STRATEGI INDONESIA DALAM MENGHADAPI KONSTELASI SIBER GLOBAL

INDONESIA'S STRATEGY IN FACING THE GLOBAL CYBER CONSTELLATION

SKRIPSI

Oleh:

BAYU FARIS ARGANATA

NIM 120910101036

JURUSAN ILMU HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS JEMBER

2019

STRATEGI INDONESIA DALAM MENGHADAPI KONSTELASI SIBER GLOBAL

INDONESIA'S STRATEGY IN FACING THE GLOBAL CYBER CONSTELLATION

SKRIPSI

Diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat untuk menyelesaikan studi pada Program Studi Ilmu Hubungan Internasional (S1) dan mencapai gelar Sarjana Sosial

Oleh:

BAYU FARIS ARGANATA

NIM 120910101036

JURUSAN ILMU HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS JEMBER

2019

PERSEMBAHAN

Segala puji bagi Allah Subhanahu Wata'ala Tuhan Semesta Alam atas rahmat, ridho, serta berkat yang telah diberikan-Nya, sehingga skripsi ini dapat terselesaikan. Skripsi ini saya persembahkan untuk:

1. Kedua orang tua saya, Almarhum Bapak Noor Cholis dan Almarhumah Ibu Sri Banah
2. Saudara saya Wahyu Pribadi Putra, Heru Suprayogi, dan Dina Febri Aquaristi
3. Para sahabat
4. Dosen serta staff Perguruan Tinggi
5. Almamater Fakultas Ilmu Sosial dan Ilmu Politik Jurusan Ilmu Hubungan Internasional Universitas Jember

MOTTO

"IT HAS BECOME APPALLINGLY OBVIOUS THAT OUR TECHNOLOGY HAS EXCEEDED OUR HUMANITY"

(JELAS MENJADI MENGGEMPARKAN BAHWA TEKNOLOGI TELAH MELAMPAUI KEMANUSIAAN KITA)

–ALBERT EINSTEIN[1]–

[1] Albert Einstein. 14 Agustus 2015. Teknologi Menurut Seorang Albert Einstein. Jagokata.com. diakses pada tanggal 29 Desember 2018.

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Bayu Faris Arganata

NIM : 120910101036

menyatakan dengan sesungguhnya bahwa karya ilmiah yang berjudul **"STRATEGI INDONESIA DALAM MENGHADAPI KONSTELASI SIBER GLOBAL"** adalah benar-benar hasil karya sendiri, kecuali kutipan yang sudah saya sebutkan sumbernya, belum pernah diajukan pada institusi manapun, dan bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa ada tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika ternyata di kemudian hari pernyataan ini tidak benar.

Jember, 14 Januari 2019
Yang menyatakan,

Bayu Faris Arganata
NIM 120910101036

SKRIPSI

STRATEGI INDONESIA DALAM MENGHADAPI KONSTELASI SIBER GLOBAL

INDONESIA'S STRATEGY IN FACING THE GLOBAL CYBER CONSTELLATION

Oleh:

Bayu Faris Arganata

NIM 120910101036

Pembimbing

Dosen Pembimbing Utama : Dra. Sri Yuniati, M.Si

Dosen Pembimbing Anggota : Adhiningasih P. S.Sos, M.Si

PENGESAHAN

Skripsi berjudul "Strategi Indonesia dalam Menghadapi Konstelasi Siber Global" telah diuji dan disahkan pada:

Hari : Senin

Tanggal : 14 Januari 2019

Waktu : 09:00 WIB

Tempat : Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jember

Tim Penguji:

Ketua

Drs. Agung Purwanto, M.Si.
NIP 196810221993031002

Sekretaris I

Dra. Sri Yuniati, M.Si
NIP 196305261989022001

Sekretaris II

Adhiningasih P. S.Sos, M.Si
NIP 197812242008122001

Anggota II

Fuat Albayumi, S.IP., MA.
NIP 197404242005011002

Mengesahkan
Dekan,

Dr. Ardiyanto, M. Si
195808101987021002

RINGKASAN

Strategi Indonesia dalam Menghadapi Konstelasi Siber Global : Bayu Faris Arganata, 120910101036 : 2018 : 79 Halaman : Jurusan Hubungan Internasional Fakultas Ilmu Sosial dan Politik Universitas Jember.

Perkembangan teknologi memunculkan internet sebagai sesuatu yang bisa digunakan dan dimanfaatkan untuk banyak hal. Internet dijadikan sebagai alat untuk berkomunikasi, berbisnis, mengelola seluruh data administrasi dan data pribadi, sekaligus sebagai media penyimpanan data itu sendiri. Karena semua hal itu, maka terjadilah sebagian proses kehidupan manusia di sebuah ruang maya yang terhubung dengan koneksi internet. Ruang maya tersebut dikenal sebagai dunia siber. Perkembangan dunia siber telah menciptakan berbagai macam fenomena siber. Pada satu sisi mendatangkan manfaat, di sisi lain mendatangkan bahaya bagi pengguna. Indonesia merupakan negara dengan jumlah pengguna internet yang begitu banyak dan pertumbuhannya sangat pesat setiap tahunnya. Masyarakat Indonesia menggunakan internet untuk banyak hal. Mulai dari pendidikan, pemerintahan, perbankan, komunikasi, dan masih banyak lainnya. Dengan begitu, Indonesia menjadi salah satu negara yang sangat aktif dalam memanfaatkan keberadaan dunia siber. Hal tersebut tentunya membuat pemerintah Indonesia menyusun strategi untuk menanggapi adanya ancaman serius di dunia siber yang mampu mengganggu stabilitas keamanan negara. Skripsi ini memaparkan tentang strategi yang disusun oleh pemerintah Indonesia dalam menyikapi dan menghadapi segala kemungkinan buruk yang terjadi kepada Indonesia akibat adanya konstelasi siber global.

Penulisan skripsi ini menggunakan metode penelitian studi literatur dengan mencari data-data sekunder yang sesuai untuk menjelaskan permasalahan. Pengumpulan data yang digunakan lebih difokuskan pada informasi yang berasal dari buku, jurnal, surat kabar cetak maupun elektronik, dan data berupa artikel yang bersumber dari internet yang terkait dengan topik permasalahan. Data yang telah terkumpul kemudian dianalisis dengan menggunakan metode deskriptif kualitatif. Konsep yang digunakan dalam menganalisis permasalahan ini adalah

konsep strategi keamanan dan konsep keamanan nasional yang dianggap sesuai untuk menjelaskan strategi yang dibuat oleh Pemerintah Indonesia dalam menghadapi konstelasi siber global.

Indonesia menyusun kebijakan strategi untuk meghadapi gelombang fenomena siber yang mencakup ancaman dan kejahatannya dengan membentuk institusi pemerintahan yang langsung berada di bawah komando presiden untuk menjadi poros koordinasi dalam menanggapi segala hal tentang dunia siber, institusi tersebut bernama Badan Siber dan Sandi Negara (BSSN). Selain BSSN, Indonesia juga membentuk *Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center* (Id-SIRTII/CC) sebagai organisasi resmi dan khusus dalam bidang pemanfaatan teknologi komunikasi berbasis internet. Pemerintah Indonesia juga menggelar program pelatihan yang bertujuan untuk menjaring talenta Warga Negara Indonesia (WNI) dalam menjalankan tugas sebagai tentara siber, program tersebut diberi nama *Born To Control*. Ketiga hal yang dilakukan tersebut merupakan upaya reaksi dan tindakan yang dilakukan oleh Indonesia untuk menciptakan rasa aman bagi masyarakat dan negara.

.

PRAKATA

Segala puji syukur penulis haturkan kepada Allah SWT yang telah memberikan anugerah, keajaiban, rahmat, nikmat, serta karunia-Nya yang begitu banyak sehingga penulis dapat menyelesaikan skripsi yang berjudul **"Strategi Indonesia dalam Menghadapi Konstelasi Siber Global"**. Skripsi ini disusun untuk memenuhi salah satu syarat dalam menyelesaikan pendidikan strata satu (S1) pada jurusan Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jember. Selesainya pengerjaan skripsi ini tidak lepas dari bimbingan, bantuan dan dukungan dari berbagai pihak. Oleh karena itu penulis menyampaikan banyak terima kasih kepada:

1. Bapak Dr. Ardiyanto, M.Si., selaku Dekan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jember,
2. Bapak Drs. Bagus Sigit Sunarko, M.Si, Ph.D selaku Ketua Jurusan Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jember,
3. Ibu Dra. Sri Yuniati, M.Si dan Ibu Adhiningasih P. S.Sos, M.Si selaku Dosen Pembimbing selama penulis menyusun skripsi,
4. Bapak Dr. Muhammad Iqbal S.Sos, M.Si selaku Dosen Pembimbing Akademik,
5. Seluruh Dosen dan Staff Jurusan Ilmu Hubungan Internasional,
6. Almarhum kedua orang tua saya, Bapak Noor Cholis dan Ibu Sri Banah yang semasa hidupnya selalu memberikan dukungan, doa, nasehat, serta semangat bagi penulis untuk penyelesaian skripsi ini,
7. Kakak-kakak saya; Wahyu Pribadi Putra & Evi Kusumawati, Heru Suprayogi & Chanira Nuansa Bunga, Dina Febri Aquaristi & M. Siswandi yang tiada henti memberikan dukungan untuk segera menyelesaikan skripsi ini,
8. Sahabat perantauan; Hilman Thonthowi, Alif Fauzan, Muhammad Taufik Qurrahman, Pandu Pratama Yuda, Aad Rifqy, dan Syah Thanthawi,

9. Sunjava's People; Eric Dwiharta dan Ipung Sudrajat,
10. Klub Kopi My Way; Wildan FU, Fajryan, Egar, Adhyt, Tri, Rekka, Eva, Dewi, Kiki, Bahrul, Bima, dan Radix,
11. Para rekan seperjuangan, Mahasiswa Hubungan Internasional Universitas Jember terutama angkatan 2012,
12. Semua pihak yang tidak dapat disebutkan satu per satu atas bantuannya dalam penyelesaian skripsi ini.

Dalam penulisan skripsi ini tentu masih terdapat kekurangan dan kesalahan. Oleh karena itu penulis menerima segala kritik dan saran demi kesempurnaan skripsi ini. Akhirnya penulis berharap, semoga skripsi ini dapat memberikan manfaat.

Jember, 14 Januari 2019

Penulis

DAFTAR GAMBAR

2.1 Sumber-sumber Ancaman Siber.....19
2.2 Dampak teknologi sebagai privasi.....22
3.1 Tabel Negara Jumlah Pengguna Internet Terbanyak 35
3.2 Penetrasi Pengguna Internet di Indonesia.....36
3.3 Negara Asal Serangan Siber.....46

DAFTAR SINGKATAN

APJII	: Asosiasi Penyelenggara Jasa Internet Indonesia
BSSN	: Badan Siber dan Sandi Negara
CIA	: *Central Intelligence Agency*
CNII	: *Critical National Information Infrastructure*
FBI	: *Federal Beureau Investigation*
Id-SIRTII/CC	: *Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center*
KOMINFO	: Kementerian Komunikasi dan Informatika Republik Indonesia
KUHP	: Kitab Undang-undang Hukum Pidana
P3K	: Pengkajian dan Pengembangan Kebijakan
Perpes	: Peraturan Presiden
SCADA	: *Supervisory Control dan Data Acquisition*
UU	: Undang-undang

DAFTAR ISI

HALAMAN JUDUL ..... **i**
PERSEMBAHAN ..... **ii**
MOTTO ..... **iii**
PERNYATAAN ..... **iv**
LEMBAR BIMBINGAN ..... **v**
HALAMAN PENGESAHAN ..... **vi**
RINGKASAN ..... **vii**
PRAKATA ..... **ix**
DAFTAR GAMBAR ..... **xi**
DAFTAR SINGKATAN ..... **xii**
DAFTAR ISI ..... **xiii**
BAB 1. PENDAHULUAN **1**
1.1 Latar Belakang **1**
1.2 Ruang Lingkup Pembahasan **5**
1.2.1 Batasan Materi 5
1.2.2 Batasan Waktu 5
1.3 Rumusan Masalah **6**
1.4 Tujuan Penelitian **6**
1.5 Kerangka Konseptual **6**
1.5.1 Konsep Strategi Keamanan 7
1.5.2 Konsep Keamanan Nasional 9
1.6 Argumen Utama **11**
1.7 Metode Penelitian **11**
1.7.1 Teknik Pengumpulan Data 11
1.7.2 Teknik Analisis Data 12
1.8 Sistematika Penulisan **12**
BAB 2. KONSTELASI SIBER GLOBAL **14**
2.1 Kemunculan Dunia Siber **14**

2.2 Ancaman Dunia Siber 15
2.3 *Cyber Crime* 19
2.4 *Cyber Terorrism* 24
2.5 Hukum Siber 28
BAB 3. DINAMIKA SIBER DI INDONESIA 33
3.1 *Trend* Siber di Indonesia 33
3.2 Pemanfaatan Dunia Siber di Indonesia 38
3.3 Kejahatan Siber di Indonesia 41
3.4 Kejahatan Terorisme Siber di Indonesia 47
BAB 4. STRATEGI KEAMANAN SIBER DI INDONESIA 50
4.1 Hukum Siber di Indonesia 40
4.2 Pembentukan Badan Siber dan Sandi Negara (BSSN) 52
4.3 Pembentukan Indonesia *Security Incident Response Team on Internet and Infrastructure/Coordination Center* (Id-SIRTII/CC) ...60
4.4 Program *Born To Control* 66
BAB 5. KESIMPULAN 70
DAFTAR PUSTAKA 72

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi internet membuat dunia seakan-akan menjadi tidak memiliki batasan. Internet mampu menciptakan ruang atau dunia maya tersendiri, ruang atau dunia maya itu disebut dengan dunia siber. Dunia maya atau siber seakan-akan lebih aktif daripada dunia nyata. Dunia siber mampu menghubungkan orang-orang dari satu negara ke negara lain, sehingga manusia tidak mempermasalahkan lagi batas waktu dan jarak yang berpengaruh dalam aktivitasnya sehari-hari. Perkembangan dunia maya telah menciptakan berbagai macam fenomena siber. Adanya fenomena siber ini di satu sisi bisa mendatangkan manfaat, namun di sisi lain juga bisa mendatangkan bahaya. Dunia siber mampu memicu semua hal yang terintegrasi di dalamnya, seperti sistem layanan sosial, sistem kependudukan, sistem politik, sistem ekonomi, dan sistem pertahanan keamanan suatu negara. Keadaan ini menjadi titik rawan bahkan menjadi ancaman bagi negara karena bisa disalah gunakan oleh pihak yang memanfaatkan hal tersebut demi keuntungan pribadi maupun kelompok.

Konstelasi siber global telah mampu memunculkan fenomena-fenomena baru di dunia Internasional. Dunia siber dimanfaatkan sebagai media baru untuk kepentingan suatu negara. Oleh karena itu, peluang kejahatan yang terjadi dan serangan terhadap hal tersebut akan terbuka lebar. Sistem strategi harus disusun dan segera dilakukan guna meminimalisir celah yang akan dimanfaatkan untuk kegiatan yang tidak bertanggung jawab seperti *cyber crime* maupun *cyber terorrism*.

Tindak kejahatan di dunia siber terus mengalami peningkatan. Hal itu terjadi secara nyata dan semakin luas terjadi di berbagai negara di dunia. Para pelaku kejahatan siber menggunakan keahliannya untuk mengakses dan menyerang sistem politik, sosial, budaya, dan ekonomi dari satu negara ke negara lainnya. Kerawanan tersebut tentunya akan memicu hubungan diplomatis antar negara, sehingga perlu adanya suatu sistem dalam mengatasi permasalahan yang

timbul akibat keberadaan dunia siber. Kekhawatiran mengenai keberadaan dunia siber yang mampu memunculkan fenomena baru di dunia internasional ini menjadi perhatian bagi pemerintah di seluruh dunia untuk membuat sebuah sistem pengamanan bagi negaranya maupun dunia internasional (IPLURAL, 2017).

Fenomena siber tentu sering melibatkan hubungann antar negara. Masalah tersebut memerlukan kesigapan pemerintah negara untuk mengatasinya dan menjalin kerja sama dengan negara lain di dunia dalam mengatasinya, misal dengan membuat suatu sistem diplomasi siber. Sistem diplomasi siber yang dijalankan oleh beberapa negara yang sudah menggunakan sistem ini merupakan hal baru. Adanya sistem diplomasi siber diharapkan mampu menanggulangi dan memberi solusi dari berbagai permasalahan yang muncul dalam fenomena siber. Terutama di bidang keamanan siber dari suatu negara yang memiliki keterkaitan dengan pertahanan suatu negara. Keamanan siber merupakan tantangan dalam pembangunan di sektor ekonomi, sosial, dan politik untuk melaksanakan diplomasi kontemporer. Dalam konteks Indonesia, konflik siber berdasarkan ras, etnis, dan agama semakin sering terjadi, sehingga memberikan dampak pada keamanan nasional di ruang *online* atau dan *offline*.

Pada prinsipnya, pengawasan terhadap aktivitas seseorang di internet dapat melanggar hak konstitusi warga negara khususnya mengenai privasi dan kebebasan berekspresi serta berkomunikasi. Perlindungan terhadap privasi, dan kebebasan berekspresi serta berkomunikasi merupakan bagian penting dari pengembangan demokrasi dan selaras dengan instrumen internasional. Indonesia menjunjung tinggi penegakan hak asasi manusia melalui berbagai peraturan perundang-undangan yang ada. Oleh karena itu, penerapan terhadap sistem informasi yang dapat melanggar hak asasi manusia akan dilakukan *assessment* yang komprehensif untuk memastikan tidak terjadinya pelanggaran hak asasi manusia. Dalam perundang-undangan di Indonesia dikenal adanya intersepsi atau penyadapan. Hal ini dilakukan untuk kepentingan penegakan hukum berdasarkan ketentuan-ketentuan yang tetap menjaga dan menghormati hak asasi manusia (KOMINFO, 2015).

Bila melihat kondisi keamanan siber yang terjadi di Indonesia saat ini, kebutuhan untuk menyelamatkan informasi dan data-data dalam sistem tersebut sungguh sangat darurat. Oleh karena itu dibutuhkan strategi untuk memberikan gagasan sekaligus pendefinisian posisi dan strategi diplomasi siber Indonesia yang dapat meningkatkan peran internasional Indonesia dalam konstelasi siber global maupun dalam melindungi kepentingan nasional, khususnya di bidang pertahanan. Industri pengamanan siber di Indonesia otomatis sudah sangat harus dibutuhkan pula pada saat ini. Kekhawatiran terhadap serangan siber menjadi hal yang ditakuti lembaga-lembaga sosial, politik, dan bisnis di tanah air. Dengan adanya serangan dunia siber yang juga semakin kuat, akhirnya dibutuhkan tenaga profesional untuk menjadi tentara-tentara penakluk kejahatan siber.

Perkembangan internet dan umumnya dunia siber tidak selamanya menghasilkan hal-hal yang positif. Salah satu hal negatif yang merupakan efek sampingnya antara lain adalah kejahatan di dunia siber atau, *cyber crime*. Hilangnya batas ruang dan waktu di internet mengubah banyak hal. Salah satu kegiatan yang sering dilakukan oleh pelaku kejahatan siber atau yang sering disebut *cracker* adalah mengubah halaman website, yang dikenal dengan istilah *deface* (Wulan, 2014). Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Selanjutnya, bila terjadi kasus ketika seorang *cracker* membajak situs web milik instansi negara dan berhubungan dengan keamanan pemerintahan, sampai saat ini masih belum ada hukum yang dapat digunakan untuk menjerat perbuatan *cracker* ini. Masih banyak model-model kejahatan siber yang akan dilakukan seiring perkembangan teknologi internet dan semakin luasnya konstelasi siber global berkembang di dunia.

Tingkat kejahatan siber di Indonesia berada pada level darurat dan mengkhawatirkan. Menurut data yang dihasilkan oleh *State Of The Internet* pada tahun 2013 yang menyebutkan bahwa dari 497 orang di dunia yang tertangkap karena kasus kejahatan siber 108 orang diantaranya merupakan warga negara Indonesia (KOMPAS, 2015). Namun demikian, lembaga *Security Threat* di tahun yang sama juga menyebutkan bahwa Indonesia adalah negara paling beresiko mengalami serangan kejahatan siber. Hal tersebut dibuktikan dari tercatatnya 36,6

juta serangan kejahatan siber yang terjadi di Indonesia dalam kurun waktu 2012 hingga 2015. Dari kasus-kasus kejahatan siber yang terjadi di Indonesia, total kerugian mencapai Rp. 33,29 milliar. Angka yang jauh lebih besar dibandingkan perampokan nasabah bank secara konvensional (KOMPAS, 2015).

Namun demikian ironisnya, di Indonesia, kebutuhan tenaga ahli profesional di bidang *cyber security* belum dipikirkan dengan serius. Ketidakseriusan itu menjalar juga pada sistem Indonesia yang masih seperti tidak menghiraukan dengan benar-benar adanya fenomena kejahatan siber. Ketika negara-negara di dunia sibuk menyelamatkan berbagai macam hal yang terintegrasi dengan internet dan yang menimbulkan ancaman bagi negara dan masyarakatnya melalui sistem *cyber security* yang disusun, di Indonesia, kekhawatiran mengenai hal tersebut tidak nampak begitu serius. Hal tersebut dibuktikan dengan data-data yang menyebutkan bahwa serangan siber yang terjadi di Indonesia terus naik jumlahnya dari tahun ke tahun, dan masih banyaknya Warga Negara Indonesia (WNI) yang menjadi pelaku kejahatan siber dalam lingkup nasional maupun internasional.

Fenomena siber Indonesia menarik untuk dibahas lebih lanjut karena pada kenyataannya infrastruktur siber Indonesia masih lemah dibanding negara lain. Walaupun saat ini Indonesia juga sedang mengkampanyekan *cyber ethics* yang berupa seruan moral penggunaan teknologi siber yang bertanggung jawab, namun peran Internasional Indonesia dalam mendukung kebijakan siber nasional perlu diperbanyak lagi aktualisasinya (Kementerian Luar Negeri Republik Indonesia 2017). Langkah Indonesia untuk dapat berperan aktif dalam konstelasi siber global menjadi komitmen Kementerian Luar Negeri Indonesia masuk ke dalam dunia siber agar bisa memperjuangkan kepentingan Indonesia di tingkat internasional. Adanya aktualisasi lebih tinggi yang dilakukan oleh Indonesia, yaitu membuat suatu strategi yang disusun oleh Indonesia guna berperan sekaligus menghadapi konstelasi siber global.

1.2 Ruang Lingkup Pembahasan

Ruang lingkup pembahasan dalam penulisan karya ilmiah ini terbagi menjadi dua bagian, yaitu batasan materi dan batasan waktu. Ruang lingkup materi membatasi cakupan pembahasan yang nantinya juga menentukan tingkatan analisis pada konsep dan teori yang akan digunakan dalam karya ilmiah ini. dengan menetapkan ruang lingkup pembahasan, maka penulis secara komprehensif dapat menjelaskan fokus bahasan pada titik tertentu.

1.2.1 Batasan Materi

Batasan materi diperlukan dalam suatu penulisan untuk memfokuskan garis besar pembahasan masalah yang akan diteliti. Batasan materi dalam tulisan ini, penulis membatasi materi penelitian terkait penjelasan strategi yang sedang dan akan dilakukan Indonesia untuk menghadapi konstelasi siber global. Mulai dari menjelaskan konstelasi siber global yang sedang berlangsung beserta norma-norma siber internasional, dinamika siber di Indonesia, hingga merujuk pada strategi yang sudah dilakukan oleh Indonesia. Penulis juga membatasi materi pada studi kasus yang ada di Indonesia, tidak menggunakan pembanding strategