# PENDAHULUAN

## Latar Belakang Masalah

Ilmu pengetahuan dan teknologi (IPTEK) yang berkembang pesat, bertujuan untuk menjadikan masa depan manusia lebih baik di masa mendatang. Salah satu bentuk perkembangan IPTEK adalah adanya jaringan internet. *The U.S Supreme Court* mendefinisikan internet sebagai "*international network of interconnected computers"* yang artinya “jaringan internasional dari komputer, yang saling berhubungan” (Reno v. ACCLU 1997).[[1]](#footnote-1)

Keberadaan internet membuat kehidupan masyarakat berubah, dari yang bersifat nyata *(real)* ke realitas baru yang bersifat maya *(virtual)* atau disebut *cyber space* *(*dunia maya).[[2]](#footnote-2) *Cyber space* ini dalam kenyataanya terbentuk melalui jaringan-jaringan komputer yang menghubungkan antar Negara atau antar Benua yang berbasis *protocol transmission control* *protocol / internet protocol*. Artinya dalam sistem kerja dengan *internet protocol* ini telah mengubah jarak dan waktu tidak terbatas, menjadikan dunia saling terhubung dan saling terkait.[[3]](#footnote-3)

Internet dan teknologi yang serba digital ini telah membawa kemudahan bagi segala aktivitas manusia sehari-harinya, termasuk membawa dunia bisnis yang revolusioner. Saat ini bisnis menjadi lebih mudah, lebih cepat, dan lebih murah untuk dilakukan. Bahkan melalui internet kegiatan pasar dunia bisa diketahui selama 24 jam. Sehingga membantu kegiatan komunitas komersial menjadi besar, pesat, serta menembus ke berbagai batas Negara.

Hal signifikan lain dari kehadiran internet, yaitu mengakibatkan adanya pergeseran paradigma dalam praksis hubungan internasional, dimana diplomasi suatu Negara tidak hanya dilakukan oleh para duta besar, para diplomat atau perwakilan-perwakilan yang telah ditunjuk oleh Negara, melainkan dapat dilakukan oleh semua masyarakat dari berbagai aspek sosial, ekonomi, dan kultur yang berbeda.

Saat ini, internet telah melekat sebagai kebutuhan masyarakat global. Tercatat lebih dari 360 juta *internet user* pada akhir tahun 2000 di seluruh dunia dan terus mengalami peningkatan sekitar 74%. Artinya menjadi lebih dari 3 miliar *internet user* pada tahun 2014.[[4]](#footnote-4)

Meningkatnya *internet user* berjalan beriringan dengan dampak negatif, yang menjadi ancaman baru bagi masyarakat global itu sendiri, yaitu *cyber crime.[[5]](#footnote-5)* Indra Safitri (dalam Maskun) mengemukakan bahwa kejahatan dunia maya (*cyber crime)* adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakterisktik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas sebuah informasi yang disampaikan dan diakses oleh pelanggan *internet.[[6]](#footnote-6)* Dalam beberapa literatur, *cyber crime* sering diidentikkan sebagai *computer crime.* *Organization of European Community Development*, mendefinisikan *computer crime* sebagai : *"any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data"* (artinya perilaku ilegal, tidak etis atau tidak sah yang berkaitan dengan pemrosesan otomatis dan atau pengiriman data).[[7]](#footnote-7)

Selain itu, Samuel C Mc Quade dalam bukunya *Encyclopedia of Cyber Crime* mengatakan bahwa *cyber crime* dapat dilakukan dari suatu tempat yang menawarkan konektivitas internet, akibatnya tidak seperti penipuan atau pencurian tradisional, karena dalam tindak kejahatan ini pelaku tidak mendatangi langsung korban, sehingga membuat pelaku selalu tidak dapat diketahui keberadaannya, pelaku bersembunyi dalam batas-batas yang tak terbatas di dunia maya, dengan waktu yang lama.[[8]](#footnote-8) Sifat dari *cyber crime* yang menembus ruang dan lintas Negara inilah yang membuat *cyber crime* dianggap sebagai fenomena global.

Pelaku *cyber crime* yang lintas Negara, juga diperkuat dengan meningkatnya jumlah *internet user* yang tersebar di dunia. *Internet user* yang tinggi itu lah yang meningkatkan penyebaran insiden *cyber crime* di berbagai Negara. Salah satu contoh insiden *cyber crime* terjadi diAmerika Serikat, pada sebuah bank di UAE dan Oman, telah mengalami serangan oleh sekelompok orang *hacker,* yang mengalihkan dana sebesar $45juta. Artinya, kemungkinan total kekerugian akibat *cyber crime* di dunia, dalam satu tahun dapat mencapai ratusan juta dollar Amerika.[[9]](#footnote-9) Kondisi-kondisi tersebut menjelaskan, berpotensinya *cyber crime* sebagai ancaman keamanan nasional suatu Negara.

Meluasnya aktivitas *cyber crime* ke berbagai Negara, menyadarkan komunitas internasional betapa rapuh dan lemahnya jaringan internet terhadap ancaman *cyber crime* yang dapat menyerang kapan saja. Kekhawatiran ini yang kemudian menjadikan alasan internet menjadi ancaman integral dari sebuah Negara, karena banyaknya data-data sensitif yang disimpan di ruang maya (*cyber space*), mulai dari data pribadi, data penting negara, data penting perusahaan serta administrasi dunia dan data penting lainnya.

Hal ini kemudian yang menjadikan aktifitas *cyber crime* sebagai potensi dan ancaman yang mengusik stabilitas sistem teknologi yang di adopsi oleh Negara. Dimana sistem teknologi yang diadopsi negara ini, bertujuan untuk memudahkan sistem birokrasi dan pelaksanaan program-program kenegaraan tanpa harus mengalami ketertinggalan oleh pertumbuhan dunia global yang sangat cepat. Akan tetapi, sikap sentimen individu atau kelompok yang agresif terhadap Negara terkadang menjadi pemicu timbulnya kasus-kasus pembobolan terhadap sistem teknologi, terutama yang memanfaatkan jaringan internet sebagai medianya. Sehingga hal tersebut tentunya menciptakan instabilitas dalam sebuah Negara dan sangat berpotensi menjadi ancaman.[[10]](#footnote-10)

Salah satu bentuk ancaman lain bagi negara adalah penyerangan terhadap infrastruktur negara yang berkaitan dengan internet, mengingat infrastruktur Negara adalah salah satu pilar penting untuk dipertahankan demi mendongkrak kemajuan suatu Negara. Oleh sebab itu adanya *Cyber crime* dianggap sebagai sebuah isu baru dalam praksis hubungan internasional, karena dinilai akan memicu ancaman baru bagi keamanan Negara sama seperti aspek-aspek ancaman non militer lainnya.

Munculnya isu baru seringkali disebut sebagai isu keamanan non tradisional *(non traditional security).* Buzzan mengemukakan Keamanan non-tradisional adalah keamanan komprehensif yang menekankan pada aspek ancaman apa yang dihadapi oleh negara. Kandungan politik keamanan komprehensif adalah upaya menciptakan kestabilan dan ketertiban semua aspek keamanan. Pendekatan keamanan non-tradisional muncul terutama sebagai dampak dari globalisasi dan berbagai macam aspek-aspeknya memungkinkan kemudahan pergerakan baik itu individu atau kelompok yang dapat mengancam keamanan nasional maupun internasional, sehingga meningkatkan peranan mereka dalam praksis hubungan internasional.[[11]](#footnote-11) Oleh sebab itu potensi dan ancaman *cyber crime* dalam *cyber space* telah membuat banyak negara memutuskan untuk menanggulangi isu baru tersebut karna dinilai telah mengancam stabilitas Negara.

Salah satu negara yang mengalami serangan *cyber crime* dengan mengancam stabilitas suatu Negara terjadi di Jepang. Tepatnya serangan *cyber crime* di Jepang telah menyerang berbagai lingkup, seperti lingkup infrastruktur nasional,lembaga Pemerintahan, dan lingkup industri. Pada **lingkup industri**, serangan *cyber crime* telah menyerang perusahaan kontraktor pertahanan terbesar di Jepang, yang memproduksi pembuatan mesin (seperti pembangkit listrik tenaga nuklir, jembatan, mesin pesawat, kapal, pendingin udara untuk berbagai industri di seluruh dunia). Perusahaan kontraktor tersebut yaitu *Mitsubishi Heavy Industries Ltd.[[12]](#footnote-12)*

Kasus lainnya dari *cyber crime* di Jepangyang terjadi pada lingkup **infrastruktur nasional** Jepang yang terjadi pada: Badan Antariksa JAXA (*Japan Aerospace Exploration Agency*);[[13]](#footnote-13) Badan Energi Atom Jepang (JAEA);[[14]](#footnote-14) dan PLTN Monju yang komputernya mengalami peretasan.[[15]](#footnote-15)

Selain itu, Lembaga Pemerintah Jepang pun menjadi sasaran pelaku *cyber crime* dengan penyerangan terhadap Majelis Rendah Jepang,[[16]](#footnote-16)Majelis Tinggi Jepang*,[[17]](#footnote-17)* dan Badan Legislatif.[[18]](#footnote-18)

Serangan *cyber crime* yang dihadapi oleh Pemerintah Jepang telah membuktikan bahwa *cyber crime* bukan hanya merupakan masalah kriminal semata. Oleh karenanya*, cyber crime* termasuk masalah keamanan yang dapat mengganggu stabilitas negara. Sehingga, Pemerintah Jepang menempatkan isu *cyber crime* sebagai suatu agenda penting yang harus segera ditanggapi dan diselesaikan dengan mengambil langkah-langkah, baik itu strategi nasional maupun kerjasama internasional. Pemerintah Jepang di Masa Perdana Menteri Shinzo Abe, menangani isu *cyber crime* secara lebih agresif dan memperkuat keamanan Jepang dari ancaman *cyber crime*.

