

# BAB I

## Pendahuluan

### 1.1 Latar Belakang

Internet merupakan sarana pertukaran informasi yang sangat luas. Informasi apapun bisa diakses kapan saja dengan mudah dan cepat. Dalam perkembangannya, internet sudah mulai menjadi salah satu kebutuhan hidup bagi masyarakat modern. Banyak layanan yang mulanya hanya dapat diperoleh di kehidupan nyata yang mulai bermunculan di internet dengan proses yang lebih mudah dan singkat. Sebagai contoh adalah adanya transaksi belanja dan *online banking* di mana terjadi perpindahan dana di dalam internet dalam bentuk uang virtual (Filipkowski, 2008). Dengan adanya layanan ini, masyarakat dapat bertransaksi lintas negara dengan lebih mudah dan cepat. Dengan adanya transaksi ini dan adanya aliran dana di internet, ekonomi dapat berkembang dengan cepat.

Namun di sisi lain, ada pihak-pihak yang berniat untuk menggunakan kemudahan-kemudahan yang tersedia di internet ini untuk melakukan tindakan-tindakan ilegal. Terutama pihak-pihak yang berusaha untuk menyamarkan dan melegalkan dana atau uang ilegal yang mereka miliki dengan proses *money laundering*. Penyalahgunaan internet untuk upaya pencucian uang oleh pihak-pihak tersebut merupakan sebuah ancaman yang potensial bagi keamanan ekonomi internasional (Solicitor General Canada, 1998). Tindakan ini dikenal dengan istilah *cyber laundering*.

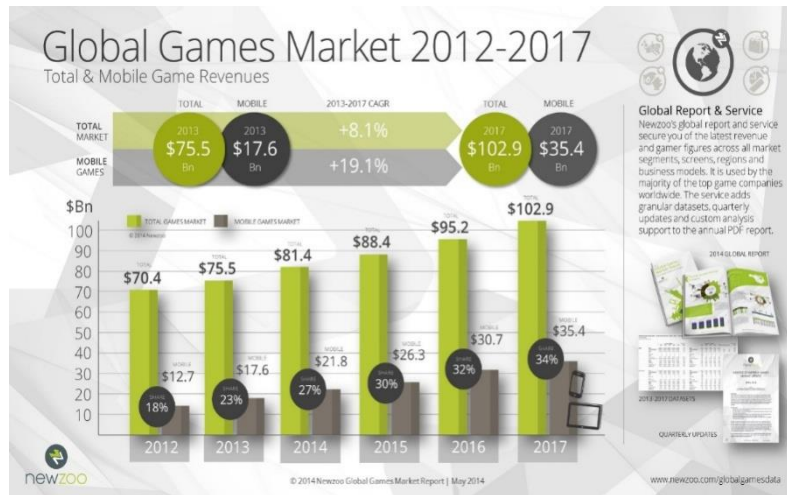
*Cyber laundering* memanfaatkan layanan-layanan dan media-media finansial *online* yang tersedia di dalam internet yang menggunakan uang virtual. Pencucian uang melalui internet dipercaya merupakan sebuah teknik terbaru dan termutakhir dalam metode pencucian uang (Levi dan Reuter, 2006). Dengan *cyber laundering*, proses pencucian uang menjadi lebih cepat. Meskipun demikian, dengan keadaan internet yang masih belum dipenuhi dengan aturan hukum, menambah kemungkinan akan banyaknya pelaku yang berpindah dari pencucian uang secara konvensional menuju ke *cyber laundering* dapat semakin meningkat sebagai akibat dari anonimitas yang ada, tidak adanya kontak fisik, kecepatan transaksi dan jangkauan yang lebih luas di dalam layanan internet. (Filipkowski, 2008).

Salah satu media yang menggunakan layanan finansial di internet yang dijadikan sebagai sarana *cyber laundering* adalah *online games*. Media permainan ini menyediakan layanan berbayar secara virtual bagi jutaan pemainnya yang berasal dari berbagai negara. Dengan jumlah pemain tersebut, para pencuci uang dapat dengan mudah membuka banyak akun palsu untuk bertransaksi, misalnya dengan menjual uang virtual yang mereka beli dengan uang ilegal kemudian dijual kembali kepada para pemain melalui transaksi *online* agar uang tersebut menjadi legal (Richet, 2013).

Salah satu contoh dari *online games*, yaitu *Second Life* dari *Linden Lab*, bahkan memiliki mata uang sendiri yang dapat dikonversikan menjadi uang nyata. Di samping itu, permainan ini juga memberikan pemainnya hak milik dan properti atas apa yang dimiliki mereka secara virtual, memberikan

nilai jual pada barang-barang di dalam permainan tersebut. Sebagai contoh, jika seseorang memiliki rumah di dalam permainan tersebut, maka pemain tersebut memiliki hak atas rumah tersebut sebagaimana seseorang memiliki hak atas rumah di dunia nyata. Pemain dapat menjual rumah tersebut kepada pemain lain dan dapat pula menggunakan mata uang nyata yang dikonversikan menjadi mata uang yang berlaku di dalam permainan. Berkembangnya pasar bebas yang ada di dalam permainan ini dan kebijakan *Linden Lab* yang mengikatkan akun pemain dengan akun bank (Irwin dan Slay, 2010), selanjutnya dapat menjadi salah satu celah yang dapat disalahgunakan untuk *cyber laundering*.

Sejalan dengan adanya fakta tersebut, dengan terus berkembangnya pasar *online games*, kemungkinan ancaman *cyber laundering* menjadi semakin besar. Hampir setiap tahunnya, pasar *online games* selalu meningkat jumlah profitnya (Versace, 2014; Newzoo, *Global Games Market Will Reach \$102.9 Billion in 2017*, 2014; Newzoo, *Global Report: US And China Take Half Of \$113 Bn Games Market in 2018*, 2015).



**Gambar 1.1: Grafik perkiraan perkembangan penjualan games termasuk online games tahun 2012-2017. Newzoo, 2014.**

Peningkatan tersebut dapat menjadi ladang pencucian uang yang besar dan luas jika dibiarkan begitu saja dan akan mengakibatkan banyaknya aliran dana ilegal melalui internet, yang kemudian bisa saja digunakan untuk tindak ilegal lainnya, tidak hanya sekedar untuk dicuci.

Meskipun demikian, sejauh ini pengawasan terhadap transaksi uang masih berfokus kepada pencucian uang secara tradisional. Badan-badan intelejensi keuangan di berbagai negara, termasuk Indonesia, lebih giat dalam mengawasi pencucian uang secara tradisional tersebut. Dalam hal pengawasan transaksi uang di dalam internet, badan-badan intelejensi keuangan tersebut hanya sekedar mengetahui mengenai bahwa terdapat transaksi uang melalui internet, tetapi belum memutuskan untuk memberikan pengawasan pada transaksi tersebut, terutama pada bidang *e-commerce*. Padahal, transaksi ini sama saja dengan transaksi non-internet dan memiliki potensi untuk digunakan sebagai sarana pencucian uang secara digital.

Atas dasar adanya potensi ancaman ini, penulis memutuskan untuk meneliti fenomena ancaman *cyber laundering* di internet melalui *online games*

sebagai tema skripsinya. Penulis akan meneliti bagaimana potensi dan kemungkinan proses sekuritisasi terhadap *cyber laundering* melalui *online games* dilakukan dan ancaman-ancaman yang dapat muncul dari pencucian tersebut. Penulis juga akan mengkaji mengenai ancaman lanjutan dari ancaman *cyber laundering* tersebut bagi keamanan ekonomi apabila dibiarkan tanpa adanya regulasi dari pihak yang berwenang di Indonesia.

## **1.2. Rumusan Masalah**

Dari penjelasan di atas penulis akan menarik sebuah rumusan masalah yang akan di teliti lebih lanjut.

- a. “Bagaimanakah potensi ancaman yang ditimbulkan dari *cyber laundering* melalui *online games* di Indonesia bagi keamanan ekonomi nasional dan internasional?”.
- b. “Mengapa potensi ancaman *cyber laundering* melalui *online games* ini dapat menjadi ancaman yang perlu disekuritisasikan?”

## **1.3. Tujuan Penelitian**

Penelitian penulis ini bertujuan untuk membantu meningkatkan kewaspadaan dan kesadaran (*awareness*) mengenai adanya potensi ancaman *cyber laundering* di internet, terutama melalui *online games* yang masih belum teregulasi di Indonesia.

#### 1.4. Manfaat Penelitian

Dari hasil yang akan dilakukan ini penulis berharap agar penelitian ini kedepan akan memberikan hasil :

- a. **Manfaat Teoritis** : Menambah bahan bacaan bagi para mahasiswa ataupun pelajar lainnya dalam studi Hubungan Internasional mengenai masalah *cyber laundering* dan juga untuk memberi masukan bagi penulis yang akan melanjutkan penelitian ini serta menjadi acuan untuk meningkatkan kesadaran akan bahaya ancaman yang ada di internet.
- b. **Manfaat Praktis** : Memberi gambaran untuk mahasiswa, pelajar ataupun pembaca lainnya tentang ancaman dari *cyber laundering* dan memberi masukan bagi Pemerintah Indonesia dan pemerintah negara-negara lain agar lebih menyadari akan banyaknya celah yang bisa disalahgunakan di dalam penggunaan internet dan *online games* yang dapat mengakibatkan terjadinya peredaran dana yang tidak jelas dan berpotensi untuk digunakan lebih lanjut dalam membiayai kejahatan transnasional.
- c. **Manfaat Sosial** : Pada penelitian ini diharapkan dapat meningkatkan kesadaran masyarakat dunia agar lebih waspada ketika mereka berinteraksi dan bertransaksi di dalam internet.

