

BAB II

TINJAUAN PUSTAKA DAN KERANGKA PEMIKIRAN

2.1 Tinjauan Pustaka

2.1.1 Hubungan Internasional

Hubungan internasional adalah interaksi antar aktor sosial dalam menjalin hubungan sosial yang melintasi batas-batas negara, baik itu aktor negara maupun non-negara. Setiap aktor memiliki maksud dan tujuan tujuannya masing-masing dalam melakukan tindakan maupun menjalin suatu hubungan tertentu (Spindler, 2013).

Secara terminologis, istilah Hubungan Internasional diprakarsai oleh seseorang yang memiliki ketertarikan besar terhadap isu-isu hubungan antar negara yaitu Jeremy Bentham. Cakupan dalam hubungan internasional yaitu segala bentuk hubungan antar bangsa dan kelompok-kelompok bangsa dalam masyarakat dunia, berbagai macam kekuatan, tekanan serta proses yang menetapkan cara hidup, cara bertindak serta cara berpikir manusia (Darmayadi et al., 2015).

Robert H.Jackson dan Georg Sorensen berpendapat bahwa studi Hubungan Internasional adalah studi yang mempelajari hubungan dan interaksi antarnegara, mencakup segala bentuk aktivitas dan berbagai kebijakan pemerintah nasional, organisasi internasional (IGO), organisasi non-pemerintah (NGO) dan perusahaan multinasional (MNC). Ditegaskan pula bahwa Hubungan Internasional tidak hanya mengenai hubungan atau interaksi antar negara tetapi juga aktor non-negara (Bakry, 2017).

Menurut Juliet Kaarbo dan James Lee Ray, *Global Politics* lebih merepresentasikan pada latar belakang historis dan teoritis dalam memahami kompleksitas hubungan internasional kontemporer. Globalisasi menjadi salah satu faktor penting yang berpengaruh terhadap hubungan antar negara dan aktor-aktor non-negara saat ini, isu-isu terkait integrasi regional, konflik etnis, norma-norma internasional, isu lingkungan, serta ancaman terhadap kedaulatan negara (Bakry, 2017).

Hubungan Internasional kontemporer ditandai dengan meluasnya cakupan yang dapat ditelaah, mengkaji perilaku berbagai aktor dalam arena hubungan internasional. Perilaku atau tindakan dalam praktiknya dapat berupa perang, konflik, kerjasama, pembentukan aliansi, interaksi dalam organisasi dan interaksi lainnya (Ikbar, 2014).

2.1.2 Organisasi Internasional

Organisasi Internasional sebagai salah satu aktor dalam hubungan internasional, maka keberadaannya akan mempengaruhi kebijakan luar negeri negara anggotanya. Kebutuhan untuk berpartisipasi seakan menarik kearah perubahan dalam perilaku politik luar negeri serta proses pembuatan kebijakan negara anggota (Ikbar, 2014: 240).

Organisasi internasional merupakan sebuah seni untuk mewujudkan dan mengatur masyarakat luas yang terdiri dari beberapa negara merdeka guna mempermudah dalam menjalin kerjasama untuk mencapai tujuan bersama. Menurut Coulumbia dan Wolfe, organisasi internasional merupakan sebuah proses

untuk mewujudkan suatu pengaturan dalam menjalin hubungan antar negara dan non-negara (Ikbar, 2014: 240).

Menurut Michael Haas, memiliki dua pengertian mengenai organisasi internasional. Pertama, organisasi internasional sebagai suatu Lembaga atau struktural yang memiliki serangkaian aturan, anggota, jadwal, tempat dan waktu pertemuan. Kedua, organisasi internasional adalah pengaturan bagian-bagian menjadi kesatuan utuh serta tidak adanya aspek non-lembaga (Ikbar, 2014: 241).

Cheever dan Haviland Jr, mendefinisikan organisasi internasional sebagai pengaturan bentuk kerjasama internasional yang melembaga antar negara-negara, berdasarkan kesepakatan pertama untuk menjalankan fungsi-fungsi yang bermanfaat timbal balik yang diimplementasikan melalui pertemuan dan aktivitas staf secara berkala (Triwahyuni et al., 2015: 81). Oleh sebab itu, organisasi internasional mencakup tiga unsur yaitu:

- 1) Keterlibatan negara dalam suatu pola kerjasama.
- 2) Pertemuan secara berkala.
- 3) Staf sebagai pegawai sipil internasional (*international civil servant*).

