BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era revolusi industri 4.0 ini, peran teknologi mulai mendominasi dalam segala aspek kehidupan dan bernegara. Proses digitalisasi telah menjadikan interaksi dan hubungan antar negara lebih mudah sehingga mengakibatkan kerap terjadi praktik-praktik spionase dalam tingkat yang lebih masif jika diperbandingkan dengan spionase yang dilakukan secara konvensional.

Spionase secara konvensional yang telah dilakukan oleh negara-negara di dunia dari abad-keabad mempunyai pengertian yang diambil dari bahasa Perancis yaitu memata-matai, mengintai berbagai informasi penting tentang perkembangan negara dan pemerintahan suatu negara dengan sembunyi dan tanpa izin pemiliknya.[1] Dewasa ini spionase berkembang dengan adanya teknologi dan alat komunikasi yang telah menjamah segala lini termasuk pemerintahan, militer dan masyarakat dimana spionase dalam masa ini dilakukan dengan bantuan jaringan komputer. Praktik spionase yang dilakukan melalui jaringan komputer dan menggunakan *server proxy* atau kerap dikenal sebagai *cyber espionage.*

Cina merupakan negara yang kerap diberitakan menjadi negara pelaku *cyber espionage*, negara ini telah menjadi negara yang kerap menggunakan praktik *cyber espionage* sebagai upaya untuk mengembangkan negaranya di bidang militer

[1] L. Ya Esty Pratiwi, 'Hukum Siber : Praktik Spionase Dalam Kedaulatan Negara dan Hubungan Diplomasi Berdasarkan Ketentuan Hukum Internasional', Jurnal Pendidikan Kewarganegaraan Undiksha, Vol.8 No.3, 2020.

dan pertahanan.[2] Negara ini mendapat keuntungan yang sangat banyak dalam perkembangan di bidang militer dengan mencuri dan mengintai beberapa informasi terkait perkembangan sistem persenjataan dari pusat persenjataan Amerika yaitu Pentagon Informasi yang didapat oleh Cina termasuk perkembangan terbaru dari teknologi pesawat tempur dan kapal selam tanpa awak.[3] Pentagon melaporkan hal tersebut pada tahun 2013, Cina tidak hanya mengumpulkan data militer tetapi data-data intelijen, diplomatik bahkan ekonomi juga termasuk dalam daftar sasarannya.[4]

Contoh kasus lain yang baru saja terjadi adalah antara Cina, Iran dan Amerika. Pada bulan Januari 2019, intelijen Amerika Serikat melaporkan bahwa jaringan pemerintahan dan beberapa perusahaan di AS telah di monitor dan diserang oleh Cina dan Iran.[5] Kedua negara tersebut terhubung dengan aktivitas *cyber espionage* seperti pencurian informasi pemerintahan dan memberi pengaruh kepada masyarakat Amerika Serikat dalam pemilihan presiden yang akan diadakan di tahun 2020. Kelompok *hackers* bernama Zirconium dari Cina ini telah menarget beberapa individu, instansi akademis dan institusi publik untuk diintai. Perbuatan Cina terhadap Amerika berawal dari perang dagang Amerika dengan Cina yang

[2] Christopher Bing, "U.S. cybersecurity experts see recent spike in Chinese digital espionage", www.reuters.com , 25 Maret 2020, dikunjungi pada tanggal 27 Maret 2021.

[3] *Ibid*.

[4] Elizabeth Radzisewski, "India's Response to China's Cyber Attacks", www.thediplomat.com 3 Juli 2019, dikunjungi pada tanggal 5 April 2021.

