TINDAK PIDANA SIBER DENGAN MODUS DISTRIBUTED DENIAL OF SERVICE ATTACK FOR BITCOIN DALAM PENGATURAN HUKUM DI INDONESIA

Rizka Cahaya Putri, Lushiana Primasari

NIM. E0013356

Email : rizkaputri68@gmail.com

Fakultas Hukum Universitas Sebelas Maret

Abstrak

Perkembangan teknologi telah mempengaruhi kehidupan manusia, salah satunya yakni internet. Internet merupakan salah satu kemajuan dalam bidang teknologi yang sangat melekat dengan kehidupan sehari-hari manusia. Melalui internet, manusia dapat dengan mudah melakukan mengakses informasi, komunikasi , transaksi jual-beli dan lain sebagainya. Hal tersebut tentu saja memberikan dampat positif, akan tetapi karena manusia yang tidak dapat memanfaatkan internet sebagaimana mestinya, maka internet dapat memberikan dampak negatif terhadap kehidupan manusia. Dampak negatif tersebut dapat dilihat dengan adanya kejahatan dunia maya atau kejahatan siber (*cyber crime*). Kejahatan siber yang menarik perhatian penulis untuk dibahas yakni *Distributed Denial of Service Attack For Bitcoin* atau yang dikenal dengan *Ddos4Bc*.

Pengaturan hukum yang dapat dikaitkan dengan tindak pidana siber *Ddos4Bc* yakni, Kitab Undang-undang Hukum Pidana (KUHP), Undang-undang No 19 Tahun 2016 perubahan atas Undang-undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dan Undang-undang No 8 Tahun 2010 Tentang Tindak Pidana Pencucian Uang. Namun pengaturan hukum yang berlaku di Indonesia, dirasa belum memiliki pengaturan yang tegas mengenai permasalahan *Ddos4bc* khususnya kejahatan siber yang menggunakan virus *Ddos*. Selain itu, *cyber security* di Indonesia membutuhkan lebih banyak sumber daya manusia yang mengerti mengenai teknologi.

Kata Kunci : Tindak Pidana Siber, Ddos, Bitcoin,

Abstract

The development of technology has influenced human life, one of them is internet. The Internet is one of the most technological advances inherent in human life. Through the internet, humans can easily access information, communications, buy-sell transactions and so forth. It certainly gives a positive impact, but because humans who can not use the internet as it should, then the internet can have a negative impact on human life. Negative impact can be seen with the existence of cyber crime or cyber crime (cyber crime). Cyber crime that attracted the author to discuss the Distributed Denial of Service Attack For Bitcoin or known as Ddos4Bc.

Legal arrangements that can be linked to the Cyber DDos4Bc crime, the Criminal Code (KUHP), Law No. 19 of 2016 amendment to Law No. 11 of 2008 on Information and Electronic Transactions, and Law No. 8 Year 2010 About Money Laundering Crime. However, the legal arrangements in Indonesia are considered to have no strict regulation

on Ddos4bc issues, especially Cyber crimes using Ddos virus. In addition, cyber security in Indonesia requires more human resources who understand about technology.
Keywords: Criminal Crime, Ddos, Bitcoin

A. Pendahuluan

Perkembangan teknologi komunikasi dan informasi telah menyebabkan dunia menjadi tanpa batas. Salah satu fenomena yang sampai saat ini masih terus berkembang dengan pesat adalah internet. Internet memegang peranan penting dalam segalah aspek kehidupan manusia. Tidak dapat dipungkiri, dengan kemajuan tersebut tentu saja dapat memberikan dampak yang positif bagi masyarakat, akan tetapi meskipun suatu kemajuan memberikan sisi positif, sisi negatif akan muncul. Permasalahan akan muncul jika masyarakat tidak dapat memanfaatkan internet sebagaimana mestinya, maka akan menjadi sarana perbuatan melawan hukum sehingga muncul istilah kejahatan internet.

Internet selain dapat memberikan dampat positif maupun negatif, dapat menimbulkan kerugian materiil dan immateriil. Kerugian materiil contohnya seperti penipuan, kehilangan uang ratusan juta karena mendapatkan spam email yang berisikan hal fiktif contohnya seperti korban mendapatkan email bahwa memenangkan undian mobil dan sebelum menerima hadiahnya korban diharuskan untuk mentransfer sejumlah uang ke rekening pelaku untuk keperluan administrasi dan pajak, sedangakan kerugian immateriil seperti pencemaran nama baik dan sebagainya. Hal tersebut tentunya dilakukan oleh oknum atau kelompok sindikat kejahatan yang tidak bertanggung jawab, yang ingin mengambil keuntungan dari masyarakat. Sejak tahun 2014 muncul tindak kejahatan dengan modus baru yaitu *Distributed Denial Of Service Attack For Bitcoin* atau *Ddos4Bc*. http://www.bbc.com/news/tec hnology-34205258

Distributed Denial Of service attack for Bitcoin atau yang di kenal dengan istilah *Ddos4Bc* adalah sebuah nama kelompok. Sebenarnya Ddos4Bc berawal dari Ddos, hanya saja kegiatan kelompok *DD0s4Bc* ini didukung dengan adanya sarana transaksi elektronik yaitu Bitcoin yang akan digunakan untuk transaksi uang hasil dari pemerasan yang dilakukan Ddos4Bc kepada korban, oleh sebab itu dinamakan dengan Ddos4BC. Perbedaan dari Ddos dan Ddos4Bc terletak pada target atau korban, jika Ddos biasanya menargetkan suatu situs atau website game online, sedangkan

Ddos4Bc menargetkan situs atau website milik perusahaan-perusahaan besar seperit jasa keuangan, sektor teknologi, dan lain sebagainya.

