BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Konflik merupakan faktor utama awal terjadinya perang. Konflik atau *configere* yang berarti saling memukul. Sehingga dalam arti yang sempit, konflik dapat diartikan sebagai upaya untuk saling menghancurkan satu sama lain. Pasca Perang Dunia dan Perang Dingin, perang masih menjadi salah satu cara untuk menyelesaikan konflik dan permasalahan yang dihadapi dengan negara yang bertentangan, meskipun ada alternatif yang ditawarkan untuk meyelesaikan konflik yaitu diplomasi. Perang merupakan upaya untuk mencapai puncak persaingan, menjaga kedaulatan negara dan memperkuat eksistensi diri negara dengan cara menundukkan kehendak musuh baik secara fisik maupun psikologis.

Kemajuan teknologi informasi dan komunikasi adalah salah satu produk dari era global, menjadikan hal tersebut sebagai sarana juga arena perang baru. Negara yang pada umumnya adalah aktor utama dalam peperangan, memanfaatkan dan menerapkan kemajuan teknologi informansi dan komunikasi sebagai strategi perang baru untuk menaklukan pihak musuh. Kemajuan teknologi informasi dan komunikasi memberikan dampak pergeseran cara pandang dalam berperang, dari tembak-menembak secara fisik pada dunia aktual (perang konvensional) telah bergeser menjadi perang siber *(cyber warfare)* pada dunia virtual/maya *(cyber space)* yang memberikan konsekuensi pada dunia aktual dan dunia siber itu sendiri.

Dunia maya menjadi fenomena baru yang menciptakan pusat integrasi dalam ruang fisik bergeser ke dalam ruang virtual. Dunia maya yang menggunakan jaringan telekomunikasi internet telah menyentuh ke semua aspek kehidupan dan lapisan masyarakat yang mampu mengintegrasi komunikasi secara global bahkan untuk menjalankan sistem infrastruktur vital di setiap negara. Ditinjau dari segi politik, dunia maya telah mengubah perspektif banyak negara dalam hubungan internasional secara meluas.

Pada tahun 2014, seorang *whistle-blower* sekaligus mantan agen *National Security Agency* (NSA) Amerika Serikat, yaitu Edward Snowden mengkhianti instansinya dan negaranya dengan membocorkan berbagai dokumen rahasia milik NSA kepada publik. Dokumen rahasia tersebut adalah hasil dari operasi 'kotor' yang dilakukan NSA menyangkut pelanggaran data privasi pengguna internet dan telekomunikasi dunia (http://tekno.liputan6.com/read/2185425/10-dosa-besar-nsa-yang-dibocorkan-edward-snowden diakses pada tanggal 10 April 2017).

Dari dokumen-dokumen rahasia NSA yang dibocorkan Snowden mengundang reaksi dunia, Presiden Brasil Dilma Rousseff membatalkan kunjungannya ke Amerika Serikat sebagai tindakan protes setelah mengetahui tindakan yang dilakukan oleh Amerika Serikat kepada negaranya. Selain Brasil, protes keras juga dilontarkan dari Jerman, Prancis dan Meksiko. Julian Assange pendiri situs non-profit yaitu Wikileaks juga turut membocorkan file-file yang bersifat rahasia, terutama yang menyangkut negara Amerika Serikat. Dengan domain www.wikileaks.ch, publik dapat mengakses informasi rahasia tersebut.

Choucri dalam tulisannya *Cyber Space and International Relations; Toward an Integrated System* menyatakan bahwa permasalahan yang telah terjadi pada dunia maya ini tidak lagi dibahas dalam tingkat *low politic*, tetapi telah mengantarkan pembahasan pada tingkat *high politic* (2011: 2).

Pada abad informasi ini negara-negara tengah fokus membangun *intangible power* demi kepentingan dan menjaga keamanan nasionalnya. Beberapa negara telah membangun militer untuk menghadapi ancaman *Cyber Warfare*.

