SISTEM PERTAHANAN NKRI DALAM MENGHADAPI ANCAMAN CYBER TERRORISM PADA ERA DIGITALISASI

Muhammad Lutfi Amirullah, Desrian Saputri, Angga P.

Fakultas Hukum, Universitas Diponegoro

lutfiamirullah1@gmail.com

Abstrak

Indonesia saat ini tengah dalam keadaan mendesak cyber security atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau cyber crime di Indonesia sudah mencapai tahap memprihatinkan. Naum berbeda dengan penanganan kejahatan lainya, cyber security membutuhkan pemikiran yang komprehensif untuk menanganinya. Karena itu tulisan ini membahas tentang bagaimana kebijakan cyber security yang telah dijalankan di Indonesia selama ini dan bagaimana prospek dan tantangan bagi pengembangan kebijakan cyber security di Indonesia.

Kata Kunci : kejahatan cyber, keamanan cyber, cyber security, pertahanan Indonesia

Abstract

Indonesia is reportedly a serious cyber security threat due to the fact that the level of cvber crime in the country has reached critical condition. Unlike in coping with other crime, to counter cyber security, a comprehensive solitions should be found out. This paper discusses the way of how cyber security in the country has been handling, how its prospect, and new challenges coming from its development today.

Keywords: cyber, cyber crime, cyber security, defense Indonesia

A. Pendahuluan

Perkembangan era digitalisasi yang semakin masif telah merangsang munculnya berbagai teknologi yang dapat mengakomodasi seluruh kebutuhan dan kegiatan manusia, yang pada mulanya berlangsung secara nyata (fisik) beralih pola menjadi maya (virtual). Bersamaan dengan semakin masifnya aktivitas manusia di dunia maya, ancaman-ancaman kekerasan dan kejahatan pun mulai merambah ke dalam jaringan nirkabel tersebut, satu di antaranya yang ten- gah membuat ceruh banyak negara di dunia adalah kejahatan terorisme siber atau *cyber terrorism*.

Cyber terrorism merupakan bagian dari kejahatan siber (*cyber crime*) yangmempunyai sifat transnasional karena tidak terbatas ruang dan waktu sehinggatidak hanya berdampak negatif pada individu saja, tetapi juga berdampak besarbagi organisasi dan negara serta kepentingan yang dilindungi oleh hukum padalebih dari satu yurisdiksi nasional.[1] Bahkan, pada tahun2002 menurut peneliti Microsoft, mereka memiliki taktik dengan sering kali menghilang begitu saja secara cepat dan mengganti situs mereka dengan alamatyang berbeda lagi dengan tujuan menghindari pengawasan dari pihakpemerintah maupun intelejen tapi konten tetap sama (Seib&Janbek, 2011: 59).[2] Karena teroris dapat secara efektif menggunakan dunia maya untuk komunikasi yang aman. (Bogdanoski et al, 2012: 681-684)[3]

Internet menyediakan papan pesan dan *chat room* untuk *recruitment* parateroris, membeli bom, membeli tiket pesawat, mengkoordinasikan serangan danberkumpul dalam satu tempat tanpa hadir secara fisik (Lumbaca&Gray, 2011:47).[4] Internet tidak lagi digunakan sebatas untuk melakukan kontak atau perencanaan semata, di era digital ini, internet telah ditransformasikan sebagai alat dalam melancarkan serangan. Dengan penggunaan teknologi informasi dan elektronik seperti internet, para teroris sangat mudah berkomunikasi sehingga dapat melancarkan aksi teror mereka. Meskipun terorisme dilakukan melalui dunia maya dengan memanfaatkan teknologi informasi, namun tetap pada dasarnya memiliki motivasi politik dan sosial atas serangan-serangan yang hendak dilakukan terhadap infrastruktur-infrastruktur yang dimiliki oleh negara, seperti keuangan, energi, transportasi, dan operasi pemerintah, sehingga mengakibatkan kematian terhadap orang, rasa takut dalam masyarakat, kelumpuhan ekonomi dalam suatu negara, maupun kelumpuhan infrastruktur negara tersebut (Astuti, 2015; Lubis, 2017).[5]

---

[1] Nur Qalbi., Fitrah Marinda., dan Rina Yulianti. 2020. Asean Against Cyber Terrorism: Upaya Mengatasi Propaganda Hitam sebagai Kejahatan Terorganisir. *Legislatif*, Vol. 4, No. 1, hlm.108

[2] Eska Nia Sarinastiti., & Nabilla Kusuma Vardhani. 2018. *Jurnal Gama Societa, Vol.1, No. 1*, hlm. 43

[3]Andi Widiatno., Tinjauan Yuridis Penanggulangan Tindak Pidana Terrorisme dalam Menyebarkan Propaganda melalui Mefia Sosial.