[5] Michael Frank, "China Espionage against United States",https://ge.usembassy.gov , 9 Juli 2020, dikunjungi pada tanggal 10 Oktober 2020.

telah berlangsung sejak kebijakan luar negeri Presiden Donald Trump dalam memberikan tarif yang sangat tinggi terkhususnya kepada negara tirai bambu tersebut.[6] Iran sebagai negara yang sudah sejak lama berseteru dengan Amerika Serikat dan ditambah lagi dengan mundurnya Amerika Serikat dari *Joint Comprehensive Plan of Action* atau bisa disebut *Iran Nuclear Deal* yang membuat Iran geram dan memutuskan untuk melancarkan misi spionase dengan mencuri berbagai data kekayaan intelektual dari perusahaan-perusahaan besar di Amerika guna menjualnya di Iran lagi.[7] Di Benua Asia, negara kecil seperti Vietnam pun juga tidak luput dalam penggunaan praktik *cyber espionage*. Pada tahun 2017, pemerintah Vietnam telah meretas jaringan pemerintahan filipina guna mendapatkan transkrip percakapan antara Donald Trump dan Presiden Filipina Rodrigo Duterte yang kemudian diunggah di Internet melalui *e-mail* ilegal dari Vietnam.[8] Dilaporkan Bahwa dibalik peretasan ini adalah kelompok peretas profesional yaitu APT32 atau OceanLotus Group yang merupakan salah satu unit dari pemerintahan Vietnam yang ditugaskan khusus untuk melakukan spionase terhadap dua negara tersebut.[9]

---

[6] *Ibid*.

[7] "Publicly Reported Iranian Cyber Actions in 2019", www.csis.org , h. 2, dikunjungi pada tanggal 10 Oktober 2020.

[8] Chris Bing,"A Stolen Trump-Duterte transcript appears to be just one part of alarger hacking story", www.cyberscoop.com , 31 Mei 2017, dikunjungi pada tanggal 10 Oktober 2020.

[9] Joe Uchill, "Vietnam-backed hackers used Philippine president's website for attacks: report", www.thehill.com , 11 Maret 2017, dikunjungi pada tanggal 27 Maret 2021.

Sebelum Montenegro bergabung ke NATO di 2017, APT28 atau terkenal dengan nama "Fancy Bear", kelompok peretas ternama yang terhubung dengan unit intelijen pemerintahan Rusia.[10] Operasi militer siber yang dilakukan oleh Rusia terhadap Montenegro dilakukan guna mencampuri urusan politik dalam negeri negara tersebut. Dua *booby-trap files* dikirim melalui *e-mail* yang berguna untuk menggapai akses ke komputer yang akan ditarget, mengeksfiltrasi data dan fasilitas pengawasan.

Bisa dilihat bahwa aktivitas *cyber espionage* atau memasuki jaringan siber suatu negara secara tidak sah serta mengambil data dan informasi sensitif milik negara tersebut telah menimbulkan banyak kerugian bagi negara yang mengalaminya. Kerugian yang diterima bisa dalam bentuk ekonomi melihat beberapa arsip rahasia seperti data kekayaan intelektual dan data mengenai peluang merger dan akuisisi suatu perusahaan-perusahan dalam negeri yang dapat diketahui oleh pihak lain, pada akhirnya berdampak pada kondisi perekonomian suatu negara. Dengan adanya praktik tersebut beberapa strategi dan langkah kebijakan suatu negara dapat diketahui oleh negara lain mengakibatkan timbulnya dampak yang sangat signifikan terhadap berjalannya suatu negara. Dengan dampak yang sangat nyata diakibatkan dari aktivitas ini, banyak negara masih belum melihat pentingnya untuk mengatur *cyber espionage* dalam sekala yang lebih rinci dan global. Bentuk toleransi dari negara-negara di dunia masih sangat tinggi mengingat banyak nya

[10] Dusica Tomovic,"A notorious Russian cyber-espionage group is believed to have been behind a number of attacks targeting Montenigrin Institutions in the last year", www.balkaninsight.com ,5 Maret 2018 , dikunjungi pada tanggal 10 Oktober 2020.

kasus yang muncul atas aktivitas spionase ini, karena pada dasarnya negara-negara telah melakukan spionase maupun spionase melalui siber dari zaman dahulu sehingga timbul kondisi dimana praktik tersebut dianggap tidak menyalahi aturan dan norma.