## 1.5. Kerangka Pemikiran

### 1.5.1. The Copenhagen School / Mazhab Kopenhagen

Keamanan non-tradisional mulai mengemuka pada akhir 1990-an dari sekelompok pakar yang di kenal dengan nama “*The Copenhagen School*” yaitu Barry Buzan, Ole Waever dan Jaap de Wilde. Mereka mencoba untuk memasukkan aspek-aspek di luar teori keamanan tradisional dalam hubungan internasional, seperti mengenai masalah kerawanan pangan, kemiskinan, lingkungan hidup, kesehatan, perdagangan manusia, terorisme, bencana alam yang merupakan bagian dari bagian studi keamanan (Hemawan, 2007). Dengan memasukkan hal tersebut ke dalam lingkup kajian keamanan (*security*) maka the Copenhagen School mencoba untuk memperluas objek rujukan yang di mana isu keamanan (*security*) tidak hanya akan terus membahas mengenai keamanan negara (*state*) secara tradisional tetapi juga akan membahas mengenai keamanan non tradisional (Buzan, Waever dan Wilde, 1998). Keamanan non tradisional di sini bukan hanya mengenai adanya tindakan kejahatan antar dalam bentuk kekerasan fisik atau melalui kekuatan militer, melainkan keamanan dalam bidang perekonomian yang diakibatkan oleh adanya ancaman *cyber laundering* di internet serta adanya kejahatan yang terorganisir sebagai lanjutan dari praktik *cyber laundering* tersebut. Internet sendiri merupakan zona yang masih kurang regulasi hukumnya, sehingga banyak isu-isu dan ancaman

yang terkait dengan keamanan yang dapat muncul kapan saja dari dalamnya.

Keberhasilan suatu aktor dalam menunjukkan suatu isu menjadi sebuah ancaman bergantung pada keberhasilan aktor dalam mewacanakan keamanan. Pola tersebut merupakan konsep yang dikembangkan oleh Weaver (Buzan, 1990) yang dikenal dengan istilah sekuritisasi. Ada beberapa konsep dalam sekuritisasi yang menjelaskan bagaimana suatu aktor berusaha dalam melakukan upaya sekuritisasi suatu isu. Konsep-konsep tersebut yaitu aktor sekuritisasi, *speech act*, *existential threat*, *referent object*, dan *audience*.

Aktor sekuritisasi adalah pihak yang berusaha untuk melakukan sekuritisasi. Usaha tersebut dilakukan melalui penyampaian ide atau sosialisasi. Usaha tersebut adalah *speech act*. Dalam *speech act* disampaikan mengenai *existential threat*, yaitu isu-isu ancaman eksistensial yang akan disekuritisasi. Usaha sekuritisasi ini ditujukan kepada *audience*, atau pihak-pihak yang ingin dipengaruhi oleh aktor untuk mempercayai *existential threat*, dan akan berpengaruh pada *referent object*, yaitu pihak yang akan terancam dari ancaman eksistensial tersebut nantinya apabila dibiarkan atau terlambat untuk ditindak. (Buzan, Waever dan Wilde, 1998)

Apabila digabungkan, konsep 'keamanan' merupakan wacana dari keamanan nasional yang memiliki penekanan pada pihak yang memiliki otoritas yang mengkonstruksi ancaman atau musuh, yang



memiliki kemampuan untuk membuat keputusan dan melakukan penerapan tindakan darurat. Dalam sekuritisasi, aktor melakukan perluasan cakupan keamanan nasional ke dalam berbagai bidang sehingga semua masalah bisa dilihat sebagai keamanan nasional melalui proses politik.

Jadi, aktor keamanan memiliki kekuatan untuk menyimpulkan tindakan yang diperlukan terhadap suatu masalah dan juga kekuatan politik untuk melakukan pengamanan (*securitizing*) terhadap suatu isu. Aktor keamanan melakukan sekuritisasi untuk menghilangkan suatu ancaman yang sifatnya non-tradisional; lingkungan, ekonomi, kemiskinan, dll. Perubahan eskalasi yang dilakukan aktor untuk merubah isu nonkeamanan menjadi isu keamanan dilakukan melalui proses sekuritisasi (Buzan dan Hansen, *The Evolution of International Security Studies* 2009).