[4] Op.Cit., Eska Nia Sarinastiti., & Nabilla Kusuma Vardhani., *hlm.42*

[5]Zephirinus Jondong. 2020. Kebijakan Hukum Pidana bagi Tindak Pidana *Cyber Terrorism* dalam Rangka

Pembentukan Hukum Positif di Indonesia., *Jurnal Preverensi Hukum., Vol.1., No. 2, hal.22*

Kasus cyber terrorism pertama di indonesia yang berhasil diungkap oleh Polri adalah kasus BOM Bali yang melibatkan terpidana mati Abdul Aziz alias Imam Samudra pada 2002. Pada kasus ini, pelaku memang melakukan serangan secara nyata (fisik) yang mengakibatkan jatuhnya korban jiwa, kerusakan, dan kehancuran, tapi pelaku juga menggunakan jaringan internet sebagai media provokasi dan propaganda untuk mengintimidasi dan menakuti publik. Selain itu, kasus terbaru yang tengah menggemparkan dunia, termasuk Indonesia, yaitu penyerang yang dikenal dengan nama Ransomware Wannacry telah melakukan penyerangan terhadap rumah sakit-rumah sakit.

Kasus ini menjadi rambu-rambu merah bagi Negara Indonesia yang mensyaratkan bahwa ancaman *cyber terrorism* telah tampak secara nyata dan semakin dekat dengan kehidupan masyarakat. Sebagaimana yang pernah diungkapkan Panglima TNI Marsekal TNI Hadi Tjahjanto, terdapat lima konstelasi global yang berpotensi menjadi ancaman pertahanan dan keamanan nasional sehingga negara Indonesia harus mewaspadainya. Ancaman-ancaman tersebut ialah tatanan dunia baru, terorisme, perang siber, kebangkitan Tiongkok yang menggantikan Amerika Serikat dan kerawanan laut Indonesia.[6]

Berkaca pada pandangan tersebut, dapatlah dipahami bahwa terorisme telahtumbuh menjadi ancaman besar yang harus mendapat respons progresif dari negara. Kendati pada dasarnya Indonesia telah membangun tameng untuk menghadapi masalah di bidang *cybercrime* dan terorisme. berupa pengaturan dalam perundang-undangan, tetapi sejauh mana efektivitas dan capability perundang-undangan tersebut dalam meng-cover penyelesaian masalah cyber terrorism masih menjadi tanda tanya yang harus ditelisik lebih dalam jawabannya. Sebab, Cyber terrorism merupakan konvergensi dari terorisme dan cybercrime. (Denning, dalam Gordon & Ford, 2003:3) yang berarti terdapat dua unsur dalam satu tindak pidana, yakni kejahatan siber dan kejahatan terorisme yang masing-masing diatur dalam peraturan yang berdiri sendiri. Penting pula untuk dingat, cyber terrorism tidak mengenal batas lintas negara, ruang, dan waktu, sehingga berpotensi akan terus berkembang menjadi ancaman mematikan bagi pertahanan dan keamanan negara dengan dampak perusakan yang lebih luas dan lebih masif.

[6] Nur Qalbi, *op.cit.*, hlm. 10

Menilik pada betapa serius dan gentingnya ancaman kejahatan cyber terrorism tersebut, dapatlah dinyatakan bahwa seluruh negara di dunia harus memiliki basis pertahanan siber yang kokoh dengan berorientasi pada teknologi mutakhir guna membendung dan mematahkan serangan-serangan cyber terrorism sebelum mampu mencapai target serangan.