Perkembangan dunia yang sangat cepat menuntut hukum internasional untuk lebih dinamis dalam beradaptasi dalam memberi koridor yang jelas mengenai perilaku dan hal-hal yang terjadi antar negara melalui medium apapun itu. Apakah *cyber espionage* termasuk kedalam *cybercrime* dan bagaimana hukum internasional telah mengatur kegiatan tersebut. Eoghan Casey[11] seorang profesional dan peneliti dalam bidang kejahatan digital mendefinisikan *cybercrime* sebagai "*cybercrime is referred to any crime that involves computer and networks, including crimes that do not rely heavily on computer*".

Satu definisi umum yang dapat digunakan guna mengidentifikasi suatu tindakan siber adalah dimana aktivitas yang menggunakan komputer dan jaringan internet untuk melaksanakan suatu tindakan kriminal.[12] Terminologi *cybercrime* bisa digunakan untuk mencakup beberapa tindakan kriminal, salah satu pendekatan untuk memahami *cybercrime* juga bisa ditemukan dalam *Budapest Convention on Cybercrime* yang mengklasifikasikan ada empat tipologi dan bentuk dalam kejahatan; pelanggaran terhadap kerahasiaan, integritas dan ketersediaan data dan

[11] Eoghan Casey, 'Digital Evidence and Computer Crime', Elsevier, Maryland, USA, 2011. Hlm. 145

[12] Marco Gercke, 'Understanding Cybercrime: Phenomena, challenges and legal response', Elsevier,Jenewa, Swiss, September 201, h 256.

sistem komputer, pelanggaran terkait komputer, pelanggaran terkait konten dan pelanggaran terkait hak cipta.[13] Dengan beberapa variabel-variabel tersebut dapat dilihat beberapa unsur yang memungkinkan untuk diidentifikasi dalam praktik *cybercrime*.

Dalam lingkup hukum internasional, spionase antar negara sudah sangat lazim dan kerap dilakukan oleh negara. Praktik spionase antar negara sudah dilakukan bahkan dari zaman Mesir kuno sampai sekarang, sehingga kebiasaan dalam melakukan hal seperti ini akan sangat lazim bila di lakukan. Menurut Handar S[14], spionase diartikan sebagai kegiatan memata-matai yang melibatkan pemerintah atau individual saja guna mendapatkan informasi rahasia penting tanpa izin pemiliknya. Hukum internasional telah lama mengatur mengenai spionase yang dilakukan dalam masa perang tetapi sangat jarang membahas mengenai spionase dalam masa damai.[15] Dalam pengaturannya dalam masa perang, berbagai konvensi internasional seperti *Hague Convention IV 1907* pasal 29 hingga 31 termasuk pendapat ahli seperti Hugo Grotius menjadikan kegiatan spionase sebagai tindakan yang dapat dilakukan oleh suatu negara.[16]

---

[13] *Ibid*.

[14] Rofi'a Zulkarnain,'Tindakan Spionase Melalui Penyadapan Antar Negara Sebagai Cybercrime', **Tesis**, Fakultas Hukum Universitas Brawijaya, Malang, 2019, h.2

[15] David Wallace, 'Peeling Back the Onion of Cyber Espionage after Tallin 2.0', Maryland Review Volume 78 Issue 2 Article 2, 2019. h. 17

[16] *Loc.cit*, Rofi'a, h.4

The Summit Declaration of Brussels menyatakan bahwa penggunaan sarana intelijen dalam agenda berkenaan dengan negara musuh dianggap sah dalam perang.[17] Pasal 46 dalam Konvensi Den Haag 1907 memberikan prosedur tentang penanganan mata-mata yang tertangkap, pasal ini sudah diterima oleh hukum internasional selama seratus tahun lebih.[18] Kosongnya pengaturan mengenai spionase dalam masa damai menjadikan polemik, Quincy Wright[19] mencatat bahwa dalam masa damai, penyusupan ke dalam wilayah teritorial suatu negara dengan menggunakan agen dari negara lain yang melanggar hukum setempat juga bisa dianggap melanggar aturan hukum internasional. Aturan ini untuk memberlakukan kewajiban kepada negara untuk menghormati integritas teritorial dan kemerdekaan politik negara lain. Dalam putusan *Permanent Court of International Justice* dalam *Lotus Case* menyatakan bahwa pembatasan pertama dan terpenting yang diberlakukan oleh hukum internasional atas suatu negara adalah bahwa jika negara mengabaikan aturan, negara tersebut tidak boleh menjalankan kekuasaannya dalam bentuk apapun di wilayah negara lain.[20] Asas kedaulatan territorial yang menjadi salah satu asas terpenting dalam memberikan penilaian terkait sah atau tidak nya kegiatan *cyber espionage*.

