kejahatan *cyber*. Hal yang dapat dilakukan secara tehnis adalah pemberian pelatihan dalam membuka usaha rumahan atau lapangan pekerjaan. Program ini dapat dilaksanakan melalui *cyberspace* yang tujuannya menjadikannya sebagai media kontra kejahatan *cyber* (*cyber crime)* dalam mewujudkan keamanan yang berbasis pada kesejahteraan.

Dalam mewujudkan pembangunan ketahanan nasional, terorisme melalui internet memerlukan pengawasan dan pengendalian (kontrol) dari berbagai elemen. Hal ini bukan hanya tugas pemerintah, Badan Nasional Penanggulangan Terorisme (BNPT), dan Kementerian Komunikasi dan informasi, tetapi juga masyarakat sipil yang bersinggungan atau berinteraksi langsung di *cyberspace*.

Untuk menghindari *auction fraud*, masyarakat harus jeli melihat berbagai kemungkinan yang akan muncul. Ketika melakukan perbelanjaan online, diharapkan masyarakat memberikan pemberitahuan terhadap aparat penegak hukum jika barang yang dipesan belum sampai. Hal ini untuk mengantisipasi kemungkinan pendanaan terorisme melalui internet.

Kembali pada masalah regulasi terhadap FTF Indonesia. Indonesia perlu regulasi yang ajeg dalam menaungi penegakkan hukum terhadap FTF dengan terminologinya sebagai FTF itu sendiri. Sehingga, UU yang dikenakan bukan UU yang menindak

pelaku FTF pada tingkatan kegiatan kejahatan atau kriminalitas sampingan yang dilakukannya. Sementara itu, terkait dengan asas mawas diri ke dalam, pemerintah atau aparat keamanan diharapkan mampu mengintensifikasikan kegiatan pengawasan terhadap tahanan lokal di balik lapas. Sementara itu, diperlukan sistem *cyber* yang holistik untuk dapat mengatasi masalah serangan *cyber* seperti serangan hacking atau peretasan. Pembentukan Dewan Keamanan *Cyber* Nasional juga menjadi salah satu inisiatif yang patut digalakkan.

Hal yang paling fundamental adalah pencegahan penyebaran paham radikal melalui internet. Upaya yang dapat dilakukan adalah mengintensifkan kerjasama dengan lembaga instansi terkait dalam upaya kontra narasi melalui situs. Hal ini ditargetkan untuk melawan arus ideologi yang salah dari situs-situs yang secara konten memuat paham radikal dan menyensor situs dengan muatan gagasan yang mengarah pada tindak kekerasan. Peran serta masyarakat dalam ikut serta menanggulangi masalah *cyberterrorism* sangat penting. Hal ini merupakan perwujudan *core value* dalam menghalau ancaman terhadap aspek astagrata ketahanan nasional. Berdasarkan penjelasan mengenai penanggulangan pememanfaatan internet untuk kepentingan teroris oleh UNODC, rekomendasi yang didapat yaitu diperlukannya pengendalian informasi dan komunikasi dan identifikasi aktivitas internet. (Golose 2015, 183)

1. Pengendalian Informasi dan Komunikasi

Pada dasarnya, menurut UNODC, internet memainkan peran yang efektif sebagai media dalam penyebaran paham radikal atau terorisme. Oleh sebab itu, dibutuhkan sistem kendali terhadap informasi dan komunikasi dengan cara mengawasi akses terhadap infrastruktur jaringan. Selain itu, dibutuhkan pendekatan lebih intensif seperti penyensoran konten internet. Rekomendasi lain adalah kombinasi antara pengawasan infrastruktur jaringan dan penyensoran.

2. Identifikasi Aktivitas Internet

Menurut UNODC, dibutuhkan identifikasi atas aktivitas internet yang mengarah pada peningkatan aksi terorisme. Aktor yang memiliki cukup andil disini adalah pemangku kepentingan pada sektor swasta. Diharapkan pemangku kepentingan pada sektor swasta dapat ikut serta membantu dalam memonitor berbagai macam arus komunikasi, hasutan, ataupun radikalisasi yang mengalir di dunia maya. Hal ini dapat diwujudkan dengan kerjasama masyarakat dan pemegang pengaruh di sektor swasta seperti perusahaan *cyber*, warung internet, dan masyarakat dapat bahu-membahu dalam mengatasi masalah *cyberterrorism* secara komprehensif.

4. Simpulan

Cyberterrorism adalah isu strategis yang saat ini perlu menjadi perhatian. Semua lini sektor, baik swasta maupun pemerintah, harus dapat memandang masalah ini secara menyeluruh karena dampak dari masalah ini berkenaan dengan aspek-aspek astagatra ketahanan nasional Indonesia. Aspek kewilayahan berkaitan dengan terganggunya kedaulatan NKRI oleh ancaman teror dan skala aksi kekerasan. Ideologi yang salah dapat memecah bahkan memberi gagasan bagi suatu kelompok tertentu untuk untuk melakukan pemisahan akibat rasa tidak puas terhadap pemerintah atau kebijakan yang berlaku.

Dari aspek astagrata, isu *cyberterrorism* mengancam keseluruhan

aspek terkait dampak yang dihasilkan. Selain politik, pertahanan keamanan, dan ideologi, isu *cyberterrorism* mengancam ketahanan ekonomi (dampak dari terganggunya infrastruktur jaringan dan komunikasi yang diretas untuk kepentingan terorisme) dan sosial budaya. Asas-asas ketahanan nasional menjadi indikator yang memberi gambaran bagi pembangunan ketahanan melalui penanggulangan *cyberterrorism* yang diperlukan oleh Indonesia.

Daftar Pustaka

Buku

Golose, Petrus. 2015. *Invasi Terorisme Ke Cyberspace*. YPIK, Jakarta.

Hendropriyono, AM. 2009. *Terorisme: Fundamentalis, Kristen, Yahudi, Islam.* Kompas Media Nusantara, Jakarta.

Jackson, Robert & George Sorensen. 2005. *Pengantar Studi Hubungan Internasional*. Pustaka Pelajar; Yogyakarta.

Thornton, Rod. 2007. *Asymmetric Warfare*. Polity Press, UK

Internet

Analisis Keterkaitan Wawasan Nusantara Dengan Ketahanan Nasional www.academia.edu/7049399/ANALISIS_KETERKAITAN_WAWASAN_NUSANTARA_DENGAN_KETAHANAN_NASIONAL. Diakses Pada 14 November 2015. Pukul 12.20 WIB

Jurnal Elektronik. Gabriel Weimann. *"Cyberterrorism: How Real Is The Threat?"* pada United States Institute of Peace: Special Reports. Hal. 4 (www.usip.org)

Pengertian Azas Ketahanan Indonesia Menurut UUD (www.dosenpendidikan.com/pengertian-azas-ketahanan-indonesia-menurut-uud/) Diakses pada 14 November 2015. Pukul 20.19 WIB

Sumber Lain

Informasi dari Badan Intelijen Negara. 2015. Nama Narasumber Sengaja Tidak Disebutkan.

Universitas Pertahanan, 2015. *Dynamic of Terrorism: Cyberterrorism dan Studi Kasus*. Prodi *Asymmetric Warfare*..

Universitas Pertahanan, 2015, *Dynamic of Terrorism: Terror Crime Nexus,* Prodi *Asymmetric Warfare*.