Terkait dengan adanya ancaman *cyber laundering*, masalah ini termasuk dalam keamanan ekonomi ( *Economic Security* ) yang dimana pada kasus ini akan mengancam keamanan ekonomi antar negara karena adanya peredaran dana yang tak jelas asalnya yang bisa saja dana itu berasal dari tindak kejahatan atau praktik ilegal seperti korupsi, penghindaran pajak, pencurian, dan juga penipuan. Tentunya masalah ini juga akan menimbulkan masalah baru jika dibiarkan dan akan menyinggung isu keamanan lain karena efek dari pembiaran ancaman ini adalah meluasnya ancaman ini menjadi bentuk ancaman lain dalam efek

yang berantai. Hal tersebut akan berpengaruh kestabilan ekonomi negara tempat ancaman tersebut muncul dan akan mempengaruhi kestabilan keamanan antar negara di dunia internasional jika ancaman tersebut sudah menjalar, disertai dengan tindak kejahatan lebih lanjut yang menyertainya seperti pendanaan terorisme, peredaran narkoba, dan tindak kejahatan lain yang menggunakan dana dari uang hasil pencucian.

## **1.6. Metode Penelitian**

### **1.6.1. Definisi Konseptual**

#### **1.6.1.1. Internet**

Internet adalah jaringan besar yang saling berhubungan dari jaringan-jaringan komputer yang menghubungkan orang-orang dan komputer-komputer diseluruh dunia, melalui telepon, satelit dan sistem-sistem komunikasi yang lain (Beal, t.thn.). Internet dibentuk oleh jutaan komputer yang terhubung bersama dari seluruh dunia, memberi jalan bagi informasi (mulai dari text, gambar, audio, video, dan lainnya ) untuk dapat dikirim dan dinikmati bersama (Bussiness Dictionary, t.thn.)

### **1.6.1.2. *Virtual Money***

Uang virtual (*virtual money*) adalah uang yang tidak nyata atau tidak berwujud yang digunakan dalam komunikasi dan transaksi secara virtual di dalam internet. *Virtual money* merupakan representasi dari nilai nominal uang di kehidupan nyata yang berfungsi sebagai alat pertukaran, unit hitung, dan penyimpanan yang tidak mempunyai bentuk fisik yang legal, serta tidak terikat oleh aturan negara manapun dan berlaku pada komunitas atau grup yang menyetujui penggunaan dari *virtual money* (Financial Action Task Force, 2014). Berdasarkan pengertian ini, jenis uang ini memiliki berbagai wujud di internet, tergantung dari persetujuan pihak yang menggunakannya.

### **1.6.1.3. *Online Games***

*Online games* atau permainan daring (dalam jaringan) adalah sebuah *game* yang dimainkan melalui jaringan internet, bisa melalui PC, laptop, maupun perangkat lain yang memadai untuk tersambung dengan internet. Jenis dari permainan ini bisa beragam, mulai dari permainan yang dimainkan sendiri (*single player*), berdua (*two players*), hingga banyak orang (*multi players*). Permainan ini ada yang berbayar dan ada pula yang gratis, dimana permainan berbayar akan memerlukan pembayaran secara *online* untuk tetap terus bermain atau untuk mendapatkan keuntungan

tertentu ketika bermain, seperti karakter yang lebih kuat atau barang-barang yang tidak dimiliki oleh pemain lain. Beberapa permainan yang berbayar biasanya mewajibkan pemainnya membayar untuk berlangganan, agar mereka dapat terus bermain selama masa langganan pemain masih berlaku. (Schurman, 2016)

#### **1.6.1.4. Cyber Laundering**

*Cyber laundering* adalah tindakan pencucian uang (*money laundering*) yang prosesnya dilakukan melalui internet. Uang tidak lagi dicuci dalam bentuk fisik, tetapi dicuci dalam bentuk uang virtual yang dengan mudahnya beredar di internet. Uang dipindahtangankan dan dilapisi (*layering*) dengan kebebasan transaksi dan anonimitas yang ada di dalam internet. *Cyber laundering* adalah upaya pencucian uang melalui proses perubahan wujud dari wujud legal yang sah menuju ke wujud virtual dan kemudian dicuci dalam bentuk tersebut di dalam internet untuk kemudian dijadikan menjadi wujud legalnya kembali dengan catatan transaksi yang sah. Catatan transaksi ini bisa menggunakan layanan pembayaran yang ada di dalam internet, seperti *micro-payment*, *online banking*, dan *smart cards* (Filipkowski, 2008) yang umumnya digunakan untuk membeli barang di dalam internet pada situs belanja ataupun *online games* (Strauss, 2013).