---

[17] Lt. Col. Geoffrey B. Demarest,'Espionage in International law, Denver Journal of International law and Policy', Denver Journal of International Law and Policy, Denver,321, 1991

[18] *Ibid.*

[19] *Ibid*.

[20] Russel Buchan, 'Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary',Cornell International Law Journal,2019, hal.901

Menurut Roger Scott [21] spionase bukan merupakan aktivitas kejahatan karena tidak melanggar asas *jus cogens*. Kemudian pernyataan tersebut dibantah oleh Radsan, [22] beliau mengatakan spionase dalam masa damai merupakan kejahatan internasional dan pelanggaran internasional. Dalam tahap penentuan mengenai apakah spionase termasuk kejahatan atau tidak, ternyata masih banyak banyak inkonsistensi diantara para ahli tersebut sehingga menimbulkan kekaburan hukum dalam aktivitas spionase itu sendiri.[23]

Katharina Zilkowski mempersempit lagi dengan memberikan beberapa contoh aktivitas yang termasuk dalam *cyber espionage* yaitu; pengawasan, pemantauan, menangkap, eksfiltrasi komunikasi elektronik yang dikirim atau disimpan.[24] *Rule* 32 pada Tallin Manual 2.0 menyimpulkan bahwa *cyber espionage* tidak melanggar hukum internasional tetapi bila dalam proses pelaksanaanya ada beberapa aspek pelanggaran terhadap hukum internasional, kegiatan *cyber espionage* tersebut dapat dikatakan melanggar hukum. [25] Contoh sederhana suatu negara dapat melanggar hukum internasional apabila negara pelaku tersebut

---

[21] Luke Pelican,'Peacetime Cyber-Espionage: A Dangerous But Necessary Game',The Catholic University of America,CommLaw Conspectus, 2012

[22] Afsheen John Radsan, The Unresolved Equation of Espionage and International Law, Michigan Journal of International Law, 2007.

[23] *Ibid*.

[24] Benedikt Muller, Cyberspace and International Relations, Springer, 2014, h 16.

[25] Michael N. Schmitt,' Tallin Manual 2.0 International Applicable to Cyberwarfare',Cambridge University Press,New York, 2013

menggunakan pos diplomatik untuk melaksanakan spionase atau *cyber espionage* sekalipun, dimana diatur dalam pasal 2, pasal 3, pasal 27 ayat 1, pasal 42 dalam *Convention on Diplomatic Relations 1961* yang melarang penyalahgunaan wewenang fasilitas diplomatik, penyalahgunaan wewenang seorang diplomat, melakukan intervensi/ikut campur urusan negara lain serta dengan sengaja mengambil informasi negara lain tanpa cara yang sah.[26]

Jangkauan wilayah kedaulatan negara meliputi *cyberspace*, dimana negara berdaulat dalam mengatur kegiatan siber oleh subjek hukum didalam yurisdiksinya.[27] Asas kedaulatan tersebut mungkin dapat dijadikan hambatan bagi *cyber espionage*. Perdebatan diantara ahli seperti Pehlivan dan Michael N. Schmitt masih belum menemukan titik temu untuk menjawab apakah *cyber espionage* merupakan pelanggaran hukum internasional dan merupakan *cybercrime.*