Tabel 1.1

Negara dengan Organisasi Militer Siber

No.	Negara	Organisasi
1.	Albania	*Interinstitutional Maritime Operational Center* (IMOC)
2.	Argentina	Jefatura VI
3.	Austria	Abwehramt
4.	Australia	-Cyber Security Policy -Coordination Branch of The Attorney-General's Department
5.	Amerika Serikat	-US Strategic Command (STARTCOM) -US Cyber Command (CYBERCOM) -National Security Agency (NSA)
6.	Belarusia	Belarus Cyber Armed Forces
7.	Brazil	-Cyber-Warfare Communication Center -Center of Cyber Defense

8.	Canada	Canadian Forces Information Operations Group
9.	China	People's Liberation Army -Blue Army
10.	Colombia	Colombia Computer Emergency Response Team (Colombia CERT)
11.	Korea Utara	Biro 121
12.	Korea Selatan	-Cyber War Center -Computer Emergency Response Teams
13.	Denmark	3rd Eletronic Warfare Company
14.	Estonia	-Defense League -Cyber Security Allience
15.	Prancis	National Agency for The Security of Information System
16.	Jerman	National Cyberdefence Center
17.	India	-The Defence Information Warfare Agency -The Defence Intelligence Agency -National Technical Intelligence Communication
18.	Israel	-The Israel Defense Forces' Unit 8200 -The C41 Corps -The Center for Encryption and Information Security (Matzov) -The National Cybernetic Taskforce
19.	Iran	Irian Cyber Army
20.	Italia	-Telematics Section of Carabineri -Defence Innovation Center -Division for Information Security

21.	Kazakhtan	Kazakh Computer Emergency Response Team
22.	Malaysia	Cyber Security Malaysia
23.	Myanmar	Defense Services Computer Directorate
24.	Belanda	National Cyber Security Centre
25.	Polandia	Independent Information Force
26.	Rusia	Federal Agency of Government Communication and Information
27.	Swiss	Center for Eletronic Operations of The Armed Forces Command Support Organization
28.	Britania Raya	-Cyber Security Operations Centre -The Office of Cyber Security and Information Assurance
29.	Ukraina	The Ministry's Donetsk Law Institute
30.	Finlandia	Security and Defence Commite

Sumber: Lewis. Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization, 2011: 5-21

Keseriusan perang non-tradisional melalui domain dunia maya ditunjukan dengan terciptanya senjata siber *(cyber weapon)*. Virus Stuxnet adalah salah satu senjata yang digunakan untuk merusak fasilitas pengayaan nuklir Natanz yang berlokasi di daerah ibu kota Natanz, Provinsi Isafan 130 mil seletan dari Tehran, Iran. Aksi ini sebagai respon Amerika Serikat dan Israel terhadap proyek nuklir Iran. Israel menganggap proyek nuklir Iran akan menjadi ancaman baru bagi Israel (Pratama, 2016: 380).

NSA Amerika Serikat dan Unit 8200 Israel bekerjasama dalam pembuatan senjata siber yaitu Virus Stuxnet. Virus Stuxnet ini menjadi ancaman menakutkan

di dunia maya terutama bagi Iran, virus ini berhasil melumpuhkan seperlima tabung pengayaan uranium Iran (http://tekno.liputan6.com/read/634340/snowden-nsa-dan-israel-ciptakan-virus-stuxnet-yang-serang-iran diakses pada tanggal 10 April 2017).

Virus Stuxnet menjadi contoh sebagai senjata siber yang dapat menaklukan musuh dengan mengkaburkan batas ruang, waktu, dan bukti. Ketiga konsep tersebut yang dahulunya dianggap sebagai penghambat dalam perang tradisional (Pratama, 2016: 382).

Menurut Richard A. Clarke sebuah negara dikatakan belum berhasil dalam membangun bidang siber jika hanya dapat melakukan serangan siber, tetapi ada 3 indikator yang dapat menjadi tolak ukur untuk berhasil dalam bidang siber, yaitu: *offense, defence* dan *dependence*. *Offense* merupakan ukuran kemampuan suatu negara dalam melakukan penyerangan guna melemahkan jaringan-jaringan sistem komputer musuh atau merusak pertahanan siber (*cyber deffense*) dari pihak musuh. *Defence* yang dimaksud adalah pengukuran kemampuan suatu negara guna beraksi dalam suatu serangan siber, dimana aksinya tersebut dapat memberikan pertahanan dan mengurangi serangan-serangan dan dampak dari serangan siber musuh. *Dependence* adalah suatu tingkat ketergantungan suatu negara terhadap jaringan dan sistem yang rentan jika terjadi serangan siber (Clarke, 2010: 72).

Sederet manfaat yang ditawarkan kemajuan teknologi informasi internet mempunyai kekurangan, dunia maya masih sangat rentan terjadinya ancaman siber, karena serangan pada dunia maya tidak dapat diprediksi, arena virtual yang

begitu luas (*borderless*) dan belum adanya hukum internasional yang mengikat tentang kejahatan siber. Semakin tinggi ketergantungan suatu masyaratakat akan teknologi informasi, semakin tinggi pula resiko yang dihadapi. Saat ini aspek perekonomian, sosial dan pertahanan begitu tergantung pada internet. Aktivitas perbankan, transaksi perekonomian, pemeliharan dan penggunaan transportasi, pengendalian persenjataan hingga komunikasi tidak terlepas dari interkoneksi tersebut.

Semua orang mendapatkan kesempatan untuk masuk dan mengakses dunia maya, sehingga dapat dimungkinkan setiap individu, kelompok bahkan negara mampu untuk mengobrak-abrik sistem yang ada hingga mampu memrusak dan menguasai aset serta pertahanan individu ataupun negara lain melaui dunia maya (Soewardi, 2013: 32).

Gary Mckinnon seorang *hacker* warga negara Inggris, pada tahun 2001-2002 menyerang atau mengakses komputer secara illegal termasuk sistem pentagon dan *National Aeronautics and Space Administration* (NASA) hanya untuk mencari informasi atau data tentang *Unidentified Flying Object* (UFO) dan dari aksi ini menyebabkan kerusakan senilai $700.000, dan juga pada tahun 2011-2012 Gary mematikan 2000 komputer tentara Amerika Serikat di Washington selama 24 jam.

Tiongkok dalam operasi *"Bizantium Hades"* berhasil dalam memanfaatkan *cyber space* untuk melakukan spionase *(cyber espionage)* terhadap Amerika Serikat. Dari aksi ini, Tiongkok mendapatkan data dalam pembuatan pesawat tempur Amerika Serikat yaitu F-35. Tiongkok diuntungkan dengan

adanya data pembuatan pesawat tempur, membuat Tiongkok menghemat waktu dalam riset pembuatan pesawat tempur. Chengdu J-20 dan Shenyang J-31 pesawat tempur milik Tiongkok yang dituding Amerika Serikat adalah pesawat tempur yang dibuat dengan bedasarkan spesifikasi teknis F-35.

Kerentanan dunia maya membuat sering terjadinya ancaman siber, serangan siber, kejahatan siber dan mengkerucut pada *cyber warfare*. *Cyber warfare* sebagai perang modern telah mendapatkan perhatian lebih dalam, karena perang ini sama pentingnya dalam perang menjaga kedaulatan negara. Seperti darat, laut, udara, dan ruang angkasa, dunia maya menjadi matra ke lima dalam medan perang. *Cyber warfare* mengacu pada penggunaan fasilitas www (*world wide web*) dan jaringan komputer untuk melakukan perang di dunia maya (Soewardi, 2013: 32).

Ancaman *cyber warfare* terbesar dunia yang pernah dicatat oleh situs *Discovery*, seperti:

1. Serangan Worm Stuxnet, melumpuhkan pembangkit nuklir Bushehr dengan worm tahun 2010.
2. Operasi Aurora tahun 2009, menyerang Perusahaan besar termasuk Google dan Adobe Systems, oleh para hacker dan berhasil mencuri properti intelektual dari perusahaan-perusahaan tersebut.
3. Serangan terhadap Pusat Komando AS tahun 2008, sebuah *flash drive* yang tidak berwenang yang diselipkan ke salah satu laptop di sebuah markas militer AS di Timur Tengah. *Flash drive* tersebut mengandung kode berbahaya yang dikembangkan oleh intelijen asing dan menyebar

melalui sistem komputer Departemen Pertahanan AS dan menyebabkan data dikirim ke server asing.

