

## BAB II

### KAJIAN PUSTAKA

#### 2.1. Review Studi Terdahulu

Guna mendukung penelitian ini, penulis menggunakan referensi dari beberapa peneliti terdahulu untuk dijadikan sebagai bahan bacaan dan sumber data. Beberapa penelitian terdahulu yang telah penulis baca merupakan penelitian yang memiliki tema relevan dengan tema penelitian penulis namun memiliki perbedaan pada pandangan, fokus dan teori. Hal ini membuat penulis dapat mengetahui lebih lanjut mengenai penelitian yang sedang penulis jalani. Terdapat tiga referensi penelitian dan jurnal yang penulis gunakan sebagai kajian pustaka bagi penelitian ini.

Yang pertama ialah jurnal penelitian yang dilakukan oleh Handrini Ardiyanti dengan judul *Cyber Security* dan Tantangan Pengembangannya di Indonesia. Dalam penelitian ini membahas dan menjelaskan bagaimana kebijakan *cybersecurity* yang telah dijalankan di Indonesia selama ini beserta upaya dan tantangan dalam pengembangan kebijakan *cybersecurity* tersebut. Dalam penelitian ini dijelaskan beberapa kebijakan-kebijakan *cybersecurity* yang telah dijalankan di Indonesia. Penelitian ini menggunakan kerangka pemikiran dari manajemen teknologi informasi serta *cybersecurity* dan pertahanan negara. Jika melihat dari global *cybersecurity*, dapat dibangun berdasarkan lima bidang kerja yakni; kepastian hukum, teknis dan tindakan prosedural, struktur organisasi, *capacity building* serta kerjasama internasional. Dari kelima kebijakan-kebijakan tersebut

dijelaskan juga bentuk prospek kerja dan tantangan dalam upaya pengembangan kebijakan *cybersecurity* di Indonesia.<sup>1</sup>

Alasan penulis mengambil studi terdahulu tersebut adalah karena penulis hendak menganalisis kebijakan *cybersecurity* yang telah dilakukan oleh Indonesia sebagai strategi pertahanan negara dalam menangani *cybercrime*. Jurnal ini dirasa dapat memberi sedikit kemudahan bagi penulis dalam meneliti kebijakan apa saja yang telah dilakukan oleh Indonesia dalam mempertahankan negaranya dari ancaman *cybercrime*. Namun tetap ada perbedaan dari penelitian yang dilakukan oleh Handrini Ardiyanti dengan penelitian yang sedang penulis jalani, yakni dari segi fokus masalah serta isi. Pada penelitian yang dilakukan oleh Handrini Ardiyanti hanya membahas mengenai kebijakan-kebijakan yang telah dijalankan Indonesia selama ini dalam garis besar pada beberapa bidang kerja, sedangkan yang hendak penulis teliti ialah lebih berfokus pada bentuk kerjasama internasional Indonesia dengan negara lain dalam menangani *cybersecurity* ini. Selain itu, pada penelitian ini juga tidak memberikan periode tahun yang jelas dalam menganalisa kebijakan Indonesia melainkan menjelaskan semua kebijakan dari hampir 10 tahun yang lalu, sedangkan penelitian yang sedang penulis jalani hendak menganalisa kebijakan Indonesia dan hasil kerjasama internasionalnya lebih singkat dari tahun 2017 hingga 2020.

Penelitian terdahulu kedua yang relevan dengan tema proposal kali ini ialah hasil karya Sofia Trisni, Rika Isnarti dan Abdul Halim dengan judul Peningkatan

---

<sup>1</sup> Handrini Ardiyanti. Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 5(1). 2016.

Keamanan Siber Asean Melalui Kerjasama Keamanan Siber dengan Australia membahas tentang bagaimana ASEAN yang diharapkan dapat membangun kerjasama dengan Australia dalam mengantisipasi adanya serangan *cyber* dikarenakan Australia memang menjadi salah satu negara yang cukup kuat dan serius dalam memperkuat keamanan negaranya dari bahaya *cybercrime*. Dalam menangani ancaman *cyber*, ASEAN telah melakukan upaya pada level bilateral dan regional. Namun, sejauh ini aksi yang dilakukan oleh ASEAN masih hanya dalam batas pembuatan legal dokumen dan peningkatan kerjasama dalam penegakan hukum. Karena hal itu, ASEAN dirasa masih memerlukan upaya yang lebih nyata dan komprehensif dalam menanggulangi ancaman *cyber* ini, salah satunya dengan menjalin kerjasama dengan negara lain.<sup>2</sup>