Melihat berbagai kasus yang sudah terjabarkan diatas terlihat bahwa negara bukan satu-satunya aktor dalam tindakan spionase tersebut melainkan banyak dari organisasi siber yang justru beroperasi dalam kegiatan tersebut. Identifikasi peran dalam kegiatan *cyber espionage* menjadi tantangan yang lain dalam dunia internasional. Masih terjadi hambatan yang besar untuk menjadikan berbagai *non-state actor* bertanggungjawab atas tindakan spionase tersebut mengingat yurisdiksi hukum interasional yang masih belum menjangkau berbagai *non-state actor* seperti

[26] Ardellya Mustika Rahiem,'Pertanggungjawaban Negara Australia Terhadap Penyadapan Kepala Negara Republik Indonesia Ditinjau Dari Konvensi Wina 1961', E-Journal Komunitas Yustisia Universitas Pendidikan Ganesha, Vol.3 No.1, 2020, h.5

[27] Harold Hongju Koh,'International Law in Cyberspace',Harvard International Law journal , Vol.4,Desember 2012, h 6

korporasi multinasional, perusahaan dalam negeri dan *non-state terrorist* sebagai subjek hukum internasional.[28] Negara kerap memberikan bantuan dan asistensi bahkan berpartisipasi secara langsung dalam kegiatan tersebut menampik fakta bahwa negara tersebut sendiri telah mengatur mengenai spionase dan bagaimana spionase dilarang di peraturan domestik. Yang menjadi tantangan adalah memastikan negara tersebut mematuhi berbagai aturan yang mereka atur sendiri dan memastikan aturan tersebut dapat di implementasikan secara menyeluruh agar negara tidak terkesan membenarkan kegiatan tersebut. [29]

Meskipun ada urgensi yang tinggi untuk meregulasi isu ini guna memitigasi bahaya dari *cyber espionage,* hukum internasional masih belum bisa mengatasi masalah tersebut. Dengan tidak ada nya traktat yang spesifik mengenai *cyber espionage,* praktik antar negara yang begitu masif masih belum dapat dijadikan sebagai landasan untuk menjadikan kegiatan tersebut kedalam *opinio juris necessitates* yang dimana asas tersebut merupakan suatu keyakinan bahwa suatu tindakan atau kebiasaan dilakukan dengan sesuai dengan kewajiban hukum yang ada.

Kerangka hukum internasional telah tertinggal dengan ritme perkembangan dalam *cyberspace*. Dengan melihat praktik *cyber-espionage* tidak menunjukan tanda untuk mereda, sangat penting untuk tidak hanya melihat kepada hukum dan asas yang berlaku sekarang mengenai praktik ini dengan ada nya kekaburan dan

[28] Jean d'Aspremont, 'Sharing Responsibility Between Non-State Actors and States in International Law:Introduction', Neth International Law Review, Vol 62, No 49-67, 2015.

[29] *Ibid*.

batasan dalam konstruksi hukum tetapi perlu dipertimbangkan hukum yang akan dirancang atau dibentuk dengan tujuan untuk beradaptasi dengan situasi dan kondisi.[30]

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang diatas, rumusan masalah yang akan dibahas dalam penelitian ini adalah sebagai berikut:

1. Bagaimana Hukum Internasional mengatur kegiatan *cyber espionage*?
2. Bagaimanakah pertanggungjawaban negara pelaku aktivitas *cyber-espionage* menurut Hukum Internasional?

1.3 Tujuan Penelitian

Berdasarkan uraian latar belakang diatas, rumusan masalah yang akan dibahas dalam penelitian ini adalah sebagai berikut :

1. Menganalisa dan mengidentifikasi *cyber-espionage* dalam hukum internasional
2. Menganalisa pertanggungjawaban negara pelaku aktivitas cyber-espionage

1.4 Manfaat Penelitian

Dalam proses pelaksanaan penelitian ini, pada akhirnya diharapkan dapat memberikan manfaat;

[30] Katharina Ziolkowski, 'Peacetime Regime for State Activities in Cyberspace', International Law, International Relations and Diplomacy, NATO CCD OE Publication, Tallin 2013, h.178

1. Terhadap civitas akademika Fakultas Hukum Universitas Airlangga diharapkan dapat bermanfaat untuk menganalisa dan memecahkan masalah terkait kekosongan hukum dari *cyber espionage*.
2. Sebagai instrumen untuk memperluas pengetahuan mengenai hukum Internasional dan Hukum Siber.