B. Pembahasan

1. Bagaimana Sistem Pertahanan Indonesia dalam *cyber terrorisme*

Sejalan dengan Pembukaan Undang-Undang Dasar 1945, maka Negara Republik Indonesia adalah negara kesatuan yang berdasarkan hukum dan memiliki tugas untuk memelihara kehidupan yang damai serta secara aktif turut serta dalam memelihara perdamaian dunia. Salah satu permasalahan yang sedang ramai dibicarakan di media sosial maupun elektronik adalah ancaman terrorisme. Sebagai negara yang mempunyai kewajiban dalam melindungi harkat dan martabat manusia, Indonesia telah menciptakan peraturan perundang-undangan yang mengatur tentang terorisme. Cyber terrorism adalah bentuk kejahatan baru yang memiliki karakteristik dan bentuk sendiri, cyber terrorism di identifikasikan sebagai serangan terhadap infrastruktur nasional yang kritis atau intimidasi terhadapwarga sipil dan pegawai pemerintah dengan menggunakan jaringan dan teknologi komputer. Cyber terrorism juga di anggap sebagai serangan yang melanggar hukum terhadap jaringan komputer, jaringan informasi yang tersimpan yang bertujuan untuk mengintimidasi pemerintah atau rakyat. Serangan tersebut menghasilkan kekerasan terhadap individu, kelompok. properti pemerintah dan menimbulkan bahaya dan ketakutan. Pengaturan mengenai kejahatan cyber terrorisme belum secara jelas dan tegas diatur dalam Undang-Undang Republik Indonesia No. 5 Tahun 2018 tentang pem- berantasan tindak pidana terorisme dan Undang- Undang No 19 Tahun 2016 tentang informasi dan transaksi elektronik.

Menurut Undang-undang No. 3 tahun 2002 pasal 1 ayat 1 tentang pertahanan negara adalah segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah negara kesatuan republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara. Sistem pertahanan negara Indonesia bersifat sistem pertahanan semesta, yaitu melibatkan seluruh warga negara, wilayah, dan sumber daya

nasional lainya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah, dan keselematan segenap bangsa dari segala ancaman.[7]

Usaha penanggulangan kejahatan melalui hukum pidana merupakan bagian dari usaha penegakan hukum, khususnya bagi penegakan dalam bidang hukum pidana. Sebagaimana telah diuraikan sebelumnya bahwa pembaruan hukum pidana pada hakikatnya adalah suatu upaya untuk melakukan reorientasi dan reformasi hukum pidana yang sesuaidengan nilai sentar sosio-politik, sosio filosofis, sosio kultural masyarakat Indonesia yang melandasi kebijakan criminal dan kebijakan penegakanhukum Indonesia. Namun, sifat melawan hukum untuk tindak pidana cyber terrosime tidak terpenuhi dalam rumusan pasal-pasal UU ITE karena dalamtindak pidana cyber terorisme serangan atau ancaman secara melawan hukum tersebut dilakukan terhadap computer, jaringan computer, dan data yang tersimpan dalam jaringan tersebut, yang memiliki tujuan untuk mengintimidasi atau memaksa pemerintah atau masyarakat untuk tujuan politik atau sosial tertentu. Contoh kasus yang baru ini terjadi di Indonesia adalah Ransomware WannaCry, pada saat itu Ransomware menyerang 2 rumah sakit yang ada di Indonesia Ransomware yang menyerang kedua rumah sakit itu, berjenis malicious software atau malware yang menyerang komputer korban dengan cara mengunci komputer atau mengenkripsi semuadata yang ada ada sehingga tidak bisa diakses kembali dan untuk guna membuka kembali data tersebut, korban harus membayar tebusan dalam bentuk bitcoin, ransonmware pun mengunci semua data.

Serangan yang telah terjadi di rumah sakit tersebut dapat di katakan sebagai tindakan cyber terrorism di karenakan serangan tersebut bersifat ancaman atau teror yang dimana ancaman tersebut telah meresahkan masyarakat luas atau fasilitas tersebut serta mengakibatkan kerusakan atau kehancuran terhadap objek-objek di rumah sakit tersebut seperti dalam contoh komputer-komputer yang ada di rumah sakit tersebut menjadi tidak berfungsi akibat serangan virus ransomware Wannacry tersebut. Cara pelaku melakukan aksinya dengan computer sebagai alat yang digunanakan lalu dengan Teknik memberi virus bersifat malware dimana virus ini dapat menyebar dengan cepat.