#### 1.6.1.5. Keamanan Ekonomi

Keamanan ( *Security* ) berasal dari bahasa latin yaitu “*securus*” yang berartikan terbebas dari suatu bahaya, terbebas dari ketakutan. Dengan kata ini juga bisa bermakna dari gabungan kata *se* dan *curus*. Sehingga jika digabungkan akan bermakna ‘*Liberation From Uneasiness, or a Peaceful Situations Without any Risk or Threat*’ (Liota, 2002). Di sisi lain, Arnold Wolfers dalam bukunya mendefinisikan bahwa keamanan sesungguhnya suatu keadaan dimana tidak adanya keburukan atau ancaman dari suatu ketidakamanan (*insecurity*). Keamanan merupakan suatu kondisi di mana aspek-aspek negatif dari ketidakamanan tersebut dapat diredam (Wolfers, 1962). Keamanan juga dapat diartikan sebagai suatu kondisi yang terbebas dari ancaman, tetapi juga sebagai suatu kondisi yang bebas untuk menanggulangi dan menangani ancaman. Kondisi yang memberikan pilihan akan cara penanggulangan ancaman yang akan datang (K. Booth, 2007; Williams, 2008).

Melalui definisi keamanan tersebut, maka keamanan ekonomi dapat didefinisikan sebagai bagaimana adanya kebebasan dari ancaman atas perekonomian atau ancaman ekonomi sehingga tercipta akses untuk mendapatkan sumber daya, keuangan dan pasar (Buzan, 1991) di mana hal tersebut merupakan elemen penting dalam kelangsungan tingkat kemakmuran yang dapat

diterima publik dan merupakan kekuatan sebuah negara. Dengan akses tersebut, maka suatu negara akan memiliki pilihan dalam pengelolaan sumber daya ekonomi untuk menjaga kestabilan kekuatan dari negara tersebut.

#### **1.6.1.6. Aset**

Aset adalah sumber daya yang atau kekayaan dari suatu perusahaan. Kekayaan disini sendiri dapat berupa sumber daya ,baik berupa benda ataupun hak kuasa yang diperoleh dari suatu peristiwa, seperti produksi atau transaksi di dalam masa kerja perusahaan tersebut, yang terjadi di masa lalu dan disimpan dengan tujuan agar menjadi manfaat bagi kinerja perusahaan di masa mendatang (Surya, 2012).

Ada beberapa cara untuk memperoleh aset, yaitu bisa diperoleh dengan cara diproduksi atau dibangun sendiri, bisa didapat dengan dibeli, juga dengan pertukaran aset maupun sumbangan dari pihak lain. Aset perusahaan umumnya berasal dari transaksi atau peristiwa lain yang terjadi di masa lalu. Perusahaan biasanya memperoleh aset melalui proses produksi perusahaan tersebut sendiri atau melalui transaksi pembelian dengan pihak di luar perusahaan. Barang atau jasa yang telah didonasikan oleh pihak lain kepada perusahaan juga dapat dianggap sebagai aset.

Manfaat yang didapat oleh suatu perusahaan dengan adanya aset adalah potensi dari aset tersebut untuk memberikan sumbangan, baik langsung maupun tidak langsung, dalam bentuk arus dana simpanan dan sesuatu yang setara dengan dana simpanan, kepada perusahaan di masa yang akan datang. Potensi tersebut dapat berbentuk sesuatu yang produktif yang mampu untuk menunjang keberlangsungan kinerja perusahaan. Selain itu, ada beberapa manfaat ekonomi aset di masa depan, misalnya aset dapat digunakan baik sendiri maupun bersama aset lain dalam produksi barang dan jasa yang dijual oleh perusahaan, dipertukarkan dengan aset lain, digunakan untuk menyelesaikan kewajiban perusahaan, dan dibagikan kepada para pemilik perusahaan.

#### **1.6.1.7. Kesadaran**

Definisi sadar menurut Kamus Besar Bahasa Indonesia (KBBI) adalah insaf; merasa; tahu dan mengerti. Ini berarti kesadaran adalah mengetahui dan mengerti akan suatu hal. Kesadaran berarti memahami betul tentang suatu masalah atau peristiwa.

Terkait isu yang penulis bahas, penulis mencoba untuk mengukur sejauh mana pihak-pihak yang terlibat dalam dunia *online games* sadar mengenai potensi ancaman *cyber laundering* melalui *online games*. Penulis menetapkan ukuran kesadaran pada

kasus ini adalah pihak-pihak tersebut mengetahui dan mengerti secara detail, mampu untuk menjelaskan apa itu *cyber laundering* dan bagaimana potensi ancaman yang dimiliki olehnya.

## **1.6.2. Operasionalisasi Konsep**

### **1.6.2.1. *Virtual Payment Supplier Services***

*Virtual Payment Supplier Services* (VPSS) adalah sebuah praktik jasa di mana penyedia jasa menyediakan layanan bagi para pelanggannya, yaitu para pemain *online games*. Layanan ini berpusat pada jasa-jasa pembayaran transaksi secara virtual untuk nantinya dialihkan ke dalam *game* dalam bentuk barang dalam *game* (*in-game items*) dan juga *virtual currency* yang berlaku di dalam *game* tersebut. VPSS biasanya berbentuk sebuah situs yang menyediakan berbagai macam layanan terkait transaksi virtual.

