BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi dan informasi yang demikian cepat,membawa dampak yang cukup besar dalam kehidupan manusia. Salah satunya adalah jaringan internet yang memukinkan pertukaran informasi tanpa mengenal batas ruang dan waktu. Selain itu, adanya jaringan internet membuat setiap kegiatan manusia menjadi berkembang semakin cepat, juga pengguna internet pada akhir tahun 2000 di seluruh dunia dan terus mengalami peningkatan sekitar 741%, sehingga menjadi lebih dari 3 miliar pengguna pada tahun 2014 (ww w.internetworldstats.com/stats.htm di akses 23 Maret 2017).

Tidak bisa di pungkiri bahwa internet telah mengubah dunia. Internet telah memberikan banyak kemudahan dalam hidup manusia, seperti berkomunikasi, melakukan transaksi, mencari hiburan, memperoleh informasi dan masih banyak lagi manfaat-manfaat yang di rasakan oleh manusia. Namun demikian, pada perkembangannya ternyata pengguna internet tersebut memiliki sisi negatif. Hal itu, membuat internet berpotensi menimbulkan kejahatan di dalamnya. Kejahatan yang timbul sebagai dampak negatif dari perkembangan aplikasi internet ini sering disebut sebagai kejahatan dunia maya (*cyber crime).* Kejahatan dunia maya atau *cyber crime* merupakan kejahatan yang sangat cepat pertumbuhannya.

Semakin banyak tindak kejahatan kriminal yang memanfaatkan kecepatan, kemudian dan sifat anonimitas internet yang tidak mengenal batas tersebut. Selain itu, kejahatan dunia maya juga menimbulkan kerusakan yang lebih besar terhadap masyarakat daripada kejahatan tradisional dan lebih sulit diselidiki, karena pelaku kejahatan dunia maya dapat melakukan aksi kejahatan di lokasi yang berbeda dengan korbannya. Korban dari aksi kejahatan dunia maya mengalami kerugian baik material maupun non material.

Perubahan yang terjadi dalam peradaban dunia, yang salah satunya ditandai dengan kemajuan teknologi, menyebabkan ancaman terhadap kedaulatan suatu negara menjadi semakin kompleks. Dunia tidak lagi memandang militer sebagai satu-satunya potensi ancaman, melainkan mulai merespon terhadap ancaman nirmiliter. Salah satu ancaman nirmiliter di bidang teknologi, adalah ancaman *cyber*. Teknologi *cyber* yang terus berkembang dengan berbagai infrastrukturnya telah membuat batas antar negara menjadi semakin kabur. Konektifitas, kecepatan, dan kemudahan akses yang dimilikinya menjadi suatu hal positif yang dimanfaatkan oleh masyarakat di berbagai negara karena persebaran informasi yang semakin mudah. Sebagai gambaran, tercatat bahwa hingga kuartal ke-2 tahun 2015, pengguna internet di dunia telah mencapai 3.2 milliar. Transaksi perbankan, analisis dan komputasi data di perusahaan maupun pemerintahan, teknologi militer, hingga masyarakat umum memanfaatkan *cyberspace* sebagai media komunikasi (https://www.infokomputer.com/2016/02/berita/berita-reguler/pengguna-internet-mencapai-32-milyar/ Diakses 17 Maret 2017)

Keberadaan dari perkembangan teknologi dan informasi yang menyediakan sebuah ruang *cyber* dimanfaatkan oleh kelompok tentara untuk melakukan berbagai macam kegiatan. Hal ini terbukti dari fakta bahwa saat ini hampir sebagai besar organisasi teroris baik yang berskala besar maupun kecil telah memiliki *website*. Dalam hal ini mereka bekerjasama dengan kelompok kejahatan terorganisir dan menggunakan teknologi untuk menyebarkan propaganda, mengumpulkan dana dan melakukan pencucian uang, merekrut dan melatih anggota baru, berkomunikasi dan berkordinasi untuk melancarkan serangan sementara pemerintah melakukan penanggulangan dengan menggunakan cara-cara yang konvensional. Dengan demikian maka harus diakui bahwa pemerintah akan tertinggal apabila tidak dapat membatasi ruang gerak mereka dalam *cyber* tersebut. Salah satu alasan mengapa internet menjadi salah satu media yang aktraktif digunakan oleh kelompok teroris adalah menjadi tempat yang aman untuk melakukan berbagai kegiatan terkait dengan sulitnya melacak komunikasi yang dilakukan dalam ruang tesebut (Kriyantono, 2006 : 234)