[7] Indonesia. Undang-Undang Tentang Pertahanan Negara, UU No. 3 Tahun 2002, LN. 2002, TLN No. 4169

Upaya penanganan dalam kasus ini digunakan pendekatan *cyber*, yanga artinya bahwa melakukan counter cyber terrorism, yang terdiri dari *cyber patrol* (patroli dunia maya) , *cyber attack* (serangan siber), dan *cyber surveillance* (pengawasan siber).

Patroli siber tersebut dilakukan oleh tim pasukan siber yaitu dengan memantau aktivitas atau pergerakan jaringan terorisme lewat dunia maya. Lalu adanya tim *cyber army/cyber troops* (pasukan siber), mereka tiap hari kerjanya 91 hanya membaca website. Dalam memantau laman website, tim tersebut melakukan pelacakan terhadap situs yang menjadi komunikasi para teroris di dunia maya. Kemudian ketangkap suatu nanti ada *chatting room nya*, mereka kemudian chatting room nya diikuti masuk lalu gabungdengan mereka itu di antaranya. Pelacakan itu tersebut juga dapat dilakukan terhadap alat pengiriman pesan seperti whatsapp dan telegram. Teknik teknik *cyber patrol* ini juga sama sebenarnya dengan teknik-teknikdalam dunia nyata ada yang menggunakan *surveillance* (pengawasan)nyata.

Setelah masuk dalam obrolan komunikasi jaringan teroris itu, pihak kepolisian melakukan penyamaran untuk masuk seolah-seolah menjadi bagian kelompok-kelompok teroris dengan menggunakan berbagai akun termasuk ikut chatting dalam komunitas mereka. Sebagian besar terdeteksi tapi mereka juga sebagian besar berusaha menghindari deteksi intelijen dengan menggunakan metode-metode termasuk sistem komunikasi mereka. Setelah kejadian itu upaya demi upaya telah dilakukan untuk memperkuat sistem keamaan, dengan cara mempunyai tim khusus yang dimana tim khusus ini telah melakukan undercover. Serta juga diwajibkan memperbaharui sistem keamanan dalam komputer atau transaksi elektronik lainya begitu pun juga perbaharui anti virus dengan cara membeli prosduk original, dan melakukan back up data yang penting sehingga jika data tersebut telah hilang terkena virus tersebut dapat di kembalikan dengan mudah. Sistem pertahanan Indonesia dalam *cyber terrorisme* masih lumayan lengah, karena kurang nya edukasi dan kesadaran masyarakat dalam menggunakan media. Berbagai upayaditempuh Indonesia untuk mempertahankan kemerdekaannya, salah satunya dengan membangun sistem pertahanan yang kuat. Pembangunan sistem pertahanan yang kuat ditujukan untuk mempertahankan kedaulatan negara, keutuhan NKRI, dan keselamatan segenap bangsa dari ancaman serta gangguan terhadap keutuhan bangsa dan negara. Untuk mempertahankan kedaulatan negara dari ancaman serta gangguan, maka Indonesia menerapkan sistem pertahanan semesta (sishanta).

Dilansir dari laman resmi Kementerian Pertahanan, dijelaskan bahwa sistem pertahanan Indonesia bersifat semesta yang melibatkan seluruh sumber daya nasional yang dipersiapkan secara dini oleh pemerintah. Diselenggarakan secara total, terpadu, terarah, dan berkelanjutan untuk menegakkan kedaulatan negara, menjaga keutuhan.

Wilayah, dan keselamatan segenap bangsa dari segala bentuk ancaman. Upaya mempertahankan kedaulatan negara tidak hanya dilakukan oleh TNI, tetapi juga warga negara. Sebab sistem pertahanan semesta melibatkan seluruh sumber daya nasional. Warga negara merupakan salah satu sumber daya nasional, berarti warga negara ikut terlibat dalam sishanta. Keterlibatan warga negara dalam sishanta tercermin dari implementasi pendidikan bela negara. Pendidikan bela negara dilaksanakan untuk mencetak kader bela negara yang disiapkan menjadi komponen cadangan dan komponen pendukung. Komponen cadangan dan komponen pendukung berfungsi untuk memperbesar dan memperkuat kekuatan dan kemampuan komponen utama. Selain itu, kader bela negara juga berperan menjadi garda terdepan dalam menangkal ancaman non-militer. Jadi, dapat disimpulkan bahwa sistem pertahanan semesta (sishanta) melibatkan semua komponen, tidak hanya TNI tetapi juga warga negara. Semua bersatu-padu untuk mempertahankan kedaulatan dan keutuhan NKRI.