Alasan penulis memilih jurnal yang kedua ini sebagai bentuk referensi penelitian ialah karena dalam penelitian tersebut terdapat penjelasan bahwa suatu negara membutuhkan adanya hubungan bilateral atau kerjasama dengan negara lain dalam menangani suatu permasalahan yang umum terjadi di dunia, yang mana dalam hal ini adalah maraknya ancaman kasus *cybercrime* di kawasan ASEAN. Negara yang dituju pun sama dengan yang hendak penulis teliti, yakni Australia yang dipandang sebagai negara cukup kuat dalam mempertahankan keamanan negaranya dalam hal *cyber*. Pada penelitian yang dilakukan oleh Sofia, Rika dan Abdul lebih berfokus pada pandangannya terhadap negara-negara di kawasan ASEAN agar dapat membangun kerjasama yang lebih baik dengan Australia yang

---

<sup>2</sup> Sofia Trisni, Rika Isnarti & Abdul Halim. Peningkatan Keamanan Siber ASEAN Melalui Kerja Sama Keamanan Siber Dengan Australia: Pusat Studi ASEAN Universitas Andalas. Diakses melalui <<http://setnas-asean.id/site/uploads/document/journals/file/599d5fe21b7bc-presentasi-1-paper-psa-universitas-andalas.pdf>> pada 28 Desember 2021

dianggap sebagai salah satu negara kuat dalam menangani *cybersecurity*. Sedangkan pada penelitian yang akan penulis lakukan tidak berupa hubungan antar suatu kawasan dengan satu negara melainkan hanya berfokus pada hubungan bilateral antara Indonesia dengan Australia dalam memberi strategi *cybersecurity* untuk kedua negara. Singkatnya, pada penelitian terdahulu ini lebih menjelaskan hubungan multilateral antara Australia dan ASEAN dalam beberapa forum regional sedangkan penulis hanya akan lebih fokus dalam pembahasan hubungan bilateral Indonesia dengan Australia.

Penelitian ketiga merupakan hasil karya dari Abdullah Tulip, Nasriana dan Akhmad Idris yang berjudul Kerjasama Indonesia dengan Negara-Negara Tetangga dalam Pemberantasan Kejahatan Transnasional. Dalam penelitian ini dibahas mengenai kerjasama Indonesia dengan beberapa negara tetangga yang lebih kuat dalam menangani dan memberantas segala bentuk kejahatan transnasional yang termasuk di dalamnya kejahatan di dunia maya (*cybercrime*). Namun, pada penelitian ini lagi-lagi lebih berfokus pada ruang lingkup ASEAN untuk menjalin kerjasamanya. Dalam penelitian ini juga dijelaskan bagaimana status kejahatan transnasional dalam hukum yang berlaku di Indonesia secara luas dengan menjelaskan berbagai macam jenis kejahatan transnasional. Dalam penelitian ini menerapkan prinsip-prinsip yurisdiksi yang berkenaan dengan berlakunya hukum di suatu negara. Namun, pada kasus *cybercrime* merupakan kejahatan yang paling sulit untuk dapat ditemukan “lokasi dan alat bukti” karena *cybercrime* tidak sedikit pun meninggalkan jejak secara fisik seperti sidik jari ataupun contoh DNA yang jelas. Maka dari itu, dalam menangani masalah ini diperlukan adanya mekanisme

berbentuk kerjasama hukum antar negara-negara baik di dalam kawasan maupun internasional.<sup>3</sup>

Alasan terakhir penulis mengambil studi terdahulu ini juga dikarenakan adanya sedikit kesamaan topik dalam penelitian. Dalam penelitian tersebut dijelaskan bentuk kerjasama Indonesia dengan negara-negara tetangga, yang dimaksud dalam hal ini adalah negara-negara kawasan ASEAN untuk memberantas kejahatan transnasional. Selain itu, terdapat penjelasan tentang hukum yang berlaku di Indonesia terhadap berbagai bentuk kejahatan transnasional. Seperti yang diketahui, *cybercrime* memang termasuk kedalam kejahatan transnasional yang dapat dilakukan lintas batas negara. Maka dari itu, dalam jurnal ini dirasa dapat memberikan pandangan lebih bagi penulis perihal pentingnya kerjasama internasional dalam mengatasi suatu kejahatan yang terjadi di berbagai negara.