Berdasarkan paparan di atas, dapat dilihat bahwa Negara Jepang mengalami ancaman *cyber crime* yang cukup serius. Dikarenakan isu *cyber crime* berpotensi mengancam Keamanan Nasional dan Internasional suatu Negara, maka isu *cyber crime* dianggap menarik dan layak untuk diangkat dalam penelitian. Karena terdapat relevansi antara *cyber crime* yang menjadi suatu ancaman keamanan suatu negara dengan mata kuliah di dalam studi Hubungan Internasional, yaitu mata kuliah Studi Strategi dan Keamanan. Oleh karenanya, skripsi ini mengambil judul: “POTENSI DAN ANCAMAN *CYBER CRIME* : PENANGGULANGAN OLEH PEMERINTAHAN JEPANG”

## Identifikasi, Pembatasan, dan Perumusan Masalah

### Identifikasi Masalah

1. Bagaimana peran Pemerintah Jepang dalam menanggulangi *cyber crime?*
2. Apa saja hambatan Pemerintah Jepang dalam menanggulangi *cyber crime?*
3. Upaya apa saja yang dilakukan Pemerintah Jepang dalam menanggulangi *cyber crime?*

### Pembatasan Masalah

Mengingat luasnya permasalahan yang dihadapi, penulis membatasi fokus pembahasan pada ancaman *cyber crime* sebagai fenomena global dan peran pemerintah Jepang dalam menanggulangi *cyber crime* di Masa Perdana Menteri Shinzo Abe.

### Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka dapat dirumuskan permasalahan sebagai berikut: “Bagaimana ancaman global *cyber crime,* dapat ditanggulangi oleh pemerintah Jepang di Masa Perdana Menteri Shinzo Abe?”

## Tujuan dan Kegunaan Penelitian

### Tujuan Penelitian

Dari permasalahan di atas, penulis memiliki tujuan yang ingin dicapai yaitu:

1. Untuk mengetahui mengenai peran Pemerintah Jepang dalam menanggulangi *cyber crime.*
2. Untuk mengetahui hambatan apa saja yang dialami Pemerintah Jepang dalam menanggulangi *cyber crime.*
3. Untuk mengetahui upaya Pemerintah Jepang dalam menanggulangi *cyber crime.*

### Kegunaan Penelitian

1. **Kegunaan Teoritik**

Penelitian ini diharapkan dapat menambah pengetahuan dan pengalaman, sehingga berperan dalam pengembangan Ilmu Hubungan Internasional, khususnya mengenai potensi dan ancaman global *cyber crime* dan penanggulangan *cyber crime* oleh Pemerintahan Jepang (di Masa Perdana Menteri Shinzo Abe).

1. **Kegunaan Praktis**

Menjadi bahan dan masukan untuk membuat kebijakan terkait *cyber crime,* bagi yang berkepentingan.

## Kerangka Teoritis dan Hipotesis

### Kerangka Teoritis

1. **Keamanan Non Tradisional**

Konsep keamanan selama ini memang hanya merujuk pada sifat ancaman yang bersifat militer semata dan memfokuskan pada aspek negara (Keamanan Tradisional). Akan tetapi, konsep keamanan kini dapat dikaji sebagai pengaruh dari masing-masing posisi ekstrim antara kekuatan dan perdamaian. Isu-isu yang mengancam kelangsungan hidup suatu negara akan dipandang sebagai ancaman yang eksistensial. Menurut Buzan, keamanan berkaitan dengan masalah kelangsungan hidup (*survival*). Buzan membagi keamanan kedalam 5 dimensi yaitu, politik, militer, ekonomi, sosial, dan lingkungan.[[19]](#footnote-19)

Adanya nilai-nilai baru pada masyarakat di era global, membuat mengemukanya keamanan non-tradisional. Mengemukanya berbagai konflik komunal disekitar masyarakat, tidak terlepas dari dua persoalan besar, yaitu perkembangan yang terjadi di dunia internasional (globalisasi) dan semangat partikularisme domestik dan transnasional (yang bisa jadi merupakan “*reaction against globalization”*).[[20]](#footnote-20)

Globalisasi telah memunculkan kecenderungan similaritas dan uniformitas dari para individu, kelompok dan sistem sosial yang melewati dan atau bahkan menghapus batas tradisional negara (*vanishing traditional borders).* Dengan demikian, globalisasi memunculkan aktor-aktor baru, seperti gerakan separatis, kelompok-kelompok teroris internasional, dan kelompok penjahat lintas batas (*transnational criminal organizations*).[[21]](#footnote-21)