Menurut Thomas L.Karnes (1961) Adapun syarat-syarat dalam mendirikan organisasi internasional antara lain (Triwahyuni, 2010):

- 1) Terdapat perwakilan resmi pemerintah.
- 2) Konsentrasi negara pada upaya pengembangan struktur pemerintahan.
- 3) Nasionalisme bukan menjadi ciri utama dari setiap negara partisipan.
- 4) Setiap negara anggota memiliki kepentingan bersama.

Adapun ciri-ciri organisasi internasional yang dikemukakan oleh Leroy Bennet yaitu sebagai berikut (Made & Dana, 2021):

- 1) Organisasi bersifat permanen untuk melakukan fungsinya secara konstan.
- 2) Keanggotaan bersifat sukarela bagi peserta yang memenuhi syarat.
- 3) Memiliki instrumen dasar yang menyatakan tujuan, struktur dan metode operasional.
- 4) Memiliki organ yang bersifat konsultatif.
- 5) Sekretariat tetap untuk melaksanakan fungsi administrasi, penelitian dan informasi secara berkelanjutan.

2.1.3 Kerjasama Internasional

Kerjasama internasional adalah bentuk hubungan yang dilakukan oleh suatu negara dengan negara lain yang bertujuan untuk memenuhi kebutuhan rakyat dan untuk kepentingan negara-negara di dunia. Kerjasama internasional meliputi kerjasama dibidang politik, sosial, pertahanan, kebudayaan, dan ekonomi berpedoman pada politik luar negeri masing-masing negara (Ikbar, 2014: 273).

Kerjasama internasional menurut Keohane dapat dilihat sebagai upaya negara untuk memenuhi kebutuhannya dalam sistem internasional. Pada dasarnya kerjasama seharusnya mengarah pada keuntungan yang akan diperoleh negaranegara yang melakukannya. Serupa dengan konflik, kerjasama juga harus melibatkan dua negara atau lebih (Unsi, 2019: 11).

Menurut Koesnadi Kertasmita, bahwa kerjasama internasional bukan hanya dilakukan antar negara secara individual saja, akan tetapi juga dilakukan antar

negara yang bernaung dalam organisasi ataupun lembaga internasional. Selain itu, menurut beliau kerjasama internasional merupakan suatu bentuk keharusan sebagai akibat dari adanya hubungan interdependensi dan bertambahnya kompleksitas kehidupan manusia dalam masyarakat internasional (Oktaviani, 2022: 9).

2.1.4 Kepentingan Nasional

Kepentingan nasional merupakan suatu hal yang vital bagi setiap negara, karena pada dasarnya eksistensi sebuah negara dituntut untuk senantiasa memenuhi kepentingan nasionalnya. Sebagaimana yang dikemukakan oleh Hans J. Morgenthau dalam bukunya yang berjudul *Politics Among Nations* mengenai kepentingan nasional sebagai kemampuan minimum negara-bangsa untuk melindungi identitas fisik (wilayah, teritorial), identitas politik (rezim ekonomi politik) dan identitas kultural (norma etnis, historis, linguistik) dari gangguan negara lain (Rijal, 2018: 162).

Menurut Jack C. Plano dan Roy Olton, kepentingan nasional didefinisikan sebagai untuk meraih kekuasaan dan mempertahankannya dengan tindakan-tindakan politik. Pada penuturannya disebutkan terdapat beberapa elemen dalam kepentingan nasional, yaitu *self preservation* (pertahanan diri), *independence* (kemerdekaan, kemandirian), *territorial integrity* (integritas wilayah), *military security* (keamanan militer) dan *economic well-being* (kesejahteraan ekonomi) (Rijal, 2018: 162).

Sedangkan, Paul Seabury mendefinisikan kepentingan nasional melalui dua sudut pandang yaitu secara deskriptif yang berarti sebagai tujuan yang harus dicapai

oleh suatu negara secara tetap melalui kepemimpinan pemerintah. Secara normatif, kepentingan nasional diartikan sebagai himpunan cita-cita dari suatu negara yang harus diperjuangkan dengan cara menjalin hubungan antar negara (Putro Sudarsono et al., 2018: 89).