Tema penelitian karya Abdullah, Nasriana dan Akhmad memang hampir sama dengan tema penelitian yang sedang penulis jalani, namun terdapat perbedaan fokus dalam penelitian ini. Dalam penelitian penulis hanyalah berfokus pada kasus *cybercrime* di Indonesia dengan upaya negara membangun kerjasama internasional dengan Australia yang merupakan negara tetangga sedangkan penelitian Abdullah Tulip, Nasriana dan Akhmad Idris jauh lebih kompleks dalam menjelaskan beberapa kasus kejahatan transnasional yang terjadi di Indonesia dengan berbagai upaya negara untuk menjalin kerjasama dengan negara-negara lain, terlebih khusus pada kawasan ASEAN.

---

<sup>3</sup> Abdullah Tulip, Nasriana & Akhmad Idris. Kerjasama Indonesia Dengan Negara Negara Tetangga Dalam Pemberantasan Kejahatan Transnasional. *Laporan Penelitian Makalah Lengkap*, (0200.3), 2011.

## 2.2. Kerangka Teori dan Konsep

Penggunaan teori dan konsep dalam menganalisa suatu kasus tentu menjadi salah satu hal yang penting guna menghasilkan sebuah analisa dengan pandangan yang berbeda pada setiap peneliti. Ada beberapa teori dan konsep yang dapat digunakan sebagai dasar atau landasan untuk menganalisis efisiensi dari pembentukan kerjasama antar negara dalam kaitannya dengan *cybersecurity* guna mencegah terjadinya *cyber crime* khususnya di wilayah Indonesia dan Australia. Beberapa teori dan konsep tersebut ialah sebagai berikut:

### 2.2.1. Kerjasama Internasional

Dalam hubungan internasional tentu tidak akan lepas dari adanya interaksi antar negara-negara yang dapat berupa interaksi perang, konflik sampai kerjasama dalam organisasi internasional. Interaksi ini kerap dilakukan oleh aktor hubungan internasional yang mana di dalamnya terdapat sebuah kepentingan dari masing-masing negara. Seiring dengan meningkatnya hubungan antar negara di masa kontemporer ini, menjadikan Teori Kerjasama Internasional sebagai teori yang tepat dalam melakukan penelitian ini. Seperti yang diketahui, bahwa tidak ada suatu negara yang dapat berdiri sendiri guna memenuhi segala kebutuhan dan kepentingan negaranya, terlebih dalam meningkatkan perkembangan serta kemajuan negara. Hal ini menjadikan kerjasama internasional sebagai salah satu pilihan yang tepat untuk bisa dijalani. Selain itu, kerjasama internasional juga dapat terjalin karena adanya ketergantungan antar satu negara dengan negara lain. Perkembangan dari situasi hubungan internasional saat ini yang ditandai dengan berbagai bentuk kerjasama internasional di berbagai macam aspek seperti sosial,

budaya, pendidikan, ekonomi, hukum hingga keamanan negara telah menyita banyak perhatian negara-negara di dunia melalui berbagai rangkaian kerjasama internasional tersebut.

Kerjasama internasional diartikan sebagai upaya suatu negara untuk ikut serta atau menyepakati suatu perjanjian internasional yang telah disepakati bersama. Berdasarkan pengaturan substansinya, dalam kerjasama internasional dapat dibedakan menjadi dua kategori berupa *Law Making Treaties*, yakni: Perjanjian internasional yang mengandung berbagai kaidah-kaidah hukum yang berlaku secara universal atau berlaku bagi seluruh anggota masyarakat bangsa-bangsa; dan Perjanjian internasional yang digolongkan sebagai *treaty contracts* atau perjanjian yang mengandung ketentuan-ketentuan khusus guna mengatur hubungan atau berbagai persoalan antara pihak yang menyelenggarakan saja, sehingga ketentuan-ketentuan tersebut hanya berlaku bagi para peserta yang terlibat dalam perjanjian tersebut.<sup>4</sup>