Dari beberapa defenisi di atas terlibat bahwa hal ini aktifitas atau kegiatan teroris tersebut menjadikan *cyber* sebagai media ataupun sebagai objek/target sasaran dikenal dengan *Cyber Terrorism*. Namun dalam hal ini yang kemudian membedakan dengan kejahatan lain yang terkait dengan *cyber* ini adalah tindakan didasari oleh motivasi politik yang melatar belakangi serta tujuan yang ingin dicapai yang mentargetkan aspek psikkologis dari target yang dalam hal ini tentunya adalah masyarakat sipil agar tercipta rasa ketakutan. Meskipun tidak dapat dipungkiri bahwa akibat yang kemudian dapat dirimbulkan adalah dampak

secara fisik terkait dengan sabotase terhadap berbagai program komputer yang terkait dengan kehidupan sehari-hari seperti pada bidang transportasi.

Dalam melancarkan aksinya kelompok teroris menggunakan internet sebagai salah satu bentuk untuk menyebabkan kerusakan. Teroris melakukan perlawanan terhadap pemerintah untuk tujuan tertentu dan mereka akan menggunakan berbagai cara untuk mendapatkan tujuan tersebut. Jika serangan *cyber* ini terjadi terdapat resiko kerusakan, namun resiko terbesar bagi keamanan nasional tetap berasal dari serangan yang bersifat tradisional. Meskipun demikian namun berbagai potensi serangan yang dilakukan di ruang internet atau dengan memanfaatkan ruang internet dalam mengkoordinasi dan merencanakan serangan teror tersebut perlu untuk diwaspadai serta di cegah sedini mungkin.

Dalam serangan di ruang *cyber* terdapat dua karakteristik yakni serangan terhadap data dan terhadap sistem kontrol. Pencurian dan perusakan data mengarah kepada sabotase merupakan serangan yang umum terjadi. Serangan yang terfokus kepada pengambilan sistem digunakan untuk melumpuhkan atau memanipulasi insfrastruktur secara fisik. Meskipun demikian namun hal ini dapat menyurutkan upaya untuk melakukan pencegahan dari kegiatan teroris di ruang *cyber.* Pelacakan yang dapat dilakukan hanya mengandalkan indentifikasi *Internet Protocol Address* (IP), yang kadang sulit dilakukan karena terhambat diverifikasi sistem serta regulasi terkait dengan penggunaan dan keamanan teknologi informasi dan komunikasi yang digunakan di tiap-tiap negara. Ruang *cyber* tidak memiliki batasan namun dalam hal ini penegak hukum yang berupaya untuk melakukan pencegahan dan pemberantasan terorisme memiliki batasan terkait

dengan kedaulatan sebuah negara, upaya tersebut harus terhenti saat mereka bertemu dengan batasan kedaulatan saat mereka melakukan investigasi mengenai aktivitas yang terjadi di ruang *cyber* serta melakukan identifikasi terhadap IP *Address* menjadi sebuah proses yang kompleks dan memakan waktu yang lama (Kriyantono, 2006 : 237)

ASEAN *Regional Forum* (ARF) yang dibentuk pada tahun 1994 merupakan suatu forum yang bertujuan untuk mengembangkan dialog dan konsultasi konstruktif mengenai isu-isu politik dan keamanan yang menjadi kepentingan dan perhatian bersama, dan memberikan kontribusi positif dalam berbagai upaya untuk mewujudkan *confidence building* dan *preventive diplomacy* di kawasan Asia Pasifik. Peran ARF dalam pembentukan keamanan di bidang *cyber* tidak terlepas dari tujuan dibentuknya ASEAN *Political-Security Community* (APSC) yang bertujuan untuk membentuk perdamaian bagi negara-negara di kawasan ASEAN dan dunia dalam lingkungan yang demorkatis dan harmonis. Landasan mengenai APSC tersebut dijelaskan dalam dokumen APSC *blueprint* yang menyepakati mengenai peningkatan kerjasama dalam hal ancaman non tradisional, secara khusus mengenai kejahatan transnasional dan lintas batas. (http://*www.ASEAN.org/archive*/5187-18.pdf, diakses pada tanggal 23 Maret 2017).