Felix E. Oppenheim (1987) mengemukakan konsep kepentingan nasional sebagai tujuan mencapai kesejahteraan pemerintahan nasional pada skala internasional. Pendapat Daniel S.Papp menyatakan bahwa kepentingan nasional terdiri dari beberapa aspek, yaitu kepentingan ekonomi, ideologi, kekuatan dan keamanan militer serta moralitas dan legalitas (Syukran & Ubaidullah, 2019).

Kepentingan nasional merupakan suatu hal dasar yang menjadi tujuan atau cita-cita suatu negara dan menjadi faktor mendasar yang mempengaruhi arah kebijakannya sebagai upaya untuk mencapai kesejahteraan nasional, yang dimana negara perlu menjalin interaksi antar negara dan menciptakan hubungan kerjasama karena negara tidak dapat berjalan sendiri dalam upaya mencapai kepentingan nasionalnya.

2.1.5 Keamanan

Pendekatan tradisional yang didominasi perspektif realisme menyatakan bahwa konsep keamanan merupakan sebuah kondisi yang terbebas dari ancaman militer atau kemampuan suatu negara untuk melindungi negara bangsanya dari serangan militer yang berasal dari lingkungan eksternal. Berakhirnya Perang Dingin memunculkan perkembangan baru dalam kajian Keamanan Internasional. Pada era keemasan pertama dan kedua, fokus utama kajian Keamanan Internasional

mengarah pada instrumen penggunaan kekerasan oleh negara. Perkembangan memunculkan perdebatan dalam baru mendefinisikan konsep keamanan (Wardoyo, 2015).

Sejalan dengan perkembangan yang begitu cepat dalam hubungan internasional, menurut Barry Buzan yang disebut sebagai *the widening Schooll the widerner*, keamanan berkaitan erat dengan isu keberlangsungan hidup (*survival*). Isu-isu eksistensial yang mengancam keberlangsungan hidup perlu di prioritaskan. Buzan membagi isu keamanan pada lima dimensi yaitu politik, militer, ekonomi, sosial dan lingkungan. Setiap diemensi memiliki unit keamanan, nilai, karakteristik *survival* dan ancaman yang berbeda (Ikbar, 2014: 200).

Terdapat lima dimensi yang dapat dijadikan sudut pandang untuk memahami perkembangan konsep keamanan, yaitu (Agung Banyu Perwita, 2008: 11):

- 1) *The Origin of Threat*, pada masa Perang Dingin, ancaman yang dihadapi berasal dari pihak eksternal atau luar negeri maka dewasa ini, ancaman dapat berasal dari internal dan eksternal negara. Ancaman dari internal negara seperti konflik antar kelompok atau masyarakat.
- 2) *The Nature of Threats*, tradisional menilik ancaman dari sudut pandang militer, sedangkan globalisasi menjadikan isu keamanan lebih kompleks dan sifat ancaman yang lebih rumit karena berkaitan dengan isu-isu ekonomi, sosial, budaya, lingkungan hidup, bahkan isu demokratisasi dan HAM.
- 3) *Changing Response*, apabila pada konsep tradisional respon yang muncul adalah tindakan militer, maka dewasa ini dalam merespon isu keamanan

diperlukan menggunakan pendekatan non-militer seperti ekonomi, politik, hukum, sosial dan budaya.

- 4) *Changing of Responsibility of Security*, ketika negara tidak lagi menjadi aktor tunggal yang bertanggung jawab atas keamanan rakyat, maka keamanan bergantung peranan seluruh individu pada tatanan global.
- 5) *Core Values of Security*, fokus utama keamanan bukan lagi nilai-nilai tradisional seperti kedaulatan dan integritas territorial, tetapi muncul nilai-nilai baru seperti penghormatan pada HAM, demokratisasi, perlindungan lingkungan hidup, kejahatan lintas batas, *money laundering* dan terorisme.

2.1.5.1 Keamanan Siber

Perkembangan teknologi informasi dan komunikasi berpengaruh terhadap pergeseran konsep keamanan, dampak dari teknologi yang menghadirkan dimensi baru yaitu ruang siber. Peluang dan tantangan baru mesti dihadapi negara, adaptasi pada setiap perubahan menjadi konsekuensi negara. Munculnya ancaman keamanan baru menuntut negara untuk mengeksplorasi dan meningkatkan kapabilitasnya di bidang teknologi. Keamanan *cyber* mencakup segala sesuatu berhubungan dengan pengawasan komputer, monitoring sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental (Triwahyuni & Wulandari, 2016: 111).