1. Pendekatan Keamanan Non-Tradisional

Keamanan non-tradisional merupakan keamanan komprehensif (*comprehensive security*) yang menekankan pada aspek ancaman apa yang dihadapi oleh negara. Kandungan politik keamanan komprehensif adalah upaya menciptakan kestabilan dan ketertiban yang mencakup semua aspek keamanan.[[22]](#footnote-22) Hal tersebut diperkuat oleh Terry Terriff, et al yang mengemukakan, ancaman dalam kajian Keamanan non-tradisional memiliki empat karakteristik umum. Pertama, sebagian besar besar bagian dari masalah tidak bersifat state-centred, tetapi lebih berdasarkan pada faktor atau aktor non negara. Kedua, ancaman keamanan tidak memiliki suatu wilayah geografis tertentu. Ketiga, ancaman tersebut tidak mampu diselesaikan hanya dengan mengandalkan kebijakan keamanan tradisional. Keempat, sasaran ancaman adalah individu dan Negara.[[23]](#footnote-23)

Oleh karenanya, faktor yang menjelaskan perkembangan ini yaitu proses globalisasi dan perkembangan teknologi informasi, demokratisasi dan hak-hak asasi manusia, masalah lingkungan hidup, masalah ekonomi, sosial, dan budaya.

Jonathan Kirshner dalam bukunya *Globalization and National Security* mengatakan bahwa globalisasi adalah singkatan untuk berbagai fenomena yang berasal dari kekuatan-kekuatan terorganisir dan tanpa kewarganegaraan, tetapi yang menghasilkan tekanan yang dirasakan oleh negara. Globalisasi disini menyangkut konsekuensi-konsekuensi politis hubungan antara dua (atau lebih) Negara, globalisasi juga adalah sinonim untuk subnasional, transnasional, regional, atau supranasional bentuk organisasi politik.[[24]](#footnote-24)

Pendekatan non-tradisional (*soft / low security*) ini memiliki fokus misalnya pada keamanan ekonomi dan perdagangan, lingkungan, energi, budaya, dan masalah-masalah sosial lainnya.

Selain itu pendekatan keamanan non-tradisional ini pun berlaku jika Negara menghadapi tekanan dari lingkungan domestik dan lingkungan internasional. Lingkungan domestik disini yaitu seperti tekanan individu, LSM, dan kelompok masyarakat akibat proses demokratisasi dan penyebaran nilai-nilai hak asasi manusia. Sedangkan lingkungan internasional yaitu tekanan yang berasal dari transaksi-transaksi dan isu-isu yang melewati batas-batas nasional negara, misalnya transaksi ekonomi, penyebaran informasi, migrasi, masalah lingkungan hidup, kejahatan internasional, dan lainnya.[[25]](#footnote-25)

1. Asumsi Pendekatan Keamanan Non-Tradisional

Terdapat 6 asumsi (landasan) pendekatan keamanan non-tradisional, yaitu:[[26]](#footnote-26)

1. Keamanan seluruh entitas politik di bawah negara *(non-state actors).*
2. Negara menghadapi tekanan dari lingkungan domestik dan lingkungan internasional.
3. Negara menyerahkan kedaulatannya kepada entitas internasional.
4. Keamanan bersifat multi dimensional dan kompleks tidak hanya bersifat ancaman militer.
5. Negara dapat menjadi sumber ancaman keamanan warga negara.
6. ***Cyber Crime***
	* + - 1. Pengertian *Cyber Crime*

*Cyber crime* terdiri dari dua kata, yakni *‘cyber’* dan *‘crime’.* Kata *‘cyber’* merupakan singkatan dari ‘*cyberspace’,* yang berasal dari kata *‘cybernetics’* dan *‘space’* Istilah *cyberspace* muncul pertama kali pada tahun 1984 dalam novel William Gibson yang berjudul *Neuromancer[[27]](#footnote-27).*

Indra Safitri (dalam Maskun) mengemukakan bahwa kejahatan dunia maya (*cyber crime)* adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakterisktik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas sebuah informasi yang disampaikan dan diakses oleh pelanggan *internet[[28]](#footnote-28).*

Dalam Bahasa Indonesia, *‘cyber crime’* dapat diartikan sebagai ‘kejahatan siber’. Hal ini sesuai dengan istilah yang digunakan oleh Ahmad M. Ramli untuk mengartikan *‘cyber law’*, yang padanan katanya ‘hukum siber’. Namun ada juga pakar yang mengidentikkan istilah *cyber* dengan dunia maya. Sehingga mereka menggunakan istilah ‘kejahatan mayantara’ atau ‘kejahatan dunia maya.’[[29]](#footnote-29)

* + - * 1. Motif – motif *Cyber Crime.[[30]](#footnote-30)*
1. *Cyber crime* sebagai tindakan kejahatan murni

Merupakan motif dimana orang yang melakukan kejahatan yang dilakukan secara di sengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengrusakkan, pencurian, tindakan anarkis, terhadap suatu sistem informasi atau sistem komputer.