Dalam praktiknya, VPSS menyediakan jasa dengan biaya tertentu yang akan dibayarkan dengan uang nyata dan setelah pembayaran dilakukan, maka penyedia jasa akan memberikan jasa yang telah dibeli. Jasanya beragam dan semuanya virtual, terkait dengan *game* mana yang telah dibeli jasanya (Richet, 2013).

### **1.6.2.2. *Item and Gold Farming***

*Item and Gold Farming* adalah sebuah praktik di mana seseorang memainkan sebuah permainan secara terus menerus,



terutama *online games*, untuk mendapatkan *gold*, istilah umum bagi uang virtual yang digunakan untuk pembayaran dalam permainan, antar pemain untuk membeli barang tertentu. (Scott, 2007) *Farming* ini juga berlaku untuk *item*, yang juga merupakan istilah dalam permainan, yaitu barang-barang yang digunakan di dalam permainan, biasanya berupa barang yang cukup penting hingga barang yang sangat langka yang mampu untuk memudahkan pemain dalam menyelesaikan permainan. Uang dan barang yang sudah terkumpul, kemudian akan dijual kepada para pemain yang berminat (Heeks, 2008). Di dalam beberapa *game*, uang dan barang ini dapat dibeli dengan menggunakan uang asli untuk ditimbun, sehingga memberi celah kepada *cyber laundering*.

Di beberapa negara maju, praktik ini sudah menjadi mata pencaharian bagi beberapa orang. (Davis, 2009) Banyak pemain yang ingin menghemat waktu mereka sehingga mereka memperkerjakan pemain lain untuk mencarikan mereka uang dan barang yang kemudian mereka diberikan upah dalam bentuk uang nyata atas hasil kerja mereka. Praktik ini dapat saling terkait dengan VPSS dan juga dapat dilakukan secara independen. Transaksi pembayaran yang dilakukan biasanya melalui transfer bank secara online.

### **1.6.2.3. In-game Auctions**

*In-game auctions* adalah praktik melelang barang di dalam *game*. Praktik ini sering terdapat di dalam *online games*. Pengembang *game* biasanya memberikan fitur untuk melaksanakan praktik ini. Barang yang dilelang biasanya barang yang akan memberikan pengaruh besar terhadap performa pemain dalam menyelesaikan permainan, sehingga seringkali lelang sangat ramai dengan para pemain yang menawar barang. Praktik ini dapat dikaitkan dengan VPSS dan juga *Gold Farming* dan juga dapat dilakukan secara independen.

Terkait dengan VPSS, lelang terkadang dilakukan dengan virtual money yang jasa transaksinya disediakan oleh VPSS. Di sisi lain, terkadang lelang juga dilakukan dengan *gold* sehingga para *gold farmers* juga mampu untuk mendapatkan keuntungan dari praktik ini. Lelang juga dapat dilakukan dengan menggunakan uang nyata dengan transaksi antar bank online. (Crawley, 2014) Ketika transaksi dilakukan dengan uang nyata dan adanya fasilitas di dalam *game* untuk melakukan hal tersebut, hal ini menjadi celah yang potensial bagi *cyber laundering* untuk masuk.

### **1.6.2.4. Ancaman Ekonomi**

Ancaman ekonomi didefinisikan sebagai suatu hal yang dapat mengganggu keamanan ekonomi dan mengganggu

kebebasan dari ketidakamanan ekonomi. Ancaman ekonomi yang dialami suatu negara dapat mengancam kestabilan ekonomi pada negara tersebut sehingga mengurangi atau bahkan menghilangkan kemampuan negara dalam memilih dan mengelola sumber daya ekonomi yang dimilikinya.

Ancaman ini dapat berupa sistem ekonomi yang kurang baik, inflasi, gempuran globalisasi dan ketidakmampuan negara untuk bersaing dengan negara lain, infrastruktur yang bermasalah dengan korupsi, tindakan pelanggaran hukum seperti penghindaran pajak dan pencucian uang yang mampu melukai kestabilan ekonomi suatu negara karena pendapatannya dicuri. Dengan hilangnya pendapatan negara, maka negara tidak akan mampu untuk menjalankan fungsinya, terutama dalam penyusunan anggaran penyelenggaraan negara yang akan mempengaruhi bidang lain di luar perekonomian, seperti kesejahteraan masyarakatnya hingga pertahanan militer (Stone, 2009).