Cyber security atau keamanan siber berfungsi atau berperan untuk mengatasi, mendeteksi, menemukan, menangkal ataupun meminimalisasi tingkat resiko terjadinya gangguan, ancaman (*cyber threat*) dan serangan siber (*cyber*

attack) serta seluruh aktifitas teknologi siber yang mengancam keamanan seluruh komponen sistem siber itu sendiri yang meliputi *hardware*, *software*, data atau informasi maupun infrastruktur (Siagian et al., 2018: 5).

Konflik di dunia *cyber* tidak hanya dilakukan oleh aktor negara karena teknologi dapat dikendalikan oleh siapa saja, termasuk aktor transnasional seperti kelompok terorisme. Potensi konflik tidak lagi muncul secara fisik lagi. Sehingga mau tidak mau, negara sebagai entitas yang menaungi jutaan manusia perlu meningkatkan awareness dan keamanan *cyber* mereka. Menurut Arquilla dan Ronfeldt bahwa peningkatan teknologi sebuah negara ikut memicu munculnya potensi konflik baru yang mana salah satunya adalah *cyber war* (Ramadhan, 2017: 498).

2.1.6 Kejahatan Siber

Menurut Gregory *Cybercrime* atau kejahatan siber adalah suatu bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung ke internet, dan mengeksploitasi komputer lain yang terhubung dengan internet juga. Adanya celah-celah keamanan pada sistem operasi menyebabkan kerentanan dan terbukanya peluang yang dapat digunakan para *hacker*, *cracker* dan *script kiddies* untuk menyusup ke dalam komputer tersebut (Hasmono, 2021: 2).

Sedangkan menurut Kepolisian Inggris Tahir, *Cyber Crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. Kemudian menurut Tavani definisi *Cybercrime*, yaitu kejahatan dimana tindakan

kriminal hanya bisa dilakukan dengan menggunakan teknologi *cyber* dan terjadi di dunia *cyber* (Hardianti et al., 2022: 11).

Dari penjelasan di atas, dijelaskan bahwa *cybercrime* adalah salah satu bentuk kejahatan. Beberapa dari bentuk *cybercrime* merupakan bentuk kejahatan konvensional seperti penipuan, pencurian, pornografi, pencemaran nama baik yang ditransformasikan ke dalam *cyberspace*. Namun beberapa bentuk *cybercrime*, yang lain seperti *cyber espionage*, *cyber sabotage and extortion*, *cracking* merupakan bentuk kejahatan yang tidak ditemukan di *real space*, karena hanya dapat direalisasikan dengan alat dan perangkat yang ada dalam *cyberspace* (Tampubolon, 2019: 545).

Kompleksitas kejahatan siber pada praktiknya dikelompokkan dalam beberapa bentuk, antara lain (Maskun, 2013: 51):

- 1) *Unauthorized access to computer system and service*, merupakan segala bentuk tindakan yang dilakukan ke dalam sistem operasi atau jaringan komputer secara ilegal.
- 2) *Illegal contents*, merupakan suatu kejahatan dengan memanipulasi data atau informasi ke jaringan internet, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban publik.
- 3) *Data forgery*, merupakan tindakan pemalsuan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui jaringan internet. Dokumen-dokumen *e-commerce* menjadi sasaran utama pelaku kejahatan *data forgery*.

- 4) *Cyber espionage*, merupakan tindak kejahatan melalui jaringan internet untuk memata-matai pihak lain dengan cara memasuki sistem jaringan komputer target.
- 5) *Cyber sabotage and extortion*, merupakan tindak kejahatan dengan mengirimkan gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan yang tersambung dengan koneksi internet. Biasanya menyusupkan suatu *logic bomb*, virus atau program tertentu pada komputer.
- 6) *Offence against intellectual property*, merupakan tindakan kejahatan yang ditujukan pada hak kekayaan intelektual seseorang di internet. Seperti peniruan tampilan *web page* suatu situs secara illegal, penyiaran informasi rahasia seseorang, hak paten atau sebagainya.
- 7) *Infringements of privacy*, merupakan tindakan kejahatan yang ditujukan pada informasi pribadi seseorang yang tersimpan secara komputerisasi yang dapat merugikan secara materiel dan imateriel, seperti nomor kartu kredit, nomor PIN ATM atau informasi data pribadi lainnya.

2.1.7 Information and Communication Technology (ICT)

Era informasi menjadi era baru setelah kemunculan teknologi informasi dan komunikasi. Adaptasi penerapan ICT pada berbagai sektor secara bertahap telah menimbulkan ketergantungan kepada negara industri maju sehingga penguasaan ICT oleh setiap negara menjadi penting sebagai upaya untuk mempertahankan eksistensinya. Kekuatan ICT yang baik di negara akan meningkatkan interaksi antar

masyarakatnya, sehingga berdampak pada peningkatan efisiensi dan efektivitas industri, finansial dan militer suatu negara. Dalam kajian hubungan internasional penguasaan ICT dapat memfasilitasi suatu negara dalam mendistribusikan *power* dan *influence* ke segala penjuru dunia. Akan tetapi, kesenjangan kapabilitas penguasaan ICT antara negara maju, negara berkembang dan tertinggal mengakibatkan terjadinya hubungan yang asimetris (Putri et al., 2015: 130).

Pengaruh perkembangan ICT yang pesat tak dapat dielakkan lagi, internet sebagai infrastruktur penting dalam pemanfaatan ICT, transformasi digital menjadi agenda prioritas pembangunan negara. Selama dekade terakhir aktivitas ekonomi telah banyak bergantung pada dukungan ICT yang memberikan kemudahan dalam bertransaksi. Begitupula penerapan ICT pada sektor pemerintahan dapat memperluas sasaran dan strategi organisasi serta dapat meningkatkan efektivitas kerja dan kepuasan layanan publik (Moenardy & Chandra, 2021: 41).

Perkembangan ICT memberikan peluang baru bagi pemerintah untuk memanfaatkannya guna mencapai efisiensi, efektivitas, transparansi, dan akuntabilitas kinerja pemerintah dalam pengelolaan pemerintahan, sehingga tercapai lebih banyak pelayanan pemerintah kepada masyarakat. Penyelenggaraan pemerintahan dengan menggunakan Teknologi Informasi dan Komunikasi dikenal dengan Electronic Government atau E-Government.

2.1.8 Blockchain

Web 3.0 adalah tahap perkembangan generasi ketiga dari internet yang memberikan otonomi kepada penggunanya di samping menjanjikan pengalaman

yang mendalam, tema sentral dari web 3.0 adalah desentralisasi salah satu sistem informasi yang cerdas. Ketika menginput sebuah informasi maka mesin akan memproses secara otomatis sehingga kecil kemungkinan terjadi penyalahgunaan data (Gupta, 2022: 35). Blockchain merupakan salah satu *leading technology* di era generasi web 3.0 terutama yang berfokus pada sistem desentralisasi, yang sebenarnya adalah sebuah buku besar digital yang dapat diakses publik untuk menyimpan dan mentransfer data atau informasi tanpa adanya otoritas pusat atau perantara.

Blockchain merupakan basis data terdistribusi (*distributed ledger*) yang tersimpan dalam blok-blok terenskripsi yang saling berkaitan satu sama lain dengan kode-kode unik yaitu menggunakan tanda tangan kriptografi atau fungsi *hash* yang bersifat kekal dan tidak dapat diubah. Blok adalah kapasitas penyimpanan informasi atau data tertentu dan ketika diisi, ditutup dan ditautkan ke blok yang diisi sebelumnya akan membentuk rantai data yang dikenal dengan Blockchain. Setiap blok mengacu pada rantai blok sebelumnya sehingga dapat meminimalisir kemungkinana adanya modifikasi data yang tidak diinginkan (<https://101blockchains.com/blockchain-concepts/> diakses pada 8 Mei 2022).

Berikut adalah jenis-jenis Blockchain, yaitu:

- 1) Blockchain Privat, sistem blockchain ini dikembangkan dan dikelola oleh organisasi swasta yang memiliki otoritas atas proses penambangan dan algoritma consensus. Dapat ditentukan siapa saja yang memiliki akses untuk masuk kedalam jaringan dan mengunduh node.

- 2) Blockchain Konsorsium, kepemilikan akses oleh beberapa pihak, sistem jaringan semi-privat dan memiliki grup pengguna yang terkontrol, tetapi bekerja diberbagai organisasi
- 3) Blockchain Publik, sistem terbuka untuk semua orang. Sistem jaringan menggunakan algoritma consensus untuk memvalidasi transaksi.