2. Peraturan Perundang-undangan terkait *Cyber Terrorism*

Terrorisme merupakan suatu tindak pidana yang dilakukan untuk menebarkan suatu teror kepada suatu pihak tertentu dengan tujuan tertentu. Dengan semakin berkembangnya zaman, teknologi komunikasi dan informasi juga semakin berkembang. Perkembangan tersebut tentu membawa dampak baik dampak positif maupun dampak negatif. Dampak positif dengan adanya perkembangan teknologi adalah mempermudah diaksesnya suatu informasi secara meluas dalam waktu yang singkat. Disisi lain hal ini tentu dimanfaatkan oleh para teroris untuk mempermudah kegiatan mereka. Hal ini memberikan dampak terkait konsep terorisme yang semula bersifat konvensial menuju kearah modern dengan batasan-batasan yang semakin Sulit untuk ditetapkan sejalan dengan batas-batas cyberspace.

Konsep terkait terorisme akhirnya berubah seiring dengan berkembangya teknologi dan mulai dikenal istilah *cyber terrorism. Cyber terrorism* merupakan konvergensi dari *cyberspace* dan terorisme. Oleh karena itu perlu adanya suatu aturan yang mengatur terkait tindak pidana *cyber terrorism*. Di Indonesia sendiri aturan terkait cyber terrorism masih belum diatur secara

jelas baik pada Kitab Undang-Undang Hukum Pidana (KUHP) ataupun pada Undang-Undang seperti Undang-Undang Nomor 15 tahun 2003 tentang Penetapan Perppu No 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-undang jo. Undang-Undang Nomor 5 tahun 2018 tentang Perubahan atas Undang-Undang Nomor 15 tahun 2003 tentang Penetapan Perppu No 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang serta Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang No- mor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

3. Undang-Undang Pemberantasan Tindak Pidana Terorisme Pengaturan terkait terorisme di Indonesia diatur di UU Nomor 15 tahun 2003 dan UU Nomor 5 tahun 2018.

Yang dimaksud dengan terorisme pada undang-undang ini adalah perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana teror atau rasa takut secara meluas, yang dapat menimbulkan korban yang bersifat massal, dan/atau menimbulkan kerusakan atau kehancuran terhadap objek vital yang strategis, Iingkungan hidup, fasilitas publik, atau fasilitas internasional dengan motif ideologi, politik, atau gangguan keamanan.[8] Pada undang-undang ini tidak terdapat definisi yang jelas terkait *cyber* terrism atau siber terorisme.

Sehingga pemaknaan terkait *cyber terrorism* di Indonesia sendiri masih sangat rancu. *Cyber terrorism* tidak hanya dipandang sebagai penggunaan teknologi informasi sebagai media atau sarana kelompok atau organisasi untuk menyebarkan teror kepada pemerintah dan masyarakat melainkan juga suatu perbuatan meneror terhadap sistem komputer, jaringan ataupun informasi yang tersimpan di komputer. Pada ajaran hukum pidana, suatu perbuatan dapat dianggap telah melanggar hukum dan dapat dikenakan sanksi pidana apabila memenuhi 2 unsur yaitu unsur perbuatan (actus reus) dan unsur sikap batin pelaku (mens rea).

[8] Indonesia, Undang-Undang Pemberantasan Tindak Pidana Terorisme, UU No. 5 tahun 2018, LN No. 92 Tahun 2018, TLN No. 6216, Ps. 1