1.5 Metode Penelitian

1.5.1 Tipe Penelitian Hukum

Metode penelitian yang digunakan dalam penulisan ini adalah doctrinal research yang bertujuan untuk menemukan kebenaran berdasarkan kesesuaian aturan hukum dengan norma hukum, dan dengan asas-asas hukum.[31] Sasaran penelitian doctrinal menyasar ketentuan hukum dimana Penelitian hukum doktrinal diartikan sebagai penelitian menggunakan penjelasan secara sistematis terhadap aturan terkait salah satu kategori hukum, analisa mengenai keterkaitan antar hukum dan menjelaskan bidang kesulitan.

Penelitian ini merupakan jenis penelitian yuridis normatif yaitu penelitian yang difokuskan untuk menganalisa suatu permasalahan hukum terhadap norma-norma atau kaidah-kaidah hukum positif yang berlaku. Jenis pendekatan ini menggunakan ketentuan perjanjian internasional yang berlaku pada suatu negara atau metode hukum doktrinal yaitu teori-teori hukum dan pendapat para ahli terutama dengan permasalahan yang dibahas.[32]

[31] Peter Mahmud Marzuki, *Penelitian Hukum Edisi Revisi*,Prenadamedia Group, Jakarta, 2016, h.47.

[32] Sutrisno Hadi, *Metodology Research* Jilid 1, Yogyakarta, 1998,

Penelitian yuridis normatif dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur-literatur yang berkaitan dengan permasalahan yang diteliti.[33]

1.5.2 Pendekatan Penelitian

Terdapat 2 (dua) macam pendekatan dalam penelitian hukum diantaranya pendekatan konvensi dan perjanjian internasional (*statute approach*), dan pendekatan konseptual (*conseptual approach*).[34]

Namun, dalam penelitian ini, penulis akan menggunakan 2 (dua) jenis pendekatan yakni :

1) Pendekatan perundang-undangan (*statute approach*) dengan cara mengumpulkan segala perjanjian-perjanjian internasional yang telah berlaku dan berkaitan dengan isu hukum dengan melihat keberlakuan dari perjanjian tersebut secara normatif.[35] Dalam hal ini peneliti menggunakan berbagai konvensi bilateral yang ada terkait *cyberespionage* seperti Piagam PBB dan

---

[33] Soerjono Soekanto dan Sri Mamudji, Penelitian Hukum Normatif (Suatu Tinjauan Singkat),

Rajawali Pers, Jakarta, 2001, hal. 13-14.

[34] Peter Mahmud Marzuki, *Penelitian Hukum Edisi Revisi*, Cetakan ke – 14, Prenada Media, Jakarta, 2019, h. 133.

[35] *Ibid*.

beberapa Resolusi Majelis Umum PBB. Pendekatan ini adalah pendekatan dengan menelaah semua peraturan perjanjian internasional dan konvensi yang berkaitan dengan koridor hukum *cyber espionage* dalam hukum internasional, terutama dalam konteks negara sebagai pelaku.

2) Pendekatan Konseptual (*conceptual approach*) dengan cara memahami pandangan, doktrin dan konsep yang telah berkembang dalam ilmu hukum internasional seperti kedaulatan territorial, non-intervensi, atribusi, pertanggungjawaban negara dan yurisdiksi. Tentunya konsep yang berkaitan dengan isu hukum dalam penulisan skripsi ini, demi menemukan pengertian hukum, konsep hukum, dan asas hukum.[36] Rujukan konsep nantinya bertujuan membantu peneliti dalam memahami konsepsi *cyber espionage* dalam hukum internasional.