4. Kasus Georgia tahun 2008, berawal dari konflik Rusia dan Georgia di Ossetia Selatan. Serangan *cyber* melumpuhkan beberapa situs pemerintah Georgia dan situs-situs media lokal, setelah Georgia menyerang Ossetia Selatan. Ini merupakan serangan yang mirip dengan serangan ke Estonia pada 2007.
5. Kasus Estonia tahun 2007, dimana Estonia menghadapi gelombang serangan *cyber* yang melanda segenap infrastruktur internet negara itu, mulai dari situs-situs pemerintahan, perbankan, hingga situs-situs surat kabar lokal. Serangan ini terjadi melumpuhkan sistem pemerintahan Estonia selama 2 (dua) minggu (http://teknologi.news.viva.co.id/news/read/193494-serangan-cyber-terbesar-sepanjang-sejarah diakses pada tanggal 15 April 2017).

Amerika Serikat dan Korea Utara adalah dua negara yang menganut sistem ideologi yang berbeda, sehingga sering kali kedua negara ini mengalami pergesekan sejak lama dalam dunia politik dan keamanan. Amerika Serikat menuduh Korea Utara yang memiliki senjata nuklir dapat merusak keamanan regional hingga internasional. Namun, pernyataan Amerika Serikat tersebut dibantah oleh pihak Korea Utara. Korea Utara mengklaim bahwa senjata nuklir yang dimilikinya hanya sebagai pertahanan keamanan nasional. Meskipun Amerika Serikat dan Korea Utara sering terlibat sengketa, tidak membuat kedua negara tersebut mengambil jalan perang (konvensional) atau diplomasi untuk

menyelesaikan secara tuntas masalah mereka. Hingga akhirnya, Amerika Serikat dan Korea Utara terlibat perang dalam dunia maya (non-konvensional).

Pada November 2014, *Sony Pictures Entertainment* (SPE) mendapatkan serangan siber dari kelompok hacker bernama *The Guardians of Peace* (GOP). Serangan yang dilakukan oleh GOP ini sebagai respon kepada *Sony Pictures Entertainment* yang merilis film *The Interview*. Film *The Interview* salah satu film hasil produksi *Sony Pictures Entertainment* yang disutradarai oleh Evan Goldberg dan Seth Rogen. Film yang ber-*genre action-comedy* dengan durasi 112 menit ini menceritakan Dave Skylark (James Franco) yang membawakan acara "*Skylark Tonight*" dan produser acara Aaron Rapoport (Seth Rogen) mencoba mempertahankan eksistensi acara tersebut. Memasuki episode ke-1000 Dave dan Aaron mencoba untuk memberikan trobosan untuk meningkatkan eksistensinya dalam dunia hiburan, hingga Dave dan Aaron diundang oleh Pemerintah Korea Utara untuk datang mewawancarai Kim Jong Un (Randall Park). Presiden Kim sangat menyukai acara *Skylark Tonight* yang dibawakan oleh Dave Skylark, hingga akhirnya Dave dan Aaron berkesempatan datang ke Korea Utara.

Beberapa hari sebelum keberangkatan Dave dan Aaron didatangi oleh 2 orang agen CIA bernama Lacey (Lizzy Caplan) dan Botwin (Reese Alexander). Kedua agen CIA ini meminta Dave dan Aaron yang berkesempatan datang ke Kora Utara untuk membunuh Presiden Kim yang terkenal kediktatorannya. Hal tersebut akibat Korea Utara yang dipimpin oleh Kim Jong Un mempunyai senjata nuklir yang dapat membahayakan keamanan dunia dan menjadi negara paling berbahaya di dunia.

Tawaran yang diberikan agen CIA tersebut sempat membuat Dave dan Aaron tidak percaya dengan misi yang dibebankan pada mereka, hingga mereka menyanggupi permintaan agen CIA tersebut. Dave dan Aaron dibawa ke markas CIA untuk diberikan pelatihan dalam menggunakan peralatan-peralatan intelegen dalam mejalankan misi, agar jejak pembunuhan Kim Jong Un tidak menimbukan kecurigaan pihak Korea Utara. Dave dan Aaron dilatih dalam menggunakan sebuah alat yang mempunyai racun. Setelah menjalani pelatihan, Dave dan Aaron memulai perjalan menuju Korea Utara.