#### **1.6.2.5. Aset Pada *Online Games***

*Online games* merupakan hasil produksi dari perusahaan yang membuatnya. Dalam hal ini, *online games* dapat dikategorikan sebagai aset milik perusahaan. Namun, *online games* sendiri memiliki nilai aset yang jauh lebih beragam jika dilihat dari komponen yang ada di dalamnya, jauh apabila dibandingkan

dengan pandangan bahwa *online games* hanyalah sebagai aset tunggal perusahaan.

Aset tersebut dapat berupa aset di dalam dan di luar *online games*. Aset di luar *online games* berupa komponen-komponen yang mendukung performa dan pemasaran *online games* dari luar, seperti merchandise, perangkat yang digunakan di dalam games tersebut, baik perangkat keras maupun lunak, *engines*, lisensi dan hak intelektual terhadap *online games* tersebut, investasi sponsor, jasa distribusi yang dilakukan oleh perusahaan lain yang bekerja sama dengan perusahaan pembuat *online games*.

Aset di dalam *games* berupa server dari online games, pemain yang memainkan *games*, informasi akun dari pemain tersebut, termasuk dengan jumlah item dan harga total dari akun-akun tersebut, data-data terkait dengan sumber daya yang ada di dalam *game*, seperti misalnya model karakter, desain level, desain dari barang yang ada di dalam *game*, dan media lain seperti klip suara dan musik.

#### **1.6.2.6. Keadaan Sadar**

Keadaan sadar adalah keadaan di mana seseorang mengerti dan mengetahui akan suatu hal yang ada di sekitarnya. Dia mengerti akan situasi, letak, apa yang sedang terjadi, dan apa yang

harus dilakukan. Keadaan sadar akan membuat seseorang bertindak sesuai dengan kebutuhan situasi lingkungannya.

Dalam bahasan penulis, keadaan sadar yang dimaksud adalah suatu keadaan di mana seseorang memahami betul potensi ancaman *cyber laundering* melalui *online games*. Seseorang tersebut tidak hanya sekedar mengerti mengenai pengertian istilah *cyber laundering*, namun juga memahami kenapa hal tersebut dapat terjadi, dan setidaknya dapat untuk menjelaskan mengapa berdasarkan pengalaman mereka di dalam dunia *online games*. Selain itu, dengan keadaan sadar ini, seseorang dapat menentukan langkah-langkah pencegahan dan penanggulangan terhadap potensi ancaman *cyber laundering* tersebut.

### **1.6.3. Tipe Penelitian**

Pada penelitian ini, penulis menggunakan tipe penelitian secara eksplanatif yang dimana bertujuan untuk menemukan suatu penjelasan mengapa sebuah ancaman dapat muncul suatu dari kasus atau fenomena yang dibahas. Hasil akhir dari penelitian ini adalah mengenai sebab, akibat, dan antisipasi. Pada penelitian ini penulis berusaha untuk menjelaskan ancaman yang muncul dari kasus yang dibahas dalam rangka meningkatkan kesadaran global atas ancaman tersebut.

#### **1.6.4. Jangkauan Penelitian**

Pada penelitian ini penulis memfokuskan pada cakupan tahun dimana transaksi yang melibatkan uang di internet, terutama dalam *online games* terjadi, yaitu pada periode tahun 2010 – 2016 dimulai sejak maraknya penggunaan internet dan munculnya *online games* di dalam masyarakat Indonesia.

#### **1.6.5. Teknik Pengumpulan Data**

a. *Primary Data* ( Data Primer ) data yang didapat oleh penulis secara langsung, yakni dengan cara melakukan penelitian lapangan yang diperoleh langsung oleh penulis melalui survei dengan responden dan wawancara yang dilakukan dengan narasumber.

Survei dilakukan melalui kuesioner. Target populasi dari survei ini adalah semua pemain *online games* yang berada di Indonesia. Kuesioner akan disebar melalui media *online* agar mampu untuk mencakup area survei yang diharapkan dalam waktu yang tidak terlalu lama. Variabel yang akan digunakan dalam survei adalah “Seberapa sering intensitas pemain *online games* di Indonesia dalam bertransaksi?”, “Seberapa banyak biaya yang dikeluarkan di setiap transaksi tersebut?”, “Fasilitas apa saja yang digunakan dalam transaksi tersebut?”, “Seberapa jauh kesadaran pemain *online games* di Indonesia terhadap adanya potensi ancaman *cyber laundering*?”

Penulis juga melakukan diskusi dan wawancara baik dengan bertemu langsung maupun secara *online* melalui email atau chat pribadi dengan mengirimkan beberapa pertanyaan yang terkait kasus yang sedang diteliti kepada narasumber mengenai potensi ancaman *cyber laundering* melalui *online games*.