Memandang bahwa ancaman *cyber* yang bersifat lintas negara, maka bentuk-bentuk kerjasama internasional dapat menjadi salah satu solusi yang dapat dilakukan dalam mengatasi ancaman *cyber*. Pada lingkup regional, pengamanan *cyberspace* untuk menjadi sesuatu yang mendesak telah menjadi pembahasan

dalam berbagai diskusi dalam salah satu forum kerjasama politik dan keamanan *Association of South East Asian Nations* (ASEAN), yaitu ASEAN *Regional Forum* (ARF). Melalui kerjasama internasional di ARF, kebijakan luar negeri pemerintah dapat dimaksimalkan untuk mencapai *cyber security* sebagai salah satu kepentingan nasional bangsa. Strategi diplomasi yang tepat perlu digunakan sebagai instrumen dalam pencapaian kepentingan nasional di bidang pertahanan dan keamanan.

ARF menyepakati bahwa konsep keamanan menyeluruh (*comprehensive security*) tidak hanya mencakup aspek-aspek militer dan isu keamanan tradisional namun juga terkait dengan aspek politik, ekonomi, sosial dan isu lainnya seperti isu keamanan non-tradisional. Peserta ARF berjumlah 27 negara yang terdiri atas seluruh negara anggota ASEAN (Indonesia, Brunei Darussalam, Kamboja, Laos, Vietnam, Myanmar, Malaysia, Singapura, Thailand, dan Filipina), 10 negara Mitra Wicara ASEAN (Amerika Serikat, Kanada, China, India, Jepang, Korea Selatan, Rusia, Selandia Baru, dan Uni Eropa) serta beberapa negara di kawasan yaitu: Papua Nugini, Mongolia, Korea Utara, Pakistan, Timor-Leste, Bangladesh dan Sri Lanka (http://www.kemlu.go.id/id/kebijakan/kerjasamaregional/Pages/ARF.aspx diakses tanggal 5 Mei 2017)

Konsep dari ARF adalah untuk memelihara stabilitas keamanan kawasan dan pencegahan konflik regional. Berdasarkan hal tersebut, ARF memperkenalkan norma baru dalam ASEAN mengenai proses *cooperative security* yang menekankan konsep keterbukaan melalui promosi dialog diantara negara-negara yang memiliki kesamaan maupun perbedaan pemahaman mengenai isu tertentu.

Berbeda dengan konsep kerjasama keamanan oleh *North Atlantic Treaty Organization* (NATO) yang dibentuk berdasarkan traktat atau aliansi pertahanan pasca Perang Dunia II, ARF ditujukan untuk membangun rasa saling percaya yang mengadopsi pendekatan multilateral untuk mencegah konflik di kawasan. Pendekatan perjanjian keamanannya pun diimplementasikan dengan cara yang berbeda. Karakter ARF tidak seperti NATO yang identik dengan penggunaan kekuatan militer, melainkan lebih kepada dialog dan keterlibatan sebagai cara pencegahan konflik. Dengan demikian, konsep ARF sejalan dengan pendekatan APSC sebagai dasar dari lahirnya ARF yang mempromosikan penolakan agresi terhadap ancaman melalui penggunaan kekuatan dan lebih mengedepankan penyelesaian damai (Chanto, 2003 : 41-47).

Hal tersebut sesuai dengan pemahaman *cooperative security* yang ditegaskan oleh Moodie sebagai suatu proses kerjasama antar negara dengan kepentingan yang sama untuk meredakan ketegangan dan kecurigaan, menyelesaikan atau mengurangi sengketa, membangun rasa percaya diri, maupun memelihara stabilitas kawasan. Hingga saat ini, ARF membentuk lingkungan keamanan pada kawasan dengan pendekatan *cooperative security* melalui kerjasama regional yang diciptakan bukan untuk mengatasi konflik, melainkan meminimalkan dampak perbedaan persepsi dan kepentingan. Kondisi tersebut memberi pemahaman bahwa konsep ARF lebih cenderung kepada pendekatan *soft institutionalism* yang menerima nilai-nlai bersama dibandingkan dengan *hard institusionalism* yang berdasarkan pada yuridiksi dan supremasi hukum (Moddie, 2000 : 5).

Pada September 2012 sebuah kelompok aktifis *hack/hacker* yang bernama Null Crew, meluncurkan serangan terhadap situs pemerintahan Kamboja setelah penangkapan Gottfird Svartholm Warg (*co* pendiri *The Pirate bay*) serangan itu juga merupakan tanda protes keras terhadap sensor internet. Null Crew juga berhasil menyusup ke beberapa situs pemerintahan dan bahkan tentara Kamboja, dan membocorkan informasi yang sangat penting dan rahasia, mereka juga melancarkan perang *cyber* terhadap kamboja dalam memprotes penangkapan Warg. Lebih dari 5.000 dokumen yang berhasil mereka curi dan dibocorkan dari Departemen Luar Negeri Kamboja.

Setahun kemudian tepatnya pada bulan January 2013 website Polisi Militer Nasional Kamboja di *hacked* oleh *hacker* Indonesia uang disebut "Hmei7". Website Mahkamah Agung juga di *hack* tapi tidak ada informasi lebih lanjut yang di temukan dari penyelidikan (Dokumen *Youth Model* ASEAN *Conference* : 3)

Bukan hanya sekali saja *hacker* Indonesia berseteru dengan para *hacker* Malaysia. Ada beberapa 'peperangan' yang pernah terjadi antara keduanya. Ketika munculnya *hastag* #OpAustralia karena pemerintah Australia melakukan aksi penyadapan dan para *hacker* Indonesia menggempur *website* di negara tersebut, muncul satu rumor yang mengatakan bahwa oknum yang sengaja memancing di air keruh dan menurut pelacakan IP-nya berasal dari Malaysia

Dikarenakan hal tersebut, para peretas dari Tanah Air berbalik arah untuk melancarkan serangan ke *website-website* Malaysia dan berimbas pada bertumbangnya situs di Malaysia tersebut. Selain karena kesal karena isu adu

domba ini, ternyata para *hacker* Indonesia mengusung misi lain dalam penyerangannya itu yang didasari oleh rasa tidak senang akan ulah Malaysia yang dengan seenaknya main klaim banyak hal dari Indonesia serta perlakuan kasar terhadapn para TKI di negara mereka tersebut.

Tentunya, dikarenakan serangan tersebut, beberapa kelompok *hacker* dari Malaysia juga melancarkan serangan balasan dan aksi *defacing*, *spoofing* sampai dengan serangan DDos bermunculan dari kedua negara. Beberapa hari setelah peperangan dilakukan, secara tiba-tiba kedua belah pihak saling mengendurkan serangan dan melakukan *wait* and *see* tanpa ada klarifikasi lebih lanjut.

Bank Indonesia dilaporkan terkena serangan *cyber* masif yang menyasar ke *website* publiknya, serangan ini diduga berhubungan dengan ancaman dari kelompok hacker *Anonymous* yang menyatakan akan menyerang berbagai bank di seluruh dunia. Sebagai antisipasi serangan tersebut, Bank Indonesia telah memblokir akses dari 149 negara yang terindikasi jarang mengakses *website* mereka, termasuk negara kecil di Afrika, beberapa bank sentral sudah mengalami serangan serupa dan telah membagikan alamat IP yang digunakan oleh pelaku, tidak ada kerugian yang di alami Bank Indonesia dalam serangan DdoS (*Distributed Denial of Service*).

Dalam serangan puncak Bank Indonesia mendeteksi 274 virus dan 67 ribu email spam ditujukan ke server dan website hanya dalam waktu setengah hari untungnya serangan tersebut berhasil dimentahkan (https://inet.detik.com/security/d-3238644/situs-bank-indonesia-dihantam serangan-cyber diakses 23 April 2017).

Serangan kejahatan dalam jaringan di Indonesia oleh para peretas atau *hacker* terhitung Agustus 2015, telah merugikan negara mencapai Rp.33,29 miliar dan dalam kurun waktu tiga tahun tercatat ada 36,6 juta serangan kejahatan dalam jaringan. Sejak 2012 sampai April 2015, Subdit IT/*Cyber* telah menangkap 497 orang tersangka kasus kejahatan dunia maya. Dari jumlah itu sebanyak 389 orang warga negara asing dan 108 WNI. Kejahatan di dunia maya juga semakin meningkat seiring semakin banuak pengguna internet dan semakin baiknya koneksi internet di Indonesia.

Indonesia juga sedang mewaspadai kejahatan IT model terbaru yaitu peretasan mobil mewah yang bisa diterobos dengan jaringan teknologi. Peretasan mobil saat ini mungkin belum menjadi kasus yang sering terjadi di Indonesia dan Asia, tetapi kasus ini berpotensi menjadi kejahatan model baru di masa yang akan datang seiring dengan semakin banyaknya penggunaan mobil yang terkoneksi internet berbasis penyelarasan (*sync)*, *Wi-Fi, bluetooth, Uconnect,* dan sejenisnya. Data dari laman *www.carmudi.co.id* menyebutkan dua orang ahli *cyber* telah meretas perangkat keamanan *Jeep Cherokee* melalui perangkat komunikasi terintegrasi yang tersambung di mobil tersebut untuk mengambil alih kontrol, pendingin udara, gerak *wiper,* pedal gas dan rem. Peretasan mobil saat ini sedang menjadi isu hangat di kalangan pelaku industri otomotif di negara-negara maju. Di London, tahun 2014 terdapat 6.000 kasus pencurian mobil dengan meretas *keyless entry*. Selain itu, peretasan melalui *Uconnect* dilakukan dengan meretas akses jaringan internal mobil melalui wifi(https://m.tempo.co/read/news/2015/08/26/1

72695105/cyber-crime-lebih-dari-rp-33-m-melayang-gara-gara-hacker diakses 23 April 2017).

Ada 3 situs milik pemerintah Thailand yang diserang oleh peretas yang mengatas namakan dirinya '*Fallag Gassrini dan Dr.Lamouchi'*, antara lain milik Universitas Mahasarakham dan Rumah Sakit Lam Luk Ka. Pada Minggu 23 Agustus 2015 malam, 3 situs tersebut tidak bisa di akses hingga kini, peretas itu memasukan foto-foto Rohingya ke dalam *website* itu. Mereka juga meninggalkan pesan berupa," situs anda telah di serang oleh Fallag Gassrini dan Dr.Lamouchi"

Keesokan harinya tepatnya hari Senin 24 Agustus 2015, 3 situs lainnya turut diretas juga. Tiga antara lain milik pemerintah provinsi Tak, Sing Buri, dan Sa Kaeo tidak bisa di akses. Namun, sejauh ini belum ada konfirmasi siapa peretas itu. Menurut Kementrian Informasi dan teknologi Thailand, grup peretas ini terkenal di seluruh dunia dan sering menyerang dengan menggunakan *program Linux*.

Pemerintah Negara Thailand mengatakan mereka sedang memulihkan serta meng-*update* sistem mereka agar lebih bisa terlindungi. Hingga kini, mereka masih mencari lokasi *server* milik grup peretas Tim Fallaga (http://g lobal.liputan6.com/read/2300870/situs-pemerintah-thailand-diserang-hacker diakses 5 April 2017).

ARF *on cybersecurity initiatives* merupakan bagian dari mekanisme ASEAN dalam menangani kejahatan *cyber* yang tertuang dalam ASEAN's *Cooperation on Cybersecurity and against Cybercrime*. Kerjasama tersebut melibatkan berbagai pertemuan internasional selain ARF, seperti ASEAN *Ministerial Meeting on Transnational Crime* (AMMTC), ASEAN *Senior Officials Meeting on Transnational Crime* (SOMTC), ASEAN *Telecommunications Regulators Council* (ATRC), dan *Senior Officials Meeting on Social Welfare and Development* (SOMSWD). Berbagai pertemuan tersebut memiliki perannya masing-masing dalam mewujudkan keamanan *cyber* di kawasan Asia Tenggara.

1. *ASEAN Ministerial Meeting on Transnational Crime* (AMMTC) memiliki peran sebagai suatu pertemuan yang memfokuskan tentang peningkatan peningkatan kerjasama ASEAN mengatasi kejahatan lintas negara, khususnya antara lain penanganan *cyber* terorisme, perdagangan manusia, peredaran obat terlarang, serta kejahatan maya (*cyber crimes).* Salah satu tantangan terbesar ASEAN saat ini adalah terorisme, kejahatan lintas negara, peredaran narkoba dan perdagangan manusia.
2. ASEAN *Senior Officials Meeting on Transnational Crime* (SOMTC) memiliki peran untuk memerangi krisis keamanan di ASEAN dengan dilakukannya konsultasi dengan beberapa negara antara lain Australia, Kanada, China, Uni Eropa, India, Jepang, Korea, Selandia Baru, Rusia dan AS, dalam meningkatkan dan mempererat kerja sama dengan ASEAN dalam upaya menumpas kejahatan transnasional.

3. ASEAN *Telecommunications Regulators Council* (ATRC) adalah platform yang menyediakan regulator komunikasi dan otoritas di wilayah untuk kerjasama dalam kepentingan bersama untuk administrasi negara-negara anggota ASEAN, dan mengidentifikasi dan mempromosikan kerja sama dalam bidang telekomunikasi diantara AMSs dan memfasilitasi pertukaran infomasi melalui program kerja.
4. *Senior Officials Meeting on Social Welfare and Development* (SOMSWD) untuk mengatasi resiko social yang di hadapi oleh anak perempuan, orang tua dan orang-orang cacat

ARF on cybersecurity initiatives mulai dilaksanakan pada tahun 2006 melalui pernyataan bersama pada pertemuan di Malaysia dan ditegaskan kembali pada ARF *Statement on Cooperation in Ensuring Cyber Security*, di Phnom Penh, 12 Juli 2012, sebagai berikut.

1. Mempromosikan pertimbangan strategi lebih lanjut untuk mengarasi ancaman yang muncul di bidang ini yang sesuai dengan hukum internasional dan prinsip dasarnya.
2. Mempromosikan dialog tentang langkah-langkah pengaturan konfidensil, stabilitas dan pengurangan risiko untuk mengatasi implikasi penggunaan TIK peserta ARF, termasuk pertukaran pandangan mengenai potensi penggunaan TIK dalam konflik.
3. Mendorong dan meningkatkan kerjasama dalam mewujudkan budaya *cyber security*.

4. Mengembangkan rencana kerja ARF tentang keamanan dalam penggunaan IT, berfokus pada kerja mengenai langkah-langkah membangun kepercayaan, yang dapat menetapkan tujuan dan kerangka kerja yang sesuai untuk pelaksanaannya.
5. Meninjau kemungkinan untuk menguraikan instilah dan defenisi umum yang relevan dengan bidang penggunaan TIK (Kerjasama ASEAN untuk *cyber security* dan melawan *cyber crime*, 2013).

ARF sebagai forum dialog politik dan keamanan yang menggunakan keamanan koperasi sebagai pendekatan dalam meningkatkan hubungan antar negara anggota ASEAN dan mitra dialog ASEAN. Mengembangkan kemitraan keamanan regional merupakan agenda utama ARF, dimana kemitraan dalam membangun keamanan regional adalah tatanan keamanan suatu wilayah internasional yang didasarkan pada konsensus di antara pemerintah untuk bekerja sama dalam menangani ancaman keamanan. Dalam memaksimalkan ARF sebagai forum dalam menciptakan keamanan *cyber* regional di Asia Tenggara, ASEAN perlu memaksimalkan peran negara maju - ARF ke dalam pembangunan di ASEAN itu sendiri. Dalam beberapa tahun terakhir ini bisa dilihat melalui berbagai kerjasama yang di lakukan oleh ASEAN *Regional Forum* dengan China pada tahun 2009, dengan Jepang pada tahun 2014, dengan Uni-Eropa pada tahun 2007. Dari ketiga kerjasama tersebut sama-sama membahas mengenai *cyber terrorism* yang terjadi di Asia Tenggara sebagai bentuk tindakan *Preventive Diplomacy* untuk mencegah munculnya suatu sengketa antara para pihak,

mencegah meluasnya suatu sengketa, atau membatasi perluasan suatu sengketa (Manopo,2015:48).

Akibat adanya ancaman nyata dari *cybercrime* tersebut yang telah di alami oleh negara-negara asia tenggara, maka ARF berusaha untuk melakukan kerjasama dalam ruang lingkup kerangka kerja nasional dalam menangani kejahatan *cyber* dengan cara bekerja sama dengan badan-badan internasional dan regional untuk melakukan penyelidikan dan pengumpulan data tentang *cyber* dan berbagi bukti *cyber* dan, pengelolaan sumber daya yang efektif untuk kemitraan yang saling menguntungkan dan mendorong kerjasama internasional, interoperabilitas, dan koordinasi dalam memerangi penyalahgunaan *cyber* dan kejahatan *cyber*.

Salah satu upaya yang dilakukan ASEAN *Regional Forum* jauh sebelum *cyber terrorism* berkembang seperti sekarang maka di lakukan seminar forum regional ASEAN yang membahas secara khusus tentang *cyber terrorism* di Kota Cebu, Filipina, tanggal 3-5 Oktober tahun 2005. Seminar tersebut memberi tempat bagi negara-negara peserta ARF untuk secara tebuka berbagi informasi dan gagasan mengenai kebijakan nasional tentang *cyber terorism*, dan mendorong mereka untuk terus berkerja sama satu sama lain dalam berbagai ancaman terkait *cyber terorism* secara efektif (ASEAN *Regional Forum Document*, 2007 : 503).

Dan juga salah satu upaya yang di lakukan adalah membentuk tim yang bernama *CERT (Computer Emergency Response Team)* , merupakan tim koordinasi teknis terkait insiden jaringan internet di seluruh dunia. Belakangan tim ini disempurnakan melalui RFC 2350 dengan nama *CSIRT (Computer*

Security Incident Response Team). Adanya CSIRT ini adalah dalam rangka mewadahi serta mengatur suatu cara penanganan berbagi insiden di bidang teknologi informasi agar masalah yang terjadi BPPT dalam bidang ini dapat diselesaikan secara cepat, tepat serta bisa melaksanakan dengan baik dalam rangka pengamanan informasi. Dengan ini beberapa fungsi CSIRT antara lain sebagai berikut :

1. *Defense*, melindungi infrastruktur kritis
2. *Monitoring*, menganalisis anomay dengan pola terdefenisi dan pola tak terdefenisi.
3. *Intercepting*, mengumpulkan kontek spesifik atau disebut *targeted content.*
4. *Surveillance*, mengamati dan menganalisi aktifitas yang dicurigai dan informasi yang berubah dalam system
5. *Mitigating*, mengendalikan kerusakan dan menjaga ketersediaan serta kemampuan layanan tersebut.
6. *Remediation*, membuat solusi untuk mencegah kegiatan yang berulang-ulang dan mempengaruhi system
7. *Offensive*, pencegahan/perlawanan dengan menyerang balik seperty *Cyber Army* dan kemampuan untuk menembus system keamanan (https://csirt.bppt.go.id/ diakses 1 Januari 2017).

Dapat dilihat dari penelitian-penelitian terdahulu yang membahas tentang *Cyber Crime* di Asia Tenggara berupa karya ilmiah yang membahas hal yang sama dengan apa yang akan diteliti oleh peneliti.

Penelitian-penelitian mengenai *cyber crime* di Asia tenggara adalah karya ilmiah yang berbentuk *E-Jurnal* yang telah dilakukan oleh Rahmat Haryama S.ip yang berjudul ASEAN *Cyber Security* (Kerjasama Keamanan Dunia Cyber Dikawasan ASEAN) yang di buat pada tahun 2014 di Universitas Pertahanan Indonesia.

Dalam karya tulis tersebut yang bersangkutan dengan masalah, menjelaskan tentang kerjasama keamanan dunia *cyber* di kawasan ASEAN dan menjelaskan tentang bagaimana ASEAN dalam meningkatkan teknologi komunikasi dan informasi, sedangkan banyak negara-negara di ASEAN belum siap terlibat dalam kerjasama keamanan *cyber*.

Perbedaan dengan penelitian ini adalah, penelitian ini lebih memfokuskan kepada kinerja ASEAN Regional Forum dan bagaimana cara menanggulangi *cyber terorism* .

Penelitian lainnya yang membahas tentang ARF sebuah karya ilmiah yang berbentuk skripsi, yang telah dilakukan oleh Nurul Chintya irada yang berjudul (Peran ASEAN Regional Forum Dalam Menjembatani Penyelesaian Konflik Laut China Selatan Tahun 2002-2011) yang di buat pada tahun 2013 di Universitas Airlangga.

Dalam skripsi tersebur saudari Nurul Chintya Irada membahas mengenai ARF yang memfokuskan kepada konflik laut china selatan, Sengketa Laut China Selatan sudah lama menjadi isu krusial diantara negara-negara Asia Tenggara. Wilayah yang ditenggarai punya arti strategis segi ekonomi dan militer ini menjadi permasalahan yang tidak terselesaikan sampai sekarang karena banyak

negara yang mengklaim sebagai wilayahnya. Adapun negara-negara tersebut, antara lain China, Vietnam, Brunei Darussalam, Filipina, dan Malaysia.

Perbedaan dengan penelitian ini adalah disini membahas mengenai ARF dalam penanganan dalam *cyber crime* khususnya *cyber terorism*.

Berdasarkan uraian tersebut maka peneliti tertarik untuk melakukan penelitian yang dirumuskan dalam judul : ***" Upaya ASEAN Regional Forum* (ARF) *Dalam Penanganan Cyber Terorism di Asia Tenggara Tahun 2012-2017 "***

Penelitian ini dibuat berdasarkan beberapa mata kuliah pada program studi Ilmu Hubungan Internasional, antara lain :

1. *Cybercrime,* merupakan mata kuliah yang menjelaskan tentang kasus kasus *cybercrime* yang ada di dunia, serta menjadi dasar Peran ASEAN Regional Forum.
2. Organisasi Internasional, merupakan mata kuliah yang mempelajari fungsi dan peran Organisasi Internasional dalam menjalankan fungsinya. Disini organisasi tersebut adalah ASEAN *Regional Forum* (ARF) adalah sebuah organisasi atau forum yang bertujuan untuk mengembangkan dialog dan konsultasi konstruktif mengenai isu-isu politik dan keamanan yang menjadi kepentingan dan perhatian bersama, dan memberikan kontribusi positif.
3. Studi Keamanan Internasional, dalam mata kuliah ini mempelajari konsep keamanan suatu negara yang menjadi faktor penting dalam kehidupan bernegara suatu bangsa. Berdasarkan mata kuliah ini peneliti menilai

bahwa perkembangan teknologi dan informasi, membawa setiap negara untuk saling membantu dalam menangani cybercrime karena dapat mengancam setiap negara.

4. Hubungan internasional di Asia Tenggara, di dalam mata kuliah ini mempelajari tentang hubungan-hubungan antara negara-negara yang berada di Asia Tenggara, serta menjalani komunikasi antar negara dan menjalin kerjasama baik dalam bidang sosial, politik, dan keamanan. Serta adanya ASEAN yang mewadahi segala kepentingan dari negara-negara ASEAN dalam menaggulangi segala bentuk ancaman keamanan seperti terorisme,perompakan, perdagangan manusia, dan *cyber crime.*

1.2 Rumusan Masalah

Berdasarkan uraian di latar belakang, maka peneliti merumuskan masalah mayornya sebagai berikut :

1.2.1 Rumusan Masalah Mayor

Bagaimana Upaya ASEAN *Regional Forum* (ARF) dalam penanganan *Cyber Terorism* di Asia Tenggara tahun 2012-2017 ?

1.2.2 Rumusan Masalah Minor

1. Langkah apa saja yang telah dilakukan ASEAN *Regional Forum* (ARF) dalam penanganan *Cyber Terrorism* di Asia Tenggara tahun 2012-2017 ?
2. Kendala apa saja yang di alami oleh ASEAN *Regional Forum* (ARF) Dalam Penanganan *Cyber Terrorism* di Asia Tenggara tahun 2012-2017 ?
3. Bagaimana hasil dari upaya ASEAN *Regional Forum* (ARF) dalam penanganan *Cyber Terrorism* di Asia Tenggara tahun 2012-2017 ?

1.2.3 Pembatasan Masalah

Peneliti akan membatasi masalah penelitian pada saat lagi maraknya kasus *cyber crime* dan *cyber Terrorism* di Asia Tenggara yang terjadi pada tahun 2012. Masa waktu yang dipilih yaitu tahun 2012-2017, dikarenakan pada tahun 2012-2013 di Asia, khususnya Asia tenggara mengalami kejadian atau mengalami serangan cyber tertinggi untuk pertama kalinya, dan pada tahun 2014-2015 ancaman *cyber Terorism* ini menjadi sangat banyak dan terjadi pelanggaran dalam penggunaan *ICT*, sedangan 2016-2017 peneliti hanya meneliti apakah upaya ASEAN *Regional Forum* ini berhasil atau tidak dalam penanganan *cyber Terorism* di Asia Tenggara. Dengan demikian peneliti lebih terfokus dalam meneliti dan membahas masalah tersebut.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Maksud penelitian ini ingin mengetahui bagaimana upaya ASEAN *Regional Forum* dalam penanganan *Cyber Terorism* di Asia Tenggara, serta apa saja kendala serta hasil yang di lakukan ASEAN *Regional Forum* dalam penanganan *cyber Terorism* di Asia Tenggara.

1.3.2 Tujuan Penelitian

1. Untuk mengetahui ancaman *Cyber Terrorism* yang ada di Asia Tenggara.
2. Untuk mengetahui upaya yang di lakukan ASEAN *Regional Forum* dalam menghadapi *Cyber Terrorism*.

3. Untuk mengetahui hasil dari upaya ARF dalam bidang *cyber terorism* di Asia Tenggara.

1.4 Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Penelitian ini di harapkan dapat berguna untuk memperkaya pengetahuan mengenai peran suatu organisasi serta pengetahuan bagaimana sebuah ancaman *cyber* sangat dapat berpengaruh besar bagi suatu negara baik dalam hal positif maupun negatif.

1.4.2 Kegunaan Praktis

1. Hasil penelitian ini diharapkan dapat berguna sebagai tambahan informasi dan referensi bagi para pemerhati masalah-masalah *Cyber Terrorism*, khususnya penstudi Ilmu Hubungan Internasional yang menaruh minat terhadap Kawasan Asia Tenggara dan Indonesia.
2. Diharapkan juga memberikan informasi serta kajian lanjutan bagi para mahasiswa Hubungan Internasional.