Sampai di Korea Utara, Dave dan Aaron disambut dengan meriah oleh masyarakat Korea Utara. Dalam perjalanan menuju hotel, Dave dan Aaron disuguhi oleh pandangan masyrakat Korea Utara yang sejahtera yang mana sangat berbeda dengan yang biasa diberitakan mengenai Korea Utara. Melihat masyarakat Korea Utara yang sejahtera, Dave dan Aaron mengurungkan niat untuk membunuh Presiden Kim. Selama di Korea Utara, Dave yang disenangi Presiden Kim ditunjukan keramahan dan kebaikan oleh seorang Presiden Kim, hal tersebut membuat Dave menjadi akrab dengan Presiden Kim.

Suatu malam Dave mendapat jamuan untuk makan malam bersama Presiden Kim untuk memperingati kematian salah satu seorang loyalis Presiden Kim. Dalam jamuan makan malam, Presiden Kim mulai menampakan kediktatorannya dalam ucapannya untuk membunuh masyarakat Korea Utara untuk menunjukan kekuatannya. Setelah pulang dari makan malam bersama Presiden Kim, dalam perjalanan pulang Dave mampir ke toko buah. Dalam toko buah tersebut, Dave mendapati buah-buahan tersebut palsu. Mengetahui bahwa

semua yang dilihat Dave adalah kebohongan, Dave dan Aaron mengembalikan niatnya untuk membunuh Presiden Kim. Namun, seorang tentara wanita Korea Utara bernama Sook (Diana Bang) mengatakan jika Presiden Kim terbunuh tidak akan mengubah kediktaktoran di Korea Utara, karena akan digantikan oleh saudara atau orang dekat Presiden Kim. Revolusi adalah cara untuk menghentikan kediktatoran di Korea Utara. Salah satu cara revolusi tersebut dengan menunjukan pada dunia khususnya masyarakat Korea Utara, bahwa Kim Jong Un bukanlah tuhan seperti yang dia katakan. Dave dan Aaron dibantu tentara Sook untuk menyiapkan wawancara eksklusif dengan Presiden Kim. Dalam wawancara tersebut, Dave berhasil menampilakan seorang Kim Jong Un bukanlah tuhan.

Setalah wawancara, Presiden Kim ingin meluncurkan nuklir ke Amerika Serikat. Namun usaha Presiden Kim terhenti setelah tewas terbunuh ditembak dengan peluru tank oleh Dave. Setelah misi selesai, Dave dan Aaron kembali ke Amerika Serikat. Setelah tewasnnya Presiden Kim, Korea Utara mengalami revolusi dan tentara Sook diangkat menjadi presiden Korea Utara (http://www.imdb.com/title/tt2788710/ diakses pada tanggal 15 Juni 2017).

Dari cerita film *The Interview* di atas, dianggap sebagai film propaganda yang menyudutkan Pemerintahan Kim Jong Un di Korea Utara. Akibatnya, GOP berhasil mencuri sejumlah file yang berkaitan dengan rumah produksi di Amerika Serikat ini, sejumlah file termasuk lima film yang belum dipublikasikan oleh *Sony Pictures Entertainment*. Lima film produksi *Sony Pictures Entertainment* tersebut dipublikasikan oleh GOP secara gratis di internet (http://www.cnnindonesia.com

/hiburan/20141125094831-220-13631/sony-pictures-entertainment-dikerjai-hacker/ diakses pada tanggal 15 Juni 2017).

Selain mengambil file rahasia, GOP juga turut melakukan perusakan pada sistem jaringan pada *Sony Pictures Entertainment*, sehingga kinerja perusahaan tersebut terganggu. Selain melakukan serangan *cyber*, GOP juga mengancam *Sony Pictures Entertainment* untuk melakukan serangan fisik pada bioskop-bioskop yang menayangkan film tersebut. Setelah mendapatkan serangan siber dan mendapatkan ancaman berupa fisik, *Sony Pictures Entertainment* menyatakan akan membatalkan film *The Interview* (http://tekno.liputan6.com/read/2148615/hacker-sony-ancam-tragedi-seperti-911-akan-terulang diakses pada tanggal 15 Juni 2017).

Tuntutan GOP dalam pembatalan film *The Interview* membuat Barack Obama selaku presiden Amerika Serikat memperingatkan, bahwa tidak ada negara/kelompok lain yang berhak mengganggu atau merusak kedaulatan Amerika Serikat. Barack Obama menyatakan kasus ini akan ditelusuri oleh pemerintah Amerika Serikat dan mencari tahu pihak yang melakukan penyerangan.

Meskipun tindakan Korea Utara melalui GOP hanya tertuju pada perusahaan swasta *Sony Pictures Entertainment*, Amerika Serikat tetap mengambil inisiatif untuk merespon serangan yang di lakukan Korea Utara. Amerika Serikat memandang Korea Utara telah mengancam kedaulatan negaranya dengan menekan kebebasan berekspresi yang menjadi salah satu nilai penting yang diterapkan oleh Amerika Serikat, sehingga terjadilah *cyber warfare*

antara Amerika Serikat dan Korea Utara (http://tekno.liputan6.com/read/2152899/internet-lumpuh-korut-sebut-as-seperti-anak-ingusan diakses pada tanggal 15 Juni 2017).

Serangan balasan dari Amerika Serikat yang pertama dilakukan pada tanggal 22 Desember 2014, membuat konektifitas internet di Korea Utara tidak stabil hingga berujung mati total. Amerika Serikat melakukan aksinya dengan metode serangan *distributed denial of service* (Ddos), Serangan DdoS sebenarnya serangan siber sederhana, dimana satu jaringan komputer yang menjadi sasaran dikirim banyak data sehingga jaringan itu tidak bisa dipergunakan sementara bahkan mati. Korea Utara beraksi setelah mendapatkan serangan yang mematikan jaringan internet di negaranya, Komisi Pertahanan Korea Nasional Korea Utara menuding Amerika Serikat menjadi aktor dalam penyerangan. Amerika Serikat membantah tuduhan Korea Utara sama seperti yang dilakuakan Korea Utara saat menyerang *Sony Pictures Entertainment*.

Untuk memudahkan peneliti dalam mengkaji *cyber warfare* antara Amerika serikat dan Korea Utara, maka peneliti menggunakan beberapa penelitian terdahulu sebagai acuan dan menemukan perbedaannya. Beberapa penelitian terdahulu yang digunakan peneliti adalah penelitian Trisuharto Clinton dari jurusan ilmu hukum, Universitas Diponegoro Semarang pada tahun 2015 dengan judul penelitian *"Kajian Perang Cybernetika (Cyber-Warfare) Sebagai Konflik Bersenjata Internasional Berdasarkan Hukum Humaniter Internasional"*. Dalam penelitian Trisuharto ini, membahas mengenai perkembangan teknologi informasi dan komunikasi yang menjadi strategi perang baru dunia. Trisuharto

juga membahas bagaimana perkembangan *cyber warfare* terjadi, mengkategorikan *cyber warfare* sebagai perang bersenjata internasional, dan membahas apakah hukum humaniter internasional dapat diterapkan terhadap *cyber warfare*.

Kedua, penelitian dari Ivan Hilmi Alviantio dari jurusan ilmu hukum, Universitas Brawijaya Malang pada tahun 2013. Dengan judul *"Tinjauan Mengenai Cyber Warfare Berdasarkan Hukum Humaniter Internasional (Studi kasus perang antara Rusia dengan Georgia pada 7 Agustus 2008)"*. Penelitian yang dilakukan Ivan membahas bagaimana Rusia mampu menaklukan Georgia dengan pemanfaatan dunia maya, membahas dampak sebab akibat saat terjadinya serangan siber, membahas penerapan aturan-aturan hukum humaniter internasional diterapkan pada kasus *cyber warfare yang* terjadi di Georgia dalam perang antara Rusia dan Georgia.

Ketiga, penelitian dari Moehammad Yuliansyah Saputera dari jurusan ilmu hubungan internasional, Universitas Riau pada tahun 2015. Dengan judul *"Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare".* Penelitian yang dilakukan Moehammad membahas pengaruh *cyber security strategy* Amerika Serikat dalam mengamankan dan mempertahankan data-data digital penting serta infrastruktur vital milik Amerika Serikat dari ancaman *cyber warfare*.

Berdasarkan alasan-alasan tersebut yang menjadi dasar pertimbangan peneliti untuk mengadakan penelitian dengan judul:

"*Cyber Warfare* Antara Amerika Serikat dan Korea Utara Dalam Kasus Film *The Interview* Oleh *Sony Pictures Entertainment*".

Ada pun ketetarikan peneliti untuk meneliti dan mengangkat isu tersebut didukung oleh beberapa mata kuliah disiplin Ilmu Hubungan Internasional, diantaranya sebagai berikut:

1. *Cyber law & Cyber crime*, merupakan mata kuliah yang menjelaskan tentang kasus *cyber law* dan *cyber crime* pada dunia maya yang ada di dunia, serta menjadi salah satu pembahasan dalam *cyber warfare*.
2. Studi Keamanan Internasional, merupakan mata kuliah yang mempelajari konsep keamanan suatu negara yang menjadi faktor penting dalam kehidupan bernegara suatu bangsa. Berdasarkan mata kuliah ini peneliti menilai bahwa, perkembangan teknologi informasi dan komunikasi membawa strategi perang baru pada dunia maya yang berakibat banyaknya *cyber warfare* pada skala internasional. Sehingga dibutuhkan konsep-konsep keamanan yang menjaga kedaulatan setiap negara.
3. *Information and Communication Technology* (ICT) *for International Relation*, merupakan mata kuliah yang mempelajari isu perkembangan teknologi informasi dan dampak yang ditimbulkan dari perkembangan teknologi tersebut. Mata kuliah ini sangat berkaitan dengan penelitian yang dilakukan peneliti untuk membahas *cyber warfare*.

1.2 Rumusan Masalah

1.2.1 Rumusan Masalah Mayor

Berdasarkan latar belakang diatas, untuk memudahkan peneliti dalam melakukan pembahasan, peneliti merumuskan masalah mayor sebagai berikut :

"Bagaimana Cyber Warfare Antara Amerika Serikat dan Korea Utara Dalam Kasus Film The Interview Oleh Sony Pictures Entertainment?"

1.2.2 Rumusan Masalah Minor

1. Apa yang melatar belakangi *cyber warfare* antara Amerika Serikat-Korea Utara dalam kasus film *The Interview Sony Pictures Entertainment*?
2. Apa kerugian yang dialami oleh *Sony Pictures Entertainment* dalam kasus film *The Interview*?
3. Apa respon Amerika Serikat terhadap serangan siber Korea Utara kepada *Sony Pictures Entertainment*?

1.2.3 Pembatasan Masalah

Adapun batasan waktu yang digunakan oleh peneliti pada penelitian ini adalah pada tahun 2014 sampai dengan tahun 2015. Peneliti mengambil batasan penelitian ini berdasarkan awal terjadinya serangan Korea Utara terhadap *Sony Pictures Entertainment* dan respon Amerika Serikat terhadap serangan yang dilakukan Korea Utara terhadap industri yang berada di kawasan Amerika Serikat.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Penelitian ini dimaksudkan untuk mengetahui bagaimana *cyber warfare* antara Amerika Serikat dan Korea Utara dalam kasus film *The Interview* oleh *Sony Pictures Entertainment*.

1.3.2 Tujuan Penelitian

1. Untuk mengetahui *cyber warfare* antara Amerika Serikat dan Korea Utara dalam kasus film *The Interview* oleh *Sony Pictures Entertainment.*
2. Untuk mengetahui latar belakang *cyber warfare* antara Amerika Serikat dan Korea Utara dalam kasus film *The Interview* oleh *Sony Pictures Entertainment.*
3. Untuk mengetahui kerugian yang dialami oleh *Sony Pictures Entertainment* atas serangan siber yang dilakukan Korea Utara.
4. Untuk mengetahui respon Amerika Serikat terhadap searangan siber Korea Utara kepada *Sony Pictures Entertainment*.

1.4 Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Secara teoritis, hasil dari penelitian ini diharapkan tidak hanya menjadi acuan atau referensi pengetahuan terkait, namun memberikan pengetahuan baru mengenai *cyber warfare* sebagai perang bersenjata

internasional dan menambah kajian-kajian yang ada dalam studi hubungan internasional.

1.4.2 Kegunaan Praktis

1. Diharapkan menambah wawasan dan ilmu pengetahuan, serta bermanfaat bagi para pembaca khususnya Program Studi Ilmu Hubungan Internasional mengenai *cyber warfare* antara Amerika Serikat dan Korea Utara.
2. Sebagai acuan bagi penstudi Hubungan Internasional dan umum dalam memahami *cyber warfare* khususnya antara Amerika Serikat dan Korea Utara.