Penulis merencanakan beberapa narasumber untuk dihubungi. Narasumber tersebut adalah pihak perusahaan *game* yang ada di Indonesia dan instansi-instansi pemerintah yang bertugas untuk mengawasi transaksi keuangan di Indonesia.

b. *Secondary Data* ( Data Sekunder ) yang diperoleh penulis secara tidak langsung melalui pencarian-pencarian pustaka, yaitu dengan mengumpulkan data-data yang relevan dengan permasalahan yang akan dibahas dari literatur-literatur berupa studi kepustakaan seperti buku, jurnal yang relevan, surat kabar, artikel, dokumen-dokumen resmi yang diterbitkan maupun tidak diterbitkan yang didapatkan sesuai dengan persetujuan instansi di mana dokumen tersebut dibuat, situs-situs website serta berbagai media lain dan sumber-sumber yang memiliki hubungan dengan kasus yang sedang diteliti.

### 1.6.6. Teknik Analisis Data

Teknik analisis data yang digunakan penulis dalam penelitian ini adalah kualitatif dan kuantitatif.

#### a. *Data Collection* (Pengumpulan Data)

Penulis akan melakukan pencari data baik data primer maupun sekunder dengan wawancara langsung, survei terhadap responden yang berkaitan dengan tema penelitian, dan juga studi pustaka di bidang terkait. Pengumpulan data ini bertujuan untuk mengumpulkan data untuk mendukung penelitian dalam membahas potensi ancaman *cyber laundering* di dalam *online games*.

#### b. *Data Reduction* (Reduksi Data)

Dalam penelitian ini akan memfokuskan pada hal-hal penting saja dengan cara memilah-milah data dengan berbagai sumber yang banyak. Dengan cara ini, penulis akan berusaha untuk mengaitkan hal-hal yang berkaitan dengan fenomena yang dibahas dari informasi yang didapat, sehingga akan tercipta sebuah kumpulan data yang saling terkait yang menjelaskan secara jelas apa yang diteliti dari kasus atau fenomena yang diangkat.

#### c. *Data Display* (Penyajian Data)

Dalam penelitian ini akan menyajikan data-data dalam bentuk teks yang bersifat naratif yang dibantu dengan berbagai grafik, baik grafik dari tinjauan pustaka maupun hasil survei penulis, gambar, hubungan antar kategori dan sejenisnya yang berkaitan dengan adanya ancaman



*cyber laundering* di internet. Dengan penyajian ini, penulis berusaha untuk menjelaskan data yang telah saling terkait sebelumnya agar lebih mudah untuk dipahami sehingga mampu memudahkan pemahaman pembaca mengenai potensi ancaman *cyber laundering* melalui *online games*.

d. *Conclusion Drawing and Verification* (Penarikan Kesimpulan dan Verifikasi)

Dalam penelitian ini, setelah mengumpulkan dan menyajikan data yang di dapat, penulis kemudian menyimpulkan hasil berdasarkan bukti-bukti yang valid dan terpercaya dari penelitian yang bertujuan untuk mendapatkan hasil dan kesimpulan terkait adanya ancaman *cyber laundering* di dalam internet.

#### **1.6.7. Sistematika Penulisan**

• **BAB I** : Pada pendahuluan ini penulis akan menguraikan latar belakang dari masalah yang diteliti dan selanjutnya akan memberikan alasan mengapa penulis memilih permasalahan atau kasus tersebut. Dalam bab ini juga akan dikemukakan tujuan dari penulisan yang merupakan suatu sasaran yang ingin dicapai dari penelitian ini, disertai dengan sistematika penulisan dan metode penelitian yang akan digunakan.

• **BAB II** : Pada bab ini akan menjelaskan mengenai gambaran umum dari masalah yang dibahas, dimulai dari pengertian *cyber laundering*

secara lebih mendalam hingga penerapan dan modusnya di dalam internet dan *online games*.

• **BAB III** : Pada bab ini akan menjelaskan dan menganalisa bagaimana bahaya dari *cyber laundering* apabila tidak segera ada kesadaran untuk menciptakan regulasi internet yang kuat melalui sekuritisasi dan juga mengukur kadar kesadaran pihak-pihak terkait mengenai isu yang diangkat. Dimulai dari ancaman ekonomi yang akan ditimbulkan hingga bahaya yang mengarah kepada penggunaan dana hasil *cyber laundering* untuk mendanai kejahatan transnasional yang terorganisasi.

• **BAB IV** : Bab ini berisikan penutup dan kesimpulan dari pembahasan. Bab ini adalah bab dimana pada bagian kesimpulan akan dipaparkan jawaban-jawaban dari permasalahan yang diteliti. Pada bagian saran, penulis akan memaparkan gagasan-gagasan penting yang dimiliki dari penulis dengan data-data yang telah ditemukan dan dijelaskan oleh penulis pada penelitian di bab-bab sebelumnya.