1. *Cyber crime* sebagai tindakan kejahatan abu-abu :

Merupakan motif dimana kejahatan ini tidak jelas antara kejahatan kriminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer tersebut.

1. Sasaran *Cyber Crime*

Terdapat beberapa sasaran yang menjadi motif para pelaku *cyber crime* yaitu sebagai berikut: [[31]](#footnote-31)

1. *Cyber crime* yang menyerang individu :

Kejahatan yang dilakukan terhadap orang lain dengan motif tertentu yang bertujuan untuk merusak nama baik, mencoba ataupun mempermainkan seseorang untuk mendapatkan kepuasan pribadi. Contoh : Pornografi, *cyberstalking*, dll.

1. *Cyber crime* yang menyerang hak cipta (Hak milik) :

Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi/ umum ataupun demi materi/ nonmateri.

1. *Cyber crime* yang menyerang pemerintah :

Kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan teror, membajak ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan, atau menghancurkan suatu Negara

1. Sifat *Cyber Crime*

*Cyber crime* bersifat lintas batas nasional (t*ransnational*). Berikut ini merupakan karakteristik dari “*transnational crime*” (pasal 3 ayat 2 “*Palermo Conventions Organizational Crime*):[[32]](#footnote-32)

1. Dilakukan di lebih dari satu Negara
2. Dilakukan disatu Negara, namun sebagian besar persiapan, perencanaan, arahan dan kendalinya berlangsung di Negara lain
3. Dilakukan disuatu Negara namun melibatkan kelompok criminal terorganisir yang terkait dengan kegiatan kriminal dilebih dari satu negara.
4. Dilakukan di suatu Negara namun mempunyai efek yang subtansial dinegara lain
5. Sifat anomity, dalam dunia internet memungkinkan seseorang untuk tetap *“anonymous”,* yaitu tetap menyembunyikan indentitasnya ketika berkomunikasi secara *online*.
6. Bentuk – bentuk *Cyber Crime* antara lain: [[33]](#footnote-33)
7. *Unauthorized Access to Computer System and Service*

Kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan *(cracker)* melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet.

1. *Illegal Contents*

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.

1. *Data Forgery*

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.

1. *Cyber Espionage*

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer *(computer network system)* pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized.*

1. *Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb,* virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism.*

1. *Offense against Intellectual Property*

Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

1. *Infringements of Privacy*

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized,* yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

### Hipotesis

Berdasarkan hal-hal yang telah dikemukakan diatas, peneliti mengajukan hipotesis sebagai berikut : “Karena ancaman global *cyber crime* meningkat, direspon Pemerintahan Jepang di masa perdana menteri Shinzo Abe dengan menanggulangi *cyber crime*

### Operasional Variabel dan Indikator

**Tabel 1
Tabel Operasional Variabel dan Indikator Penelitian**

|  |  |  |
| --- | --- | --- |
| **Variabel dalam Hipotesis (Teoritik)** | **Indikator (Empirik)** | **Verifikasi (Analisis)** |
| *Variabel Bebas :*Karena ancaman global *cyber crime* meningkat, | 1. Perkembangan *Internet User* di Dunia
 | 1. Data Meningkatnya *Internet User* di Dunia.

Sumber : Internet Users by Country (2014) – finalized <http://www.internetlivestats.com/internet-users-by-country/2014/>.  |
| 1. Kerugian dari dampak *cyber crime*
 | 1. Data Besarnya kerugian akibat aktivitas *cyber crime*

Sumber : Ponemon Institute<http://resources.idgenterprise.com/original/AST-0130677_2014_US_Cost_of_Cyber_Crime_Study_FINAL_2.pdf>.  |
| 1. Insiden-insiden *cyber crime* di Dunia global
 | 1. Data Banyaknya Insiden *cyber crime* di Dunia global.

<https://csis-prod.s3.amazonaws.com/s3fs-public/171128_Significant_Cyber_Events_List.pdf?hXm.gQgDa5udj_hCMCrkHZsosRLvVE2k\>.  |
| *Variabel Terikat :*Direspon Pemerintahan Jepang di masa perdana menteri Shinzo Abe dengan menanggulangi *cyber crime*  | 1. Peran pemerintahan Shinzo abe dalam menanggulangi *cyber crime* di Jepang
 | 1. Penguatan fungsi *National Information Security Center* dan pembuatan sistem baru di *Government Security Operation Coordination team*

Sumber: *Cyber Security Strategy: Towards a world-leading, resilient, and vigorous cyberspace*[www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf](http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf). |
| 1. Pembentukan *cyber* *security strategy*

Sumber: *Information Security Policy Council*, 2013. <http://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-027-en.html>.  |
| 1. Jepang memperhatikan infrastruktur nasional dengan membuat sistem *Capability for Engineering of Protection, Technical Operation, Analysis and Response.*

Sumber: *Information Security Policy Council, 2013.*<http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf> |
| 1. Berkolaborasi dengan Perusahaan swasta, Lembaga Pendidikan dan Penelitian dengan program *New Information Security Outreach Awerness Program.*

Sumber: *Cyber Policy Council.* <http://www.nisc.go.jp/eng/pdf/CYBERSECURITY_ANNUAL%20REPORT_2013_eng.pdf>.  |
| 1. Membentuk *cyber defense unit*

Sumber: *Cyber Policy Council, Ministry of Defense.* [*http://www.mod.go.jp/e/jdf/no42/specialfeature.html*](http://www.mod.go.jp/e/jdf/no42/specialfeature.html)*.* |
| 1. Hambatan pemerintah Jepang dalam menanggulangi *cyber crime*
 | 1. Data hambatan Pemerintahan jepang dalam menanggulangi *cyber crime.*

Sumber: *Isaac Stone Fish, foreign policy*<http://foreignpolicy.com/2013/06/10/we-face-a-very-serious-chinese-military-threat/> |
| 1. Upaya Pemerintah Jepang dalam menanggulangi *cyber crime*
 | 1. Membangun kerjasama internasional terkait dunia maya, dengan aktif mengambil bagian dalam diskusi *Group of Government Expert* PBB.

Sumber: *UNITED NATIONS*, 2013. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. dalam <http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf>.  |
| 1. Membangun kerjasama bilateral Jepang-Amerika Serikat untuk meningatkan keamanan di bidang *cyber*

Sumber : SSRC.2013.<http://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-051-en.html>.  |
| 1. Membangun kerjasama multilateral Jepang-ASEAN untuk menanggulangi *cyber crime* dan upaya pembentukan kebijakan

Sumber : Join Ministerial Statement of the ASEAN-*Japan Ministerial Policy Meeting on Cybersecurity Coorperation*.2013.<http://www.meti.go.jp/press/2013/09/20130913005/20130913005-5.pdf> |

### Skema Kerangka Teoritis

**Skema 1
Skema Kerangka Teoritis**

****

## Metode dan Teknik Pengumpulan Data

### Tingkat Analisis

Pada penelitian ini, tingkat analisis yang digunakan peneliti adalah dengan cara berfikir deduktif untuk menganalisis data, yang bertujuan untuk menyederhanakan sehingga mudah untuk ditafsirkan. Metode deduktif adalah metode yang digunakan untuk menganalisis sesuatu yang spesifik, yang dihasilkan dan unit eksplanasi yang lebih tinggi.

Unit eksplanasi yang digunakan dalam penelitian ini adalah potensi dan ancaman *cyber crime,* khususnya yang terjadi di Jepang, yang menjadi agenda keamanan sehingga diperlukan adanya respon yang intensif untuk menanggapi ancaman tersebut. Metode penelitian secara deduksi merupakan penelitian yang dilakukan berupa penerapan teori, berangkat dari teori yang sudah ada, yang selanjutnya menjadi pegangan untuk membuat argumen utama dan akhirnya akan diuji kebenarannya melalui observasi fakta empiris.[[34]](#footnote-34)

### Metode Penelitian

Metode penelitian yang digunakan penulis dalam penelitian ini adalah metode deskriptif, yaitu metode deskriptif dengan pendekatan analitis. Penelitian deskriptif bertujuan untuk mendeskripsikan apa yang sedang berlaku. Di dalamnya terdapat upaya mendeskripsikan, mencatat, analisis, dan menginterpretasikan kondisi-kondisi yang sekarang ini terjadi atau ada. [[35]](#footnote-35)Metode inilah yang digunakan untuk menjelaskan potensi dan ancaman *cybercrime,* khususnya penanggulangan yang dilakukan oleh pemerintahan Jepang.

### Teknik Pengumpulan Data

Teknik pengumpulan data yang peneliti gunakan dalam penelitian ini adalah teknik studi kepustakaan atau *library research.* Teknik studi kepustakaan dipilih karena dalam penelitian ini peneliti menggunakan data-data sekunder, yaitu berupa jurnal hasil penelitian, website resmi, buku teks, dokumen, majalah berita, surat kabar, laporan lembaga pemerintah dan data-data yang terkumpul dalam berbagai artikel ilmiah.

## Lokasi dan Lamanya Penelitian

Untuk mendapatkan data dan informasi yang berhubungan dengan permasalahan-permasalahan yang diteliti, lembaga yang akan penulis ambil sebagai penunjang laporan skripsi adalah sebagai berikut :

### Lokasi Penelitian

1. Badan Perpustakaan dan Kearsipan Daerah Jawa Barat

Jl. Kawaluyaan Indah II No. 4, Jatisari, Buahbatu, Kota Bandung, Jawa Barat 40286, Indonesia

1. Perpustakaan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Pasundan

Jl. Lengkong Besar No. 68, Cikawao, Lengkong, Kota Bandung, Jawa Barat 40261, Indonesia.

### Lama Penelitian

**Tabel 2
Tabel Lamanya Penelitian**

|  |  |  |
| --- | --- | --- |
| **No.** | **Tahun****Bulan****Minggu** **Kegiatan** | **2017 - 2018** |
| **September** | **Oktober** | **November** | **Desember** | **Januari** | **Februari** |
| **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** |
| 1 | Tahap Persiapan1. Konsultasi Judul
 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1. Pengajuan Judul
 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Penelitian Lapangan1. Pengurusan surat ijin
 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1. Kepustakaan
 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Pengolahan Data |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Analisa Data |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | Kegiatan Akhir1. Pelaporan
 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1. persiapan & Draft
 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1. perbaikan hasil draft
 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1. seminar skripsi
 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Sistematika Penulisan

Sistematika penelitian ini terdiri dari 5 Bab dari masing-masing bab akan dibagi menjadi beberapa sub bab yang akan menjelaskan sebagai secara detail. Berikut adalah sistematika penulisannya :

**BAB 1 Pendahuluan :** Berisi latar belakang masalah, identifikasi masalah, pembatasan masalah, rumusan masalah, tujuan dan kegunaan penelitian, kerangka teoritis, hipotesis, metode penelitian dan teknik pengumpulan data, lokasi penelitian, jadwal dan kegiatan penelitian, sistematika penelitian.

**BAB 2 Pembahasan Variabel Bebas :** Berisi pembahasan potensi dan ancaman global *cyber crime*.

**BAB 3 Pembahasan Variabel Terikat :** Berisi pembahasan yang meliputi potensi dan ancaman *cyber crime* terhadap keamanan nasional di Jepang.

**BAB 4 Pembahasan Analisis :** Berisi hasil analisa atas variabel bebas dan terikat dengan menguraikan peran, hambatan, dan upaya pemerintahan Shinzo Abe dalam menanggulangi *cyber crime* di Jepang.

**BAB 5 Simpulan :** Berisi simpulan dari hasil penelitian yang dibahas.

1. Ari Juliano Gema, “*Cyber Crime* Sebuah Fenomena Di Dunia Maya”, dalam *National Central Bureau* (*NCB) – INTERPOL Indonesia*, Jakarta, 02 Januari 2013 dalam <http://www.interpol.go.id/id/kejahatan-transnasional/kejahatan-dunia-maya/89-cybercrime-sebuah-fenomena-di-dunia-maya>*,* diakses 5 Oktober 2017. [↑](#footnote-ref-1)
2. James R. Richards *Transnational Criminal Organizations, Cybercrime & Money Laundering.Florida*. Hal- 87. [↑](#footnote-ref-2)
3. Kenny Wiston, 2002, *The Internet: Issues of Jurisdiction and Controversies Surrounding Domain Names*, Bandung, Citra Aditya, hlm 7. [↑](#footnote-ref-3)
4. Internet World Stats, *Internet Users by Country*, 2014 dalam <http://www.internetlivestats.com/internet-users-by-country/2014/> diakses pada 5 Oktober 2017. [↑](#footnote-ref-4)
5. James R. Richards, Loc.Cit. [↑](#footnote-ref-5)
6. Maskun, Kejahatan Siber (Cyber Crime); Suatu Pengantar (Jakarta, Kencana 2013), hlm. 48. [↑](#footnote-ref-6)
7. Ari Juliano Gema, Loc.Cit. [↑](#footnote-ref-7)
8. Samuel C. McQuade, 2009, *Encyclopedia Of Cybercrime, London, Greenwood Press*, page 38. [↑](#footnote-ref-8)
9. *Significant Cyber Incidents Since* 2016, dalam <https://csis-prod.s3.amazonaws.com/s3fs-public/171128_Significant_Cyber_Events_List.pdf?hXm.gQgDa5udj_hCMCrkHZsosRLvVE2k\>, diakses pada tanggal 28 November 2017. [↑](#footnote-ref-9)
10. Jonathan Krishner, 2006. *Globalization and National Security.* (edited volume, Routledge, 2006) New York, hlm.1-2. [↑](#footnote-ref-10)
11. Anak Agung Banyu Perwita dan Yanyan Mochamad Yani, *Pengantar Ilmu Hubungan Internasional* (Bandung: PT REMAJA ROSDAKARYA, 2005, Hlm. 128. [↑](#footnote-ref-11)
12. *Significant Cyber Incidents Since* 2016, dalam <https://csis-prod.s3.amazonaws.com/s3fs-public/171128_Significant_Cyber_Events_List.pdf?hXm.gQgDa5udj_hCMCrkHZsosRLvVE2k\>, diakses pada tanggal 6 Oktober 2017. [↑](#footnote-ref-12)
13. *SPAMfighter News. 2012. Virus Strikes Computer at Japan’s Space Agency, dalam* [*www.spamfighter.com/News-17323-Virus-Strikes-Computer-at-Japans-Space-Agency.htm*](http://www.spamfighter.com/News-17323-Virus-Strikes-Computer-at-Japans-Space-Agency.htm)*,* diakses pada tanggal 6 Oktober 2017. [↑](#footnote-ref-13)
14. Pierluigi Paganini. *2012. Japan under cyber attack. The cyber threat China,* dalam[*http://securityaffairs.co/wordpress/1911/cyber-warfare-2/japan-under-cyber-attack-the-cyber-threat-china.html*](http://securityaffairs.co/wordpress/1911/cyber-warfare-2/japan-under-cyber-attack-the-cyber-threat-china.html)*,* diakses pada tanggal 6 Oktober 2017 [↑](#footnote-ref-14)
15. Ibid. [↑](#footnote-ref-15)
16. *Japan parliament hit by China-based cyberattack. 2011*, dalam <http://www.spacewar.com/reports/Japan_parliament_hit_by_China-based_cyberattack_999.html>, diakses pada tanggal 6 Oktober 2017. [↑](#footnote-ref-16)
17. Ibid. [↑](#footnote-ref-17)
18. Mohit Kumar. 2012. *Anonymous Hacks Japanese Government Websites against Anti-Piracy Laws in Japan,* dalam <http://thehackernews.com/2012/06/anonymous-hacks-japanese-government.html>, diakses pada tanggal 6 Oktober 2017. [↑](#footnote-ref-18)
19. Anak Agung Banyu Perwita dan Yanyan Mochamad Yani, *Pengantar Ilmu Hubungan Internasional* (Bandung: PT REMAJA ROSDAKARYA, 2005, Hlm. 121-122. [↑](#footnote-ref-19)
20. Ibid. Hlm. 125. [↑](#footnote-ref-20)
21. Ibid. Hlm. 126. [↑](#footnote-ref-21)
22. Ibid Hlm. 128. [↑](#footnote-ref-22)
23. Terry Terriff, et.al. 1999. *Security Studies Today.* Cambridge: Polity Press. Hlm. 115-116 [↑](#footnote-ref-23)
24. Jonathan Krishner, 2006. *Globalization and National Security.* (edited volume, Routledge, 2006) New York, hlm.1-2. [↑](#footnote-ref-24)
25. Anak Agung Banyu Perwita dan Yanyan Mochamad Yani, Loc.Cit. [↑](#footnote-ref-25)
26. Ibid. Hlm. 128. [↑](#footnote-ref-26)
27. Hengky Afrinata, Teknologi *Cyber, Cyber Space*, 2 Juni 2015 (kompasiana), dalam <https://www.kompasiana.com/lamigos/teknologi-cyber-cyberspace_557217f3307a614e38ad23ca>, diakses pada tanggal 6 Oktober 2017. [↑](#footnote-ref-27)
28. Maskun, Kejahatan Siber (Cyber Crime); Suatu Pengantar (Jakarta, Kencana 2013), hlm. 48. [↑](#footnote-ref-28)
29. Ahmad M. Ramli, Cyberlaw dan HAKI dalam Sistem Hukum Indonesia, PT. Refika Aditama, Bandung, 2010, Hlm.2. [↑](#footnote-ref-29)
30. Kejahatan Dengan Menggunakan Sarana Teknologi Informasi, dalam <http://business-law.binus.ac.id/2016/07/31/kejahatan-dengan-menggunakan-sarana-teknologi-informasi/>, diakses pada tanggal 6 Oktober 2017. [↑](#footnote-ref-30)
31. Ibid. [↑](#footnote-ref-31)
32. UNODC, “UNITED NATIONS CONVENTION AGAINST TRANSNASIONAL ORGANIZED CRIME AND THE PROTOCOLS THERETO”, dalam <https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf>, diakses pada tanggal 6 Oktober 2017. Hlm.6. [↑](#footnote-ref-32)
33. #####  Ari Juliano Gema, “*Cyber Crime* Sebuah Fenomena Di Dunia Maya”, dalam *National Central Bureau* (*NCB) – INTERPOL Indonesia*, Jakarta, 02 Januari 2013 dalam <http://www.interpol.go.id/id/kejahatan-transnasional/kejahatan-dunia-maya/89-cybercrime-sebuah-fenomena-di-dunia-maya>*,* diakses pada tanggal 7 Oktober 2017.

 [↑](#footnote-ref-33)
34. Mochtar Mas’oed. 1990. *Ilmu Hubungan Internasional, Disiplin dan Metodologi*. Jakarta: LP3ES. Hlm. 117. [↑](#footnote-ref-34)
35. Mardalis, Metode Penelitian; Suatu Pendekatan Proposal, Jakarta : Bumi Aksara, 1995, p. 26 [↑](#footnote-ref-35)