2.2 Kerangka Pemikiran

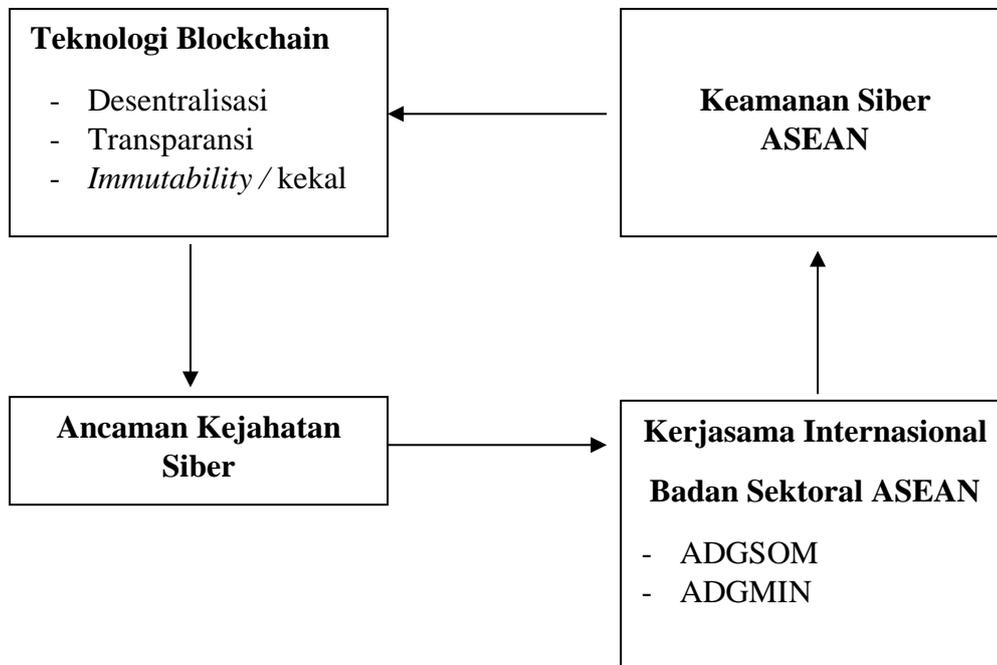
Perkembangan globalisasi mempengaruhi kajian dalam hubungan internasional dengan cakupan yang lebih luas dan pergeseran makna konsep keamanan. Munculnya dimensi baru yaitu ruang siber yang menjadi arena baru dalam melakukan hubungan internasional tentu tidak terlepas dari ancaman keamanan, maka dari itu isu keamanan menjadi tanggung bersama. Pudarnya lintas batas negara pada aktivitas di ruang siber memunculkan resiko yang cukup signifikan. Disisi lain, perkembangan teknologi banyak menunjang berbagai sektor industry dan pelayanan publik yang meningkatkan efektivitas kerja. Perkembangan ICT dan jumlah penetrasi internet yang terus meningkat menimbulkan dilematis tersendiri.

Ancaman kejahatan siber menjadi salah satu tantangan regional yang paling signifikan bagi kepentingan bersama untuk negara-negara anggota ASEAN. Kejahatan siber menjadi tantangan baru disebabkan karena meningkatnya volume dan kompleksitas ancaman yang ditimbulkan, kurangnya kesadaran masyarakat dan terbatasnya regulasi khusus yang mengatur terkait aktivitas di ruang siber.

Peningkatan kerjasama dibidang informasi dan komunikasi terus dilakukan sebagai upaya pencegahan resiko ancaman siber yang ditimbulkan dari mengadopsi teknologi baru. Pembentukan ADGSOM dan ADGMIN sebagai badan khusus untuk monitoring dan evaluasi perkembangan, peluang dan resiko implementasi teknologi blockchain dalam proses transformasi digital untuk mengoptimalkan keamanan siber di ASEAN.

Pertahanan keamanan siber perlu ditingkatkan dari waktu ke waktu seiring dengan laju perkembangan teknologi informasi dan komunikasi. Sebagai upaya menanggulangi serangan siber yang dapat mengganggu aktivitas di ruang siber. Akselerasi revolusi industri menuntut untuk mampu beradaptasi dengan segala bentuk inovasi media baru.

Blockchain sebagai teknologi yang mengusung sistem *database* terdesentralisasi dan terdistribusi dimana transaksi dicatat dengan tanda tangan kriptografi yang tidak dapat diubah. Menjadi suatu hal yang dibutuhkan untuk menjamin keamanan data dan informasi.



Bagan 2. 1 Alur Kerangka Pemikiran

Sumber: Diolah peneliti