Unsur *actus reus* adalah esensi dari kejahatan itu sendiri atau perbuatan yang dilakukan, sedangkan unsur mens rea adalah sikap batin pelaku pada saat melakukan perbuatan.[9] Pada tindak pidana *cyber terrorism* berkaitan dengan unsur mensrea menitikberatkan pada kemampuan bertanggungjawab pelaku, kesalahan dalam dirinya serta tidak adanya alasan pemaaf bagi pelaku dalam melakukan tindak pidana *cyber terrorism* tersebut. Pelaku mengetahui bahwa perbuatan yang hendak diperbuatnya adalah yang mengubah, menambah mengurangi, melakukan transmisi, merusak, menghilangkan, serta memindahkan, dan menyembunyikan dengan cara apapun suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik sebagai perbuatan yang tercela.[10] Dalam *cyber terrorism* harus terdapat unsur melawan hukum dalam perbuatan yang dilakukan pelaku dan hal tersebut haruslah diatur dalam suatu undang-undang. Perbuatan *cyber terrorism* merupakan serangan atau ancaman secara melawan hukum terhadap komputer, jaringan komputer, dan data yang tersimpan dalam jaringan tersebut, yang memiliki tujuan untuk mengintimidasi atau memaksa pemerintah atau masyarakat untuk tujuan politik atau sosial tertentu.[11] Perbuatan sebagaimana dijelaskan diatas tidaklah secara jelas memenuhi rumusan delik sebagaimana diatur pada UU Nomor 15 tahun 2003 jo. UU Nomor 5 tahun 2018 sehingga dalam perbuatan tersebut, pelaku tindak pidana *cyber terrorism* dapat dinyatakan bebas karena tidak terdapat unsur melawan hukum pada perbuatan pelaku yang dirumuskan dalam suatu undang-undang.

4. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Karakteristik dalam tindak pidana cyber terrorism, sebagaimana telah dijelaskan diatas, adalah tindakan teror terhadap sistem komputer, jaringan, dan atau basis dan informasi yang tersimpan dalam komputer dan cyber terrorism sebagai penggunaan internet oleh para teroris untuk keperluan organisasi dan media teror kepada pemerintah dan masyarakat. Terkait karakteristik yang pertama yaitu tindakan teror terhadap sistem komputer, jaringan, dan/atau basis dan informasi yang tersimpan dalam komputer dapat dianalisis melalui perbuatan-perbuatan yang dilarang menurut UU ITE sebagai berikut:

[9] M. Hafidz Habibie, 2017, "Analisis Yuridis *Mens Rea* (Sikap Batin Jahat) dalam Tindak Pidana Korupsi yang Dapat Merugikan keuangan Negara," Skripsi Universitas Negeri Semarang, Semarang, hlm. 14.
[10] Jondong, Zephirinus. 2020. *Op.Cit*. Hlm. 23
[11] Jondong, Zephirinus I*bid*. Hlm 24

a) Pasal 30 UU ITE mengatur tentang tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun. Konstruksi perbuatan dalam rumusan pasal ini menjelaskan bahwa tindakan tidak sah/illegal yang dilakukan oleh seseorang terhadap sistem elektronik milik orang lain dengan tujuan untuk memproleh infor- masi/dokumen elektronik dan/atau upaya pembobolan, penerobosan, dan penjebolan yang melanggar dan melampaui sistem pengamanan.

b) Pasal 32 dan Pasal 33 UU ITE yang mengatur tentang perlindungan terhadap suatu informasi dan/atau dokumen elektronik baik milik orang lain atau milik publik yang bersifat rahasia. Pasal 30, Pasal 32, dan Pasal 33 UU ITE pada dasarnya ditargetkan untuk mempidana pelaku terorisme cyber.25 Namun dalam hal ini terdapat ker- ancuan dalam membedakan suatu perbuatan termasuk kedalam suatu cyber crime atau cyber terrorism. The U.S. Department of Justice mem- berikan pengertian computer crime yaitu an illegal act requiring knowledge of computer technology for its perpetation, investigation, or prosecution. Atau jika diterjemahkan yaitu suatu tindakan ilegal yang membutuhkan pengetahuan teknologi komputer untuk perbuatan jahatnya, investigasi, atau penuntutan.[12]

Cyber crime sebagaimana dijelas- kan diatas secara garis besar merupakan suatu perbuatan tindak pidana menggunakan teknologi komputer, dalam hal ini cyber crime tidak mempermasalahkan terkait alasan atau motif pelaku dalam melakukan tindak pidana tersebut, berbeda dengan cyber terrorism yang memiliki tujuan terkait politik atau ideologis. Relevansi Pasal 30, Pasal 32, dan Pasal 33 UU ITE dengan per- buatan tindak pidana cyber terrorism adalah bentuk perbuatan akses tidak sah atau gangguan terhadap data komputer, informasi/ dokumen elektronik milik orang lain atau milik publik yang dilakukan dengan cara pembobolan, penerobosan, dan penjebolan yang melanggar, melampaui sistem pengamanan, dan sebagainya yang memenuhi unsur cara-cara melakukan teror dalam tindak pidana *cyber terrorism*.

[11] Alfira Nurliliani Samad, 2014, "Analisis Instrumen *Cyber-Terrorism* dalam Kerangka SistimHukum Internasional," Skripsi Universitas Hasanuddin, Makassar, hlm. 19

C. Penutup

1. Sistem pertahanan negara Indonesia bersifat sistem pertahanan semesta, yaitu melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah, dan keselamatan segenap bangsa dari segala ancaman. Upaya pertahanan yang dilakukan dalam menghadapi cyber terrorism adalah counter cyber terrorism, yang terdiri dari cyber patrol (patroli dunia maya) dan cyber surveillance (pengawasan siber) yang dilakukan oleh lembaga kepolisian negara. Patroli siber tersebut dilakukan oleh tim pasukan siber yaitu dengan memantau aktivitas atau pergerakan jaringan terorisme lewat dunia maya.

2. Sampai dengan saat ini, sistem pertahanan Indonesia belum diperkuat dengan peraturan perundangan-undangan atau pun aturan khusus yang secara spesifik mengatur tentang penanganan cyber terrorism. Landasan danacuan yang digunakan negara dalam penanganan cyber terrorism masih bertumpu pada UU Nomor 15 tahun 2003 dan UU Nomor 5 tahun 2018 tentang pemberantasan tindak pidana terorisme, di mana terorisme yang dimaksud pada undang-undang ini adalah perbuatan yang menggunakan kekerasan atau ancaman kekerasan untuk menimbulkan suasana teror atau rasa takut secara meluas, yang dapat menimbulkan korban yang bersifat massal, dan/atau menimbulkan kerusakan atau kehancuran terhadap objek vital yang strategis, Iingkungan hidup, fasilitas publik, atau fasilitas internasional dengan motif ideologi, politik, atau gangguan keamanan. Pengejawantahan undang-undang terorisme tersebut tidaklah tepat dan sesuai jika digunakan sebagai tameng hukum dalam menopang dan memperkuat sistem pertahanan negara Indonesia dalam menghadapi ancaman cyber terrorism, yang notabenenya menyerang sistem komputer, jaringan, dan/ atau basis dan informasi yang tersimpan dalam komputer.

D. Daftar Pustaka

Habibie, Muhammad Hafidz. 2017. "Analisis Yuridis *Mens Rea* (Sikap Batin Jahat)dalam Tindak Pidana Korupsi yang dapat Merugikan Keuangan Negara." Skripsi Sarjana Universitas Negeri Semarang, Semarang.

Indonesia. Undang-Undang Informasi dan Transaksi Elektronik, UU No 19 tahun 2016, LN No. 251 Tahun 2016, TLN No. 5952

Indonesia. Undang-Undang Pemberantasan Tindak Pidana Terorisme, UU No 5tahun 2018, LN No. 92 Tahun 2018, TLN No. 6216.

Jondong, Zephirinus. 2020. Kebijakan Tindak Pidana bagi Tindak Pidana Cyber Terrorism dalam Rangka Pembentukan Hukum Positif di Indonesia. Preferensi Hukum, 1(2).

Qolbi Nur, Fitrah Marinda., dan Rina Yulianti. 2020. Asean Against Cyber Terrorism: Upaya Mengatasi Propaganda Hitam sebagai Kejahatan Terorganisir. *Legislatif,* Vol. 4, No. 1

Samad, Alfiani Nurliliani. 2014. "Analisis Instrumen *Cyber-Terrorism* dalam Kerangka Sistem Hukum Internasional." Skripsi Sarjana Universitas Hasanuddin, Makassar.

Sarinastiti, Eska Nia dan Nabilla Kusuma Vardhani. 2018. *Jurnal Gema Societa*. Vol. 1. No.1.

Widiatno, Andi.Tinjauan Yuridis Penanggulangan Tindak Pidana Terorisme dalam Menyebarkan Propaganda melalui Media Sosial.