Kelompok *DD0s4Bc* dalam menjalankan aksinya, yaitu biasanya kelompok ini mengirimkan email terlebih dahulu ke target mereka. Isi dari email tersebut, berupa bentuk pemerasan apabila mereka tidak mengikuti keinginan dari kelompok tersebut, barulah mereka akan menyerang target dengan serangan *Ddos*. Serangan yang diberikan kelompok ini awal mulanya berupa serangan kecil, jika target tidak juga mengikuti perintah mereka yang menginginkan sejumlah uang dalam bentuk *Bitcoin*, maka mereka akan meningkatkan serangan dengan skala yang besar, tentu saja tebusan *Bitcoin* pun ikut naik.

Mengingat persoalan yang dihadapi tidak sesederhana penanganan kejahatan biasa, karena kejahatan siber dalam melakukan aksinya dapat dikatakan sederhana yaitu bisa dilakukan dimana saja dan tidak membutuhkan banyak sarana penunjang, meskipun dalam kejahatan ini jarang menimbulkan korban jiwa akan tetapi yang paling sering dirasakan korban ialah kerugian financial yang cukup besar, maka perlu menjadi perhatian khusus. Hal ini juga tidak lepas dari peranan hukum khususnya yang berkaitan dengan fungsi hukum pidana. Sehingga dalam melakukan analisis terhadap kejahatan siber dengan modus *Distributed Denial Of Service Attack (Ddos4Bc),* akan berpedoman terhadap Kitab Undang-Undangan Hukum Pidana, Undang-Undang No 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, dan Undang-Undang No 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Mengingat bahwa, *Distributed Denial Of Service Attack* merupakan salah satu jenis kejahatan siber dan Bitcoin merupakan mata uang digital yang dapat menimbulkan tindak pencucian uang karena sistem keamanan yang tidak ketat dan pengguna tidak diharuskan menggunakan identitas, sehingga memberikan peluang bagi pengguna untuk menggunakan identitas palsu.

B. Metode Penelitian

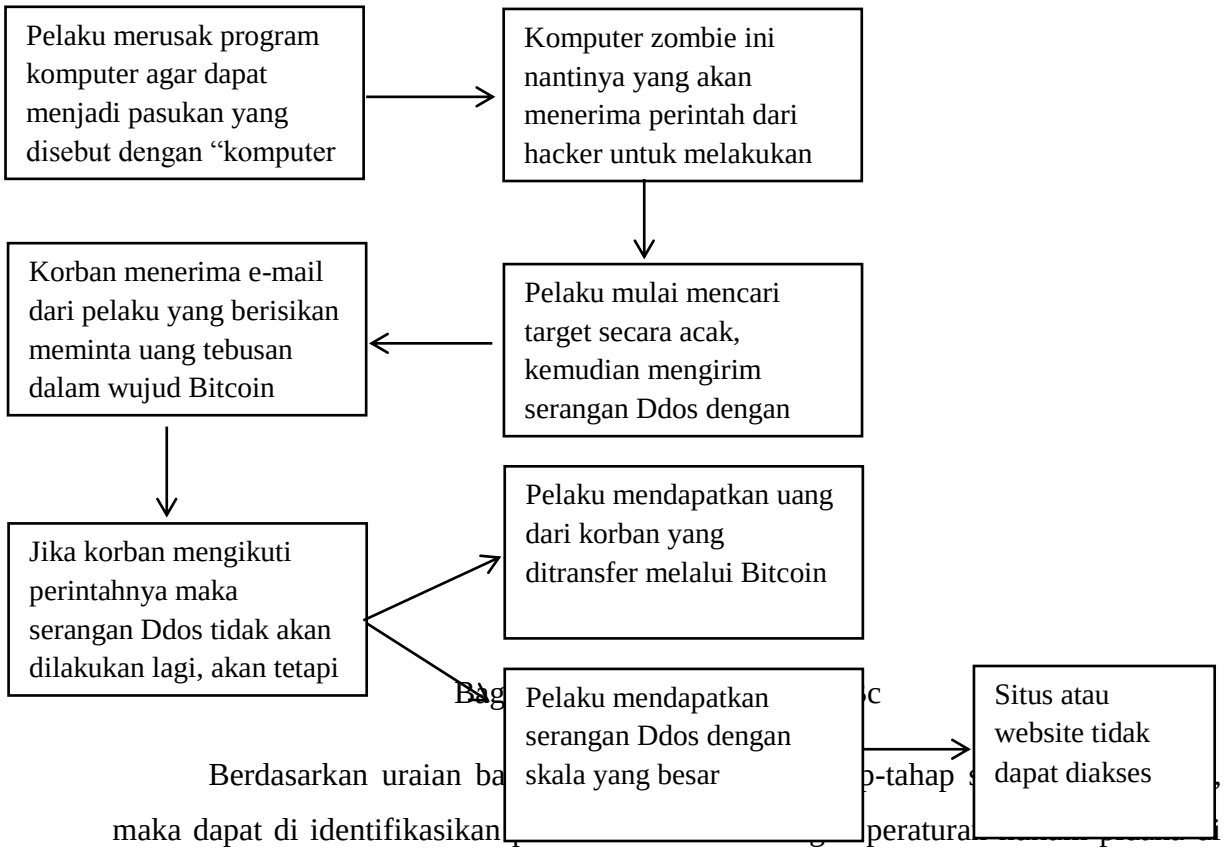
Dalam penulisan karya ilmiah ini penulis menggunakan jenis penelitian hukum normatif, dengan menggunakan pendekatan undang-undang (*statute approach*) dalam mendekskripsikan secara objektif mengenai peraturan dan pertanggungjawaban pidana terhadap tindak pidana siber *Distributed Denial of Service Attack for Bitcoin (Ddos4Bc)*. Pendekatan penelitian dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum

yang sedang ditangani (Peter Mahmud Marzuki, 2011: 93). Sumber data yang digunakan dalam penelitian hukum ini sumber data sekunder, yaitu Kitab Undang-undang Hukum Pidana (KUHP), Undang-undang No 19 Tahun 2016 perubahan atas Undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-undang No 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

C. Hasil Penelitian dan Pembahasan

1. Pengaturan Hukum dalam tindak pidana siber dengan modus Distributed Denial Of Service Attack For Bitcoin dalam sistem hukum pidana di Indonesia

Tindakan Siber *Ddos4Bc* merupakan kejahatan yang sarana utamanya menggunakan komputer dan jaringan internet. Setelah itu, penyerang akan melangsungkan aksinya dengan mengirim serangan *Ddos* ke situs atau website yang menjadi target dan mengirim e-mail yang berisikan ancaman atau pemerasan sejumlah uang yang ditransfer melalui Bitcoin. Berikut alur serangan *Ddos*:



Bag c

Berdasarkan uraian ba p-tahap s , maka dapat di identifikasikan peratura Indoensia sebagai berikut:

1. Kitab Undang-undang Hukum Pidana
   a) Terkait dengan menerobos sistem keamanan komputer milik orang lain secara paksa dapat dikaitkan dengan Pasal 167 ayat (1) KUHP yang berbunyi : "(1) Barangsiapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup yang dipakai orang lain dengan melawan hukum atau berada disitu dengan melawan hukum dan atas permintaan yang berhak atau suruhannya tidak pergi dengan segera, diancam dengan pidana penjara paling lama Sembilan bulan atau pidana denda paling banyak Rp 4.500,00
   b) Terkait melakukan pemerasan atau pengancaman yang bertujuan untuk mendapatkan sejumlah uang tebusan, dapat dikaitkan dengan Pasal 368 KUHP yang berbunyi: Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang lain dengan kekerasan atau ancaman kekerasan, untuk memberikan sesuatu barang, yang seluruhnya atau sebagian adalah milik orang lain, atau supaya memberikan hutang maupun menghapus piutang, diancam, karena pemerasan, dengan pidana penjara paling lama 9 tahun."
   c) Terkait dengan melakukan serangan *Ddos* dalam skala rendah mengakibatkan situs/website tidak dapat diakses atau digunakan sebagaimana mestinya, dapat dikaitkan dengan Pasal 406 KUHP yang berbunyi : " Barang siapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau, sebagian milik orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah."
   d) Terkait pada tahap akhir yaitu menerima uang tebusan melalui sarana Bitcoin yang bersifat anonim, dapat dikaitkan dengan Pasal 480 KUHP yang berbunyi : (1) Barangsiapa membeli, menyewa, menukar, menerima gadai, menerima hadiah, atau untuk menarik keuntungan, menjual, menyewakan, menukarkan, menggadaikan, mengangkut, menyimpan atau menyembunyikan sesuatu benda, yang diketahui atau sepatutnya harus diduga bahwa diperoleh dari kejahatan penadahan; (2) Barangsiapa menarik keuntungan dari hasil sesuatu benda, yang diketahuinya atau sepatutnya harus diduga bahwa diperoleh dari kejahatan.
2. Undang-undang No 19 Tahun 2016 Perubahan atas Undang-undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

a) Terkait dengan sengaja masuk kedalam komputer atau sistem milik orang lain dengan cara apapun, di atur dalam ketentuan Pasal 30 ayat (1) UU ITE yang menyatakan bahwa: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun".
b) Terkait dengan berbagai cara yang dilakukan kelompok *Ddos4Bc* agar dapat merusak sistem keamanan komputer milik orang lain, dapat dikaitkan dengan Pasal 30 ayat (3) UU ITE yang menyatakan bahwa: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."
c) Terkait dengan tujuan serangan yang dilakukan kelompok *Ddos4Bc* agar mendapatkan sejumlah uang dengan cara mengancam atau memeras, dapat dikaitkan dengan Pasal 27 ayat (4) UU ITE yang menyatakan bahwa : "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.
d) Melumpuhkan situs milik korban adalah tujuan dari kelompok *DdoS4Bc,* serangan tersebut akan dilakukan apabila korban tidak mengikuti perintah dari kelompok tersebut. Akibat dari serangan tersebut, korban akan mengalami kerugian financial karena situs miliknya tidak akan bisa digunakan lagi seperti sediakala dan pelanggan situspun tidak dapat mengakses lagi. Hal tersebut jika dikaitkan dalam UU ITE dapat dikenai tindak pidana sengaja melakuka tindakan yang mengakibatka terganggunya sistem elektronik secara melawan hukum yang diatur dalam Pasal 33 UU ITE yang menyatakan bahwa: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya."

3. Undang-Undang No 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang

a) Terkait dengan tindakan kelompok *Ddos4Bc* yang mengancam atau memeras sejumlah uang tebusan dan di transfer melalui Bitcoin agar tidak diketahui identitas pelaku, karena *Bitcoin* yang bersifat anonim, hal tersebut dapat dikaitka dengan Pasal 3 yang berbunyi : Setiap orang yang mentransfer, mengalihkan, membelanjakan, membayarkan, menghibahkan, menitipkan, membawa ke luar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga atau perbuatan lain atas harta kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam pasal 2 ayat (1) dengan tujuan menyembunyikan atau menyamarkan asal usul harta kekayaan dipidana karena tindak pidana pencucian uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Rp 10.000.000.000,oo (sepuluh miliar rupiah).

b) Terkait kelompok *Ddos4Bc* yang menggunakan *Bitcoin* sebagai sarana oendukung untuk melakukan tindak kejahatan , dapat dikaitkan dengan Pasal 4 yang berbunyi : Setiap orang yang menyembunyikan atau menyamarkan asal usul, sumber, lokasi, peruntukan, pengalihan hak, atau kepemilikan yang sebenarnya atas harta kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam pasal 2 ayat (1) dipidana karena tindak pidana pencucian uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Rp 5.000.000.000,oo (lima miliar rupiah).

Berbagai peraturan di atas dirasa masih belum cukup untuk menjawab persoalan kejahatan *Ddos4Bc*. Hukum Indonesia masih belum dapat memberikan kepastian hukum terhadap kasus seperti *Ddos4Bc* ini, di dalam UU ITE mungkin dalam kejahatan *Ddos4Bc* dapat menggunakan Pasal 33 UU ITE, akan tetapi pasal tersebut masih implisit atau tersirat atau tidak menyatakan secara terang-terangan. Pasal 33 UU ITE tidak bisa dijadikan acuan secara terus menerus dalam kejahatan siber khususnya mengenai virus, seiring dengan perkembangannya jaman pasti tindak kejahatan akan menjadi lebih canggih. Oleh sebab itu, Indonesia memerlukan suatu pedoman hukum yang pasti, contohnya seperti yang sudah dilakukan oleh negara Inggris dan Canada dengan mengeluarkan Undang-undang Anti *Ddos.*

1. Pertanggungjawaban Tindak Pidana Siber *Distributed Denial of Service AttackFor Bitcoin* dalam Sistem Hukum Pidana

Setiap kejahatan belum tentu dapat dipertanggungjawabkan, maka dari itu harus dilihat terlebih dahulu apakah kejahatan tersebut memenuhi unsur-unsur sehingga dapat dipertanggungjawabkan atau tidak, contohnya seperti kejahatan *Ddos4Bc* ini. Pertanggungjawaban pidana akan dikenakan kepada seseorang apabila tindakan tersebut melawan hukum. Unsur-unsur pertanggungjawaban pidana yaitu mampu bertanggungjawab, kesalahan dan tidak ada alasan pemaaf, berikut penjelasan mengenai pertanggungajawaban:

a. Mampu Bertanggung Jawab

Seseorang dapat mempertanggungjawabkan atas tindakannya, apabila tindakan tersebut melawan hukum (dan tidak ada peniadaan sifat melawan hukum atau *rechtsvaardigingsgrond* atau alasan pembenar) untuk itu. Selain itu, seseorang dapat dikatakam mampu bertanggung jawab (*toerekeningsvatbaar)* jika mencakup:

1) Keadaan jiwanya:
   a) Tidak terganggu dengan penyakit terus-menerus atau sementara.
   b) Tidak cacat dalam pertumbuhan (gagu,idiot,dan sebagainya), dan
   c) Tidak terganggu karena terejut, hypnotisme, amarah yang meluap, melindur, pengaruh bawah sadar, dan lain sebagainya. Dengan kata lain dia dalam keadaan sadar.
2) Kemampuan jiwanya:
   a) Dapat menginsyafi hakekat dari tindakannya.
   b) Dapat menentukan kehendaknya atas tindakan tersebut, apakah akan dilaksanakan atau tidak, dan
   c) Dapat mengetahui ketercelaan dari tindakan tersebut (Kanter E.Y dan S.R. Siantuti, 2002: 249-250).

Kelompok *Ddos4Bc* mampu bertanggung jawab apabila keadaan dan kemampuan jiwanya seperti yang dikatakan sebelumnya, yakni dalam keadaan sadar dan mengetahui akibat dari tindakan yang dilakukannya. Akan tetapi jika di analogikan, seseorang dalam melakukan serangan *Ddos4Bc* harus mengerti bagaimana cara menginfeksi komputer lain untuk menjadi komputer zombie yang akan menjalankan perintah untuk melakukan serangan *Ddos* ke komputer target. Hal tersebut tentu tidak semua orang dapat melakukannya, sehingga hanya orang yang mempunyai kemampuan khusus untuk melakukannya.

b. Kesalahan

Suatu tindakan dapat dikatakan sebagai kesalahan, apabila dilakukan dengan sengaja atau karena kelalaian yang dapat menimbulkan suatu keadaan atau akibat yang dilarang oleh hukum pidana dan dilakukan dengan mampu bertanggungjawab. Menurut Satochid Kartanegara mengartikan kesalahan sebagai berikut:

" Hubungan antara jiwa seseorang, yaitu yang melakukan perbuatan dengan perbuatannya, atau hubungan jiwa si pembuat dengan akibat perbuatannya, dan hubungan jiwa itu adalah sedemikian rupa, hingga perbuatan itu akibat dari perbuatan yang dilakukannya itu berdasarkan jiwa si pelaku, dapat dipersalahkan kepadanya. Jadi disini keadaan psychis dari si pelaku sedemikian rupa hingga perbuatan itu dapat dipertanggung jawabkan kepadanya."