1.5.3 Sumber Bahan Hukum

Dalam penulisan penelitian ini terdapat dua jenis bahan hukum yaitu bahan hukum primer dan bahan hukum sekunder.[37] Bahan hukum primer adalah bahan hukum berwibawa, artinya bahan hukum tersebut mengikat. Materi hukum yang mengikat dapat berupa perjanjian internasional bilateral atau multilateral yang

[36] *Ibid*, h. 135.

[37] Suharsimi Arikunto, Prosedur Penelitian suautu Pendekatan Praktek, Jakarta, Rineka Cipta, 200, Hal. 234

berlaku dan terkait dengan rumusan masalah yang akan dibahas. Bahan hukum utama meliputi:

1. Piagam PBB (*UN Charter*)
2. 1907 *Hague Convention With Respect to the Laws and Customs of War on Land*
3. *Vienna Convention on Diplomatic Relations* 1961
4. *Vienna Convention on Consular Relations 1963*
5. *Convention on Cybercrime, Budapest Convention* 2001
6. *Articles on Responsibility of States Internationally Wrongful Acts* (ARSIWA) 2001
7. 1970 *Friendly Declaration*
8. Montevido Convention on the Rights and Duties of States
9. *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*
10. *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space*
11. *The Antartic Treaty 1959*
12. *United Nations Conventions on the Law of the Sea*
13. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Selain bahan buku primer, penulisan skripsi ini juga menggunakan bahan hukum sekunder yang terdiri dari pendapat para ahli dan sarjana hukum internasional yang terdapat dalam buku-buku literatur hukum khususnya hukum internasional dan hukum diplomatik dan konsuler, hukum siber, catatan kuliah, karya ilmiah, artikel dari jurnal atau cetakan. dan media internet yang substansinya berkaitan dengan masalah yang akan dibahas dalam skripsi ini.

1.5.4 Prosedur Pengumpulan Bahan Hukum

Prosedur pengumpulan bahan hukum dilakukan dengan cara mengumpulkan semua bahan, baik peraturan perundang-undangan dan perjanjian internasional yang merupakan sumber primer dan buku-buku penunjang yang berkaitan. Penulis mempelajari, menganalisis dan merumuskan hasil dari bahan hukum untuk selanjutnya dapat diolah kembali untuk menyelesaikan pokok permasalahan yang diangkat oleh penulis di dalam skripsi ini.

1.5.5 Analisis Bahan Hukum

Bahan hukum dan bahan non-hukum yang diperoleh dalam penelitian ini akan dianalisis secara teliti dengan menggunakan metode deduktif yaitu data umum tentang konsepsi hukum baik berupa asas-asas hukum, doktrin dan pendapat para ahli yang dirangkai secara runtut sebagai susunan fakta – fakta hukum untuk mengkaji *Cyber-espinage* sebagai *Cybercrime* menurut hukum internasional.

1.6 Pertanggungjawaban Sistematika

Untuk memudahkan pembaca guna memahami isi pembahasan dari penelitian hukum ini, maka penulis akan memberikan pemaparan pertanggungjawaban sistematika. Sistematika penulisan daripada penelitian ini akan terbagi menjadi empat bab yang pada tiap babnya akan terbagi kembali menjadi beberapa sub-bab. Berikut penjabaran sistematika penulisan dalam penelitian ini.

Bab I berisikan pendahuluan dari penelitian ini yang terdiri dari latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan pertanggungjawaban sistematika. Bab ini akan menjelaskan

keperluan dilakukannya penelitian ini. Kemudian pada Bab II berisikan dua sub bab dimana sub pertama akan berisi pembahasan mengenai pokok-pokok *cyber espionage*. Pada sub bab kedua akan berisi pembahasan mengenai bagaimana *cyber espionage* diatur dalam hukum internasional.

Kemudian pada bab III berisikan dua sub bab dimana sub bab pertama akan membahas mengenai Pertanggungjawaban negara secara definisi dan konsep. Sub bab kedua akan membahas mengenai pertanggungjawaban negara pelaku *cyber espionage*. Kemudian pada Bab IV adalah bab penutup yang berisikan kesimpulan dari penelitian hukum dan saran.