Joseph Frankel mengatakan bahwa negara-negara akan melakukan kerjasama apabila mereka memperkirakan konsekuensi apa saja yang akan mereka tanggung daripada manfaat yang diperolehnya nanti. Selain itu, keberhasilan dari suatu kerjasama juga akan ditentukan berdasar sifat dan tujuan yang ingin dicapai. Dari hasil akhir kerjasama, nantinya akan dijabarkan kembali ke dalam sasaran atau objek yang telah ditentukan berdasarkan persamaan-persamaan fundamental dari

---

<sup>4</sup> Zulkifli. *Op.Cit.* Hlm. 17



masing-masing negara. Hal tersebut dimaksud dengan sebutan kerjasama fungsional.<sup>5</sup>

Menurut K.J Holsti, kerjasama internasional dapat didefinisikan menjadi lima, diantaranya sebagai berikut :<sup>6</sup>

- Kerjasama internasional ialah adanya dua atau lebih kepentingan, nilai atau tujuan untuk saling bertemu guna menghasilkan sesuatu yang dapat dipromosikan atau dipenuhi oleh semua pihak sekaligus.
- Kerjasama internasional dijadikan sebagai salah satu harapan dari suatu negara perihal kebijakan yang akan diputuskan dapat membantu negara tersebut untuk mencapai kepentingan negara.
- Kerjasama internasional merupakan sebuah persetujuan dari masalah-masalah tertentu diantara dua negara atau lebih guna memanfaatkan suatu persamaan atas kepentingan atau adanya benturan kepentingan negara.
- Kerjasama internasional merupakan aturan resmi ataupun tidak resmi mengenai berbagai transaksi dimasa mendatang yang hendak dilakukan guna menjalankan persetujuan yang telah disepakati.
- Kerjasama internasional merupakan transaksi yang dilakukan antar dua negara atau lebih guna memenuhi persetujuan mereka.

---

<sup>5</sup> Umar Suryadi Bakry. *Dasar-Dasar Hubungan Internasional Edisi Pertama*. Kencana. 2017 Hlm. 74

<sup>6</sup> Kalevi Jaakko Holsti. *Politik Internasional: Kerangka untuk Analisis, Jilid 2*. Terjemahan M. Tahrir Azhari. Jakarta: Erlangga. 1988. Hlm. 652-653



### 2.2.2. *Cyber Security*

Keamanan siber atau *cybersecurity* kini kian populer di lingkungan masyarakat seiring dengan meningkatnya pengguna jaringan internet melalui perangkat seperti komputer, laptop, *smartphone*, *desktop* serta penggunaannya yang telah menjadi sebuah keperluan sehari-hari. Tak hanya penggunaan internetnya saja yang meningkat, melainkan jumlah serangan atau *cyber attack* pun ikut meningkat. *Cybersecurity* sendiri merupakan teknologi dengan proses dan praktik yang dirancang khusus untuk dapat melindungi jaringan komputer, program serta data dari serangan atau adanya akses ilegal. Hal ini dijadikan sebagai upaya dalam melindungi informasi dari adanya *cyber attack* atau segala jenis tindakan kejahatan yang sengaja dilakukan untuk mengganggu *privacy*, integritas dan ketersediaan informasi para pengguna. *Cybersecurity* juga dapat dikatakan sebagai hal yang bersifat multidisiplin dan multidimensi subjek, sebab adanya keterlibatan dengan organisasi, hukum, kebijakan, sertifikasi, strategi, etika, personel sampai audit.<sup>7</sup>

Menurut Saco dan Deibert, ancaman dari *cybercrime* telah melanggar batas-batas Negara sehingga mengancam secara internasional. Hal ini disebabkan oleh adanya interaksi masyarakat melalui media sosial yang semakin tinggi akibat adanya kemajuan teknologi dan informasi. Deibert menjelaskan bahwa *cybersecurity* didasari oleh empat wacana terpisah dengan benda rujukan, ancaman, pilihan kebijakan dan perintah yang berbeda yaitu mencakup keamanan nasional,

---

<sup>7</sup> P.D. Persadha, A.A. Waskita & S. Yazid. Comparative Study of Cyber Security Policies Among Malaysia, Australia, Indonesia: A Responsibility Perspective. In *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)*. 2015. Hlm. 146

keamanan Negara (ancaman eksternal terhadap kedaulatan negara dan ancaman internal terhadap keamanan rezim), keamanan swasta dan keamanan jaringan.<sup>8</sup> Ancaman-ancaman dan kejahatan tersebut perlu diantisipasi, salah satunya melalui *cybersecurity*.

Hal tersebut sangat diperlukan untuk menjaga dan mengantisipasi adanya ancaman-ancaman yang berasal dari ruang *cyber*. *Cybersecurity* dapat digambarkan sebagai kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber*, asset organisasi dan pengguna. Asset organisasi dan pengguna yang termasuk dalam *cybersecurity* ialah mencakup perangkat komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam dunia *cyber*.<sup>9</sup> Dapat dikatakan bahwa *cybersecurity* merupakan segala upaya yang dilakukan baik perorangan ataupun kelompok yang secara mandiri ataupun kolektif dengan melakukan tindakan-tindakan atau upaya guna mengamankan, menjaga dan juga mengantisipasi atau meminimalisir dampak-dampak ancaman kejahatan yang berkaitan dengan ruang *cyber*. Oleh sebab itu dalam perkembangannya, *cybersecurity* harus dengan benar mempertimbangkan setiap perilaku manusia yang merancang, mengembangkan dan mengimplementasikan keamanannya. Hal ini dikarenakan manusia menjadi

---

<sup>8</sup> Hidayat Chusnul Chotimah. *Op.cit.* Hlm. 118

<sup>9</sup> Damar Apri Sudarmadi, Arthur Josias Simon Runturambi. *Loc.cit.*

aspek yang terbilang lemah dalam melakukan keamanan informasi dan dapat mengakibatkan kecerobohan tersendiri.

Menurut Kementerian Pertahanan dan Keamanan, fungsi dan *cybersecurity* dapat dijabarkan sebagai berikut :<sup>10</sup>

- Menjamin tercapainya sinergi kebijakan pertahanan *cyber*.
- Membangun organisasi dan tata kelola sistem penanganan *cybrsecurity*.
- Membangun sistem yang menjamin ketersediaan informasi dalam konteks pertahanan *cyber*.
- Membangun sistem penangkalan, penindakan dan pemulihan terhadap serangan *cyber*.
- Mewujudkan kesadaran *cybersecurity*.
- Meningkatkan keamanan sistem *cyber* pada sektor pertahanan.
- Mewujudkan riset dan pengembangan untuk mendukung pembinaan dan pengembangan kemampuan pertahanan *cyber*.
- Menyelenggarakan kerjasama nasional dan internasional guna pembinaan dan pengembangan kemampuan pertahanan *cyber*.

### 2.2.3. *Cyber Crime*

*Cybercrime* telah menjadi sebuah realitas nyata dalam kehidupan di masa kontemporer. Hal ini mungkin menjadi sebuah konsekuensi yang lebih besar ataupun lebih kecil bagi masyarakat, organisasi dan negara. Namun, selama

---

<sup>10</sup> Henike Primawanti, Sidik Pangestu. Diplomasi Siber Indonesia Dalam Meningkatkan Keamanan Siber Melalui Association Of Southeast Asian Nation (Asean) Regional Forum. *Global Mind*, 2(2), 2020. Hlm. 4

beberapa tahun belakangan, hal ini telah tumbuh menjadi suatu hal yang lebih nyata di lingkungan masyarakat. *Cybercrime* secara luas digambarkan sebagai suatu kejahatan yang terjadi di dalam ruang dinamakan “*cyber space*” dan istilah tersebut telah melambangkan bentuk ketidakamanan dan risiko online yang bisa saja terjadi. Dalam artiannya sendiri, *cybercrime* cukup berarti karena cenderung digunakan secara metaforis dan emotif daripada ilmiah atau hukum. Biasanya hal ini digunakan untuk menandakan adanya perilaku berbahaya yang entah bagaimana caranya bisa terkait dengan penyalahgunaan sistem komputer atau jaringan.<sup>11</sup>

Dalam artian lain, *cybercrime* ialah segala kejahatan yang menggunakan perangkat komunikasi secara langsung atau tidak langsung sebagai medianya, baik laptop, komputer, ponsel dan lain-lain. Definisi tersebut menjelaskan bahwa *cybercrime* ialah suatu bentuk dari setiap kejahatan yang menggunakan teknologi informasi secara langsung atau tidak langsung guna mendapatkan keuntungannya sendiri.<sup>12</sup> *Cybercrime* merupakan kelanjutan dari kriminalitas klasik yang di mana komputer beserta dengan program dan data yang ada di dalam satu jaringan yang digunakannya, dapat menjadi target serangan sekaligus sarana untuk melakukan penyerangan.

*Cybercrime* termasuk ke dalam salah satu bentuk kejahatan transnasional atau kejahatan yang terorganisir. Kejahatan terorganisir ini dapat dengan cepat memahami bagaimana mereka bisa memanfaatkan teknologi informasi dan komunikasi guna berkomunikasi, mengatur hingga mengidentifikasi korban beserta

---

<sup>11</sup> David Wall. *Cybercrime: The Transformation Of Crime In The Information Age* (Vol. 4). Polity Press. 2007. Hlm. 10

<sup>12</sup> Rizqiya Windy Saputra. A Survey of Cyber Crime In Indonesia. In *2016 International Conference on ICT for Smart Society (ICISS)*. (pp. 1-5). IEEE. 2016. Hlm. 1

dengan peluang yang bisa mereka dapatkan. Sehingga hal itu dapat meningkatkan efisiensi dalam melakukan kejahatan transnasional lainnya jauh lebih mudah. Contohnya seperti perdagangan narkoba, perdagangan manusia, perdagangan ilegal spesies langka, pencucian uang, penjualan produk palsu, penipuan atau kejahatan ekonomi lainnya.<sup>13</sup> Para pelaku dapat melakukan kejahatan ini baik secara independen ataupun bekerjasama dengan kelompok lainnya. Mereka akan saling memberikan informasi dan pelatihan yang kemudian akan digunakan dalam aksinya.<sup>14</sup>

Adapun kelompok penjahat internasional yang kerap melakukan peretasan komputer dan melakukan berbagai *cybercrime* lainnya. Oleh sebab itu, *cybercrime* bukanlah hanya suatu masalah bagi masyarakat internasional dalam subjek perdebatan politik, penelitian teknologi maupun sosiologi dan ekonomi. Melainkan, hal ini juga merupakan masalah yang dapat menyangkut semua orang dan tidak dapat dipahami dari satu perspektif saja. Hanya dengan pendekatan interdisipliner terhadap fenomena *cybercrime* saja yang mengarah pada pemahaman yang diperlukan untuk menentukan tindakan pencegahan dan reaksi yang tepat terhadap kasus kejahatan ini.<sup>15</sup>

Dalam dua dokumen Kongres PBB yang di selenggarakan di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000 mengenai *The Prevention*

---

<sup>13</sup> Solange Ghernaouti-Helie. *Cyber power: Crime, Conflict And Security In Cyberspace*. Crc Press. 2013. Hlm. 4-5

<sup>14</sup> Marc Goodman. *International Dimensions of Cybercrime*. In *Cybercrimes: A Multidisciplinary Analysis*. Springer, Berlin, Heidelberg. 2011. Hlm. 314

<sup>15</sup> *Ibid*. Hlm. 5

of *Crime and The Treatment of Offenders*, ada dua istilah yang dikenal untuk menjelaskan *cybercrime*, yakni :<sup>16</sup>

- *Cybercrime* yang dalam artian sempit disebut sebagai *computer crime*, yakni perilaku ilegal atau melanggar baik secara langsung ataupun tidak langsung menyerang sistem keamanan suatu jaringan komputer atau data yang telah diproses oleh komputer.

- *Cybercrime* yang dalam artian luas disebut sebagai *computer-related crime*, yakni perilaku ilegal atau melanggar yang berkaitan langsung dengan sistem komputer atau jaringan.

Komputer dan jaringan juga dapat terlibat dalam *cybercrime* ini, namun dengan cara yang berbeda-beda, diantaranya :<sup>17</sup>

- Komputer dan internet dijadikan sebagai alat dalam melakukan kejahatan.
- Komputer dan internet dapat dijadikan sebagai sebuah sasaran atau menjadi korban dari kejahatan.
- Komputer dan internet dapat digunakan untuk segala tujuan *incidental* yang berkaitan dengan kejahatan. Misalnya untuk mencatat penjualan obat-obat terlarang.

---

<sup>16</sup> Ketaren, E. *Op.Cit.* Hlm. 36

<sup>17</sup> Michael Cross. *Scene of the Cybercrime; Second Edition.* Elsevier. 2008. Hlm. 2

### 2.3. Kerangka Konseptual