Kesalahan dan kelalaian seseorang dapat dipertanggungjawabkan apabila tindakan tersebut memuat 4 (empat) unsur, yaitu:

1) Melakukan perbuatan pidana (sifat melawan hukum).
2) Diatas umur tertentu mampu bertanggung jawab.
3) Mempunyai suatu bentuk kesalahan yang berupa kesengajaan (*dolus)* dan kealpaan/kelalaian (*culpa).*
4) Tidak adanya alasan pemaaf (Moeljatno, 2002:164).

Menurut ketentuan yang diatur dalam hukum pidana bentuk-bentuk kesalahan terdiri dari:

1) Kesengajaan (opzet)

   Kesengajaan merupakan unsur yang paling banyak ditemukan dalam tindak pidana. Seseorang mendapatkan hukuman pidana, karena sengaja telah melakukan suatu perbuatan yang dilarang. Contohnya seperti tindak pidana siber *Ddos4Bc* ini, kelompok tersebut sengaja menyebar *virus Ddos* ke situs/web milik target sehingga dengan begitu kelompok *Ddos4Bc* dapat meminta uang tebusan kepada target. Kemudian, kesengajaan juga harus mengenai ketiga unsur tidak pidana, yaitu:

   a) Perbuataan yang dilarang.
   b) Akibat yang menjadi pokok-alasan diadakan larangan itu, dan
   c) Bahwa perbuatan itu melanggar hukum.

Selain dilihat dari keadaan dan kemampuan jiwanya, kelompok *Ddos4Bc* dapat mempertanggungjawabkan perbuatannya jika tindakannya merupakan suatu kesalahan. Hal tersebut dapat dilihat dari tindakan kelompok *Ddos4Bc* yang termasuk dalam perbuatan pidana atau melawan hukum, dengan melakukan serangan *Ddos* sehingga situs milik orang lain tidak dapat digunakan, melakukan pemerasan merupakan bagian dari perbuatan pidana. Kemudian yang dilakukan kelompok *Ddos4Bc* termasuk dalam bentuk kesengajaan seperti yang sudah dijelaskan pada uraian sebelumnya.

2) Kealpaan (*Culpa)*

Kealpaan adalah bentuk kesalahan yang disebabkan kurangnya sikap hati-hati karena kurang melihat kedepan, kealpaan ini sendiri di pandang lebih ringan daripada kesengajaan. Kealpaan terdiri atas 2 (dua) bentuk, yakni:

a) kealpaan dengan kesadaran (bewuste schuld/culpa lata). Dalam hal ini, si pelaku telah membayangkan atau menduga akan timbulnya suatu akibat, tetapi walaupun ia berusaha untuk mencegah, nyatanya timbul juga akibat tersebut.

b) kealpaan tanpa kesadaran (onbewuste schuld/culpa levis) Dalam hal ini, si pelaku tidak membayang atau menduga akan timbulnya suatu akibat yang dilarang atau diancam hukuman oleh undang-undang, sedangkan ia seharusnya memperhitungkan akan timbulnya suatu akibat (Leden Marpaung, 2012: 18)

Unsur-unsur dari kealpaan itu sendiri, yaitu:

1) Pelaku berbuat lain dari apa yang seharusnya diperbuat menurut hukum tertulis maupun tidak tertulis, sehingga sebenarnya ia telah melakukan suatu perbuatan (termasuk tidak berbuat) yang melawan hukum.
2) Pelaku telah berlaku kurang hati-hati, ceroboh, dan kurang berpikir panjang, dan
3) Perbuatan pelaku itu dapat dicela, oleh karenanya pelaku harus bertanggung jawab atas akibat dari perbuatannya tersebut.

Berdasarkan uraian di atas mengenai kelalaian, tindakan kelompok *Ddos4Bc* tidak termasuk dalam unsur kelalaian. Hal tersebut didasari dengan

proses-proses serangan *Ddos4Bc* yang terarah, sedangkan jika perbuatan *Ddos4Bc* merupakan suatu kelalaian maka tidak akan ada tindakan pemerasan atau pengancaman serta sarana Bitcoin untuk menyembunyikan asal usul uang yang di dapat oleh kelompok *Ddos4Bc*

c. Tidak Ada Alasan Pemaaf

Suatu alasan yang menghapuskan kesalahan seseorang meskipun tindakannya tetap melawan hukum, tetapi tidak dipidana karena tidak terdapat suatu kesalahan. Contohnya seperti pengroyokan seorang pencuri oleh masyarakat atau sekumpulan orang, maka orang-orang yang mengroyok tidak dapat dihukum, kemudian si pencuri juga mempunyai hak untuk membela diri dari pengroyokan tersebut dengan cara melukai salah satu pengroyok tersebut, sehingga si pencuri tidak dapat dikenakan hukuman atas tuduhan penganiayaan Pasal 351 KUHP.

Menurut Ruslan Saleh mengatakan bahwa, tiada terdapat "alasan pemaaf" yaitu kemampuan bertanggugjawab, bentuk kehendak dengan sengaja atau alpa, tiada terhapus kesalahannya atau tiada terdapat alasan pemaaf, adalah termasuk dalam pengertian kesalahan *(schuld).* Sedangkan menurut Martiman Prodjhamidjojo mengatakan bahwa unsur subjektif adalah adanya suatu kesalaha dalam bentuk kesengajaan dan kealpaan, sehingga perubuatan yang melawan hukum tersebut dapat di pertanggungjawabkan. Unsur-unsur subjektif yaitu:

1) Kesalahan
2) Kesengajaan
3) Kealpaan
4) Perbuatan, dan
5) Sifat melawan hukum (Kanter E.Y dan S.R. Sianturi, 2002: 25).

Berdasarkan uraian yang dipaparkan diatas mengenai pertanggungajawaban pidana seseorang, maka dapat dikatakan bahwa kelompok *Ddos4Bc* mampu bertanggungjawab atas perbuatannya apabila memenuhi ketiga syarat berikut ini, yaitu:

1) Pelaku mempunyai kemampuan bertanggungjawab (schuldfahigkeit atau zurechnungsfahigkeit), yang berarti keadaan jiwa pelaku harus normal.
2) Adanya hubungan batin antara sipelaku dengan perbuatannya, dalam hal ini yang berupa kesengajaan (*dolus*) atau kealpaan (*culpa*), disebut bentuk-bentuk kesalahan.

3) tidak adanya alasan yang menghapus kesalahan atau tidak ada alasan pemaaf meskipun apa yang disebut dalam a dan b ada, ada kemungkinan bahwa ada keadaan yang mempengaruhi sipelaku sehingga kesalahannya hapus, misalnya dengan adanya kelampauan batas pembelaan terpaksa.

Jika dilihat dari awal kelompok *DD0s4Bc* sudah mempunyai niat untuk melakukan serangan kepada target, hal tersebut dapat dilihat dari kelompok *Ddos4Bc* yang memilih target secara acak kemudian melakukan serangan Ddos dengan skala yang kecil. Selain adanya suatu niat, kelompok *Ddos4Bc* sengaja melakukan serangan tersebut agar situs milik target tidak dapat diakses sehingga pada saat kelompok ini mengirimkan email berupa pemerasan, maka target secara terpaksa akan mentransfer uang tebusan melalui *bitcoin*, karena apabila tidak dilakukan kelompok *Ddos4Bc* akan melakukan serangan dengan skala yang lebih besar. Dapat dilihat bahwa tindakan kelompok *Ddos4Bc* sangat terarah, dari cara pertama mereka yang melakukan serangan ke situs target, kemudian mengirim email pemerasan dan melakukan transaksi dengan sarana *bitcoin.*

Perbuatan yang dilakukan kelompok *Ddos4Bc,* ia menghendaki dan sadar bahwa perbuatannya akan menjadi suatu kesalahan dengan sengaja melakukan tindakan yang berakibat hukum. Sehingga tidak ada alasan pembenar maupun pemaaf bagi kelompok *Ddos4Bc,* karena dilihat dari contoh kasus yang ada maupun proses-proses penyerangan bahwa perbuatan kelompok *Ddos4Bc* ini merupakan perbuatdilihat dari contoh kasus yang ada maupun proses-proses penyerangan bahwa perbuatan kelompok *Ddos4Bc* ini merupakan perbuatdilihat dari contoh kasus yang ada maupun proses-proses penyerangan bahwa perbuatan kelompok *Ddos4Bc* ini merupakan perbuatdilihat dari contoh kasus yang ada maupun proses-proses penyerangan bahwa perbuatan kelompok *Ddos4Bc* ini merupakan perbuatdilihat dari contoh kasus yang ada maupun proses-proses penyerangan bahwa perbuatan kelompok *Ddos4Bc* ini merupakan perbuatan yang murni dilakukan dengan sengaja untuk mendapatkan keuntungan dari perbuatannya, tidak adanya suatu perbuatan yang ditujukan untuk pembelaan diri sendiri.

Bila suatu perbuatan dan yang melakukan dapat dipertanggungjawabkan, maka berlakunya sanksi pidana. Penulis akan menjabarkan bagaimana sanksi hukum Indonesia terhadap tindak pidana siber *Ddos4Bc* ini, apakah hukum Indonesia sudah memenuhi kebutuhan masyarakat dalam kejahatan siber yang terus berkembang.

Dalam hukum di Indonesia dapat menggunakan Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang khusus sebagai pedoman untuk menjatuhkan sanksi

terhadap seseorang yang melakukan kejahatan. Seperti yang sudah di jelaskan pada permasalahan sebelumnya, terdapat beberapa Pasal dalam KUHP yang berkaitan dengan *Ddos4Bc*, akan tetapi di dalam KUHP tidak dikatakan secara tegas bahwa pasal tersebut ditujukan untuk *Ddos4Bc* . Pasal-pasal dalam KUHP yang berkaitan dengan Ddos4Bc yakni Pasal 167 ayat (1), (2), dan (3) mengenai memasuki rumah orang tanpa izin dan dilakukan dengan cara apapun, sama halnya dengan kasus DDOs4bc yang memasuki sistem komputer milik orang lain tanpa izin dan memaksa masuk dengan cara menerobos password komputer. Kemudian terdapat beberapa Pasal lainnya seperti Pasal 368, 406 dan 480 KUHP.

Pada saat ini untuk kejahatan siber dan pencucian uang di atur dalam Undang-undang No 19 Tahun 2016 perubahan atas Undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-undang No 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, maka dari itu peraturan dalam KUHP dapat dikesampingkan dan menerapkan peraturan khusus sesuai yang di atur dalam Pasal 63 ayat (2) KUHP yang menyatakan bahwa: "Jika suatu perbuatan masuk dalam suatu aturan pidana yang umum, diatur pula dalam aturan pidana yang khusus, maka hanya yang khusus itulah yang diterapkan." Bunyi Pasal 63 ayat (2) KUHP inilah yang juga dikenal dalam ilmu hukum sebagai *asas lex specialis derogat legi generali*s, yaitu aturan hukum yang lebih khusus mengesampingkan aturan hukum yang lebih umum.

Selain dari sudut pandang unsur-unsur pertanggungjawaban, dari segi sanksi hukum pelaku Ddos4Bc mendapatkan sanksi yang cukup berat, yang dimana terkait pasal-pasal sudah dijelaskan pada pembahasan sebelumnya. Ketentuan dalam KUHP, Undang-undang ITE maupun Undang-undang TPPU dapat diidentifikasikan bahwa pelaku tindak pidana atau yang dapat dimintakan pertanggungjawaban pidana adalah individu atau orang per orang dan korporasi. Hal tersebut terbukti dari ketentuan pasal-pasal yang diawali dengan kata "Setiap orang..." dan "korporasi..".

Bagi kejahatan siber, upaya yang harus dilakukan tidak hanya memperbaharui peraturan hukum akan tetapi dari sisi pertahanan atau keamanan IT atau yang dikenal dengan cyber security juga diperlukan karena kejahatan siber sarana utamanya yakni menggunakan jaringan internet. Sehingga harus dilihat juga apakah cyber security di Indonesia cukup baik dalam menjaga keamanan internet di Indonesia atau tidak. Berikut beberapa penyedia jasa cyber security yang terbaik, sehingga dapat memberikan pandangan bagi negara Indonesia yaitu:

a. ***Root9B***

Root9B Technologies Company adalah konsultan keamanan cyber dan perusahaan dukungan operasional yang berkantor pusat di Colorado.Selain itu juga memiliki kantor regional di San Antonio, Texas, New York City, dan Charlotte serta ditambah staf lokal diluar AS dan daerah internasional lainnya.

b. ***RSA***

RSA didirikan pada tahun 1982 dan sekarang menjadi divisi dari EMC Corp, perusahaan ini merupakan pelopor keamanan informasi. Lebih dari 30.000 pelanggan menggunakan produk RSA untuk sistem keamanan pemerintahan, resiko dan kepatuhan (GRC), identitas dan manajemen akses (IAM), pencegahan penipuan, dan kerangka cybersecurity.

c. ***IBMSecurity***

IBM Security tercatat telah menghasilkan $ 2 milyar pada pendapatan untuk tahun 2015 dan mengalami pengkatan sebesar 12 persen dibanding tahun sebelumnya. *IBM Security* ini diselenggarakan empat tahun lalu dan memberikan portofolio layanan yang paling komprehensif dan produk yang mencakup operasi keamanan dan intelijen, *cloud, mobile, IAM*, jaringan, endpoint, *mainframe*, aplikasi, keamanan data, dan perlindungan penipuan.

d. ***DellSecureWorks***

SecureWorks didirikan pada tahun 1999 dan diakuisisi oleh Dell pada tahun 2011, SecureWorks merupakan penggerak awal yang membantu mendefinisikan layanan keamanan.Fokus tunggal SecureWorks adalah pada outsourcing cloud dan managed security services. Saat ini perusahaan tersebut telah menyediakan layanan kepada lebih dari 4.100 klien di 61 negara.

e. ***PaloAltoNetworks***

Palo Alto Networks telah membangun bisnis yang mendekati $ 1 miliar dalam pendapatan tahunan pada kekuatan produk dan jasa terkait dan terus berkembang secara pesat.Saat ini perusahaan tersebut telah memiliki lebih dari 28.000 pelanggan lebih dari 160 negara yang mengandalkan Palo Alto firewall dan solusi keamanan jaringan untuk melindungi terhadap bahaya ancaman cyber.

Pertahanan cyber merupakan salah satu hal penting saat ini. Hal tersebut dapat dijadikan langkah agar keamanan jaringan internet di Indonesia kuat, sehingga tidak mudah untuk diserang dengan para hacker. Langkah yang sangat penting dalam menangani kejahatan siber yakni peraturan hukum yang harus diperbaharui dan cyber security yang harus dikembangkan , jangan sampai kedua langkah tersebut sama-sama lemah sehingga dapat memberikan peluang besar bagi pelaku kejahatan siber.

Upaya lainnya yang dapat dilakukan negara Indonesia, yakni dengan melakukan pendekatan untuk menanggulangi penggunaan internet, berikut berbagai macam pendekatan yang dapat dilakukan yaitu:

a. *The constitutional approach, this approach makes the constitution of the country the prime determinant of what is 'acceptable' on the Internet. Classically this has come to be the USA's approach as efforts to enact relevant legislation have fallen foul of the constitution, in particular the First Amendment on freedom of expression. For more information on this conflict between Congressional legislation and the American constitution.*
b. *The state control approach, this approach is adopted by governments which believe that they have a right - and even a responsibility - to intervene directly and place technical controls on the content that can be accessed by their citizens. A classic case is Saudi Arabia where all of the country's Internet service providers have to go through a central node where the Saudi authorities block access to sites hosting pornography, those believed to cause religious offence, and web sites containing information on bomb-making. In China, all Internet cafes are required to keep records of sites visited, with the aim of preventing access to sites featuring pornography, gambling and those that "harm national unification, sovereignty and teritorial integrity". Prior to an important congress of the Chinese Communist Party in November 2002, the authorities even blocked all access to the Google search engine for a time. Other countries where the state is endeavouring to limit access to the Internet by its citizens include Algeria, Yemen, Bahrain, United Arab Emirates, North Korea, Vietnam, Iran, the Maldives and Singapore.*
c. *The statutory approach, this approach makes a specific piece of new legislation the prime determinant of what is 'acceptable' on the Internet. Classically this is*

the approach in Australia where the Broadcasting Services Amendment (Online Services) Act 1999 regulates online content. This Act requires Australian Internet service providers to prohibit access to or remove from their web sites material rated X or RC. The Act came into force in January 2000.

d. *The self-regulation approach, this approach rests on voluntary initiatives by the Internet service provider (ISP) industry. Classically this is the approach in Britain where there is no written constitution and government has shown no wish to legislate. Instead in 1996, the ISP industry established the Internet Watch Foundation which operates a 'notice and take down' procedure.*

e. *Rating and filtering techniques, finally, as well as or instead of any of the previously-mentioned approaches, Internet users – perhaps most especially parents and teachers – can use filtering software which – alone or in conjunction with the self-rating of sites – can limit access by particular users to particular parts of the Internet. Roger* Darlington, *Should The Internet be Regulated* ?, http://www.rogerdarlington.co.uk/regulation.html

Berdasarkan uraian yang sudah dipaparkan diatas, mengenai peraturan, pertanggungjawaban dan upaya penanggulangan secara singkat dapat ditarik kesimpula bahwa peraturan hukum di Indonesia mengenai kejahatan Ddos4Bc masih kurang tegas atau mengatur secara implisit, diperlukan suatu peraturan hukum yang tegas menyatakan bahwa Ddos4Bc merupakan suatu kejahatan yang dilarang. Selain itu dari segi pertahanan juga Indonesia dapat mengikuti cara-cara dari berbagai negara dalam menangani penggunaan internet di negara, karena kejahatan siber sarana utamanya yakni menggunakan jaringan internet.

D. Simpulan

Pengaturan hukum pidana di Indonesia belum dapat mengatur secara tegas mengenai tindak pidana siber Distributed Denial Of Service Attack For Bitcoin. Hal tersebut dapat dilihat di dalam peraturan Kitab Undang-undang Hukum Pidana (KUHP) pasal 167, pasal 368, pasal 406, dan pasal 480, selanjutnya dalam Undang-undang No 19 tahun 2016 pasal 27, pasal 30, dan pasal 33, serta Undang-undang No 8 tahun 2010 pasal 3 dan pasal 4. Pengaturan hukum pidana yang berlaku hanya menyatakan secara implisit mengenai tindak pidana siber Ddos4Bc, sehingga peraturan-peraturan tersebut tidak bisa dijadikan pedoman

secara terus menerus mengingat bahwa suatu kejahatan pasti akan selalu berkembang dengan modus dan sarana teknologi yang lebih canggih.

Selain peraturan hukum mengenai kejahatan siber, suatu peraturan untuk mencegah kejahatan siber juga sangat diperlukan yang disebut dengan cyber security. Cyber security sangat di butuhkan guna untuk mengontrol dan mengawasi kejahatan siber yang terus berkembang. Kemudian, regulasi mengenai penggunaan internet juga diperlukan seperti menggunakan identitas asli pada saat ingin menggunakan internet dari salah satu provider, dengan begitu akan mempermudah penegak hukum dalam menangani tindak pidana siber. Di indonesia, pengguna internet masih bebas untuk menggunakan identitas palsu maupun asli.

Selanjutnya, pertanggungjawaban pidana terhadap seseorang yang melakukan tindakan pidana siber Ddos4Bc, dapat dijatuhkan apabila orang tersebut sudah memenuhi unsur-unsur pertanggungjawaban pidana yakni adanya unsur kesengajaan, melawan hukum serta kapasitasnya sebagai orang perorangan atau sebagai korporasi dengan sanksi pidana penjara dan/atau denda.

E. Saran

1. Pemerintah Indonesia harus dapat mengikuti perkembangan kejahatan siber yang terus berkembang dan semakin canggih dalam sarananya. Pengaturan di Indonesia juga harus diperbaharui khususnya mengenai kejahatan virus, selain itu pemerintah Indonesia juga dapat memberikan payung hukum untuk *Bitcoin* mengingat sifatnya yang anonim dapat memberikan peluang untuk sarana kejahatan.
2. Pemerintah Indonesia harus bekerjasama dengan Internet Service Provider (ISP) atau menekankan kepada ISP untuk memblokir situs-situs seperti situs porno, politik dan agama
3. Pemerintah harus membuat regulasi mengenai pengguna internet, seperti menggunakan identitas asli sehingga dapat mempermudah penegak hukum untuk menindak pelaku kejahatan dengan menggunakan internet.
4. Setiap perusahaan memiliki konsultan keamanan IT, hal tersebut dilakukan agar dapat memberitahu kelemahan keamanan perusahaan dan dapat memberikan evaluasi untuk meningkatkan infrastruktur keamanan.

F. Daftar Pustaka

Kanter E.Y dan S.R. Sianturi. 2002, *Azas-azas Hukum Pidana di Indonesia & Penerapannya.* Jakarta: Storia Grafika.

Leden Marpaung. 2010, *Asas Teori Praktik Hukum Pidana*. Jakarta: Sinar Grafika

Moeljatno. 2002, *Asas- asas Hukum Pidana di Indomesia*. Jakarat: PT. Rineka Cipta

http://www.bbc.com/news/tec hnology-34205258

http://www.rogerdarlington.co.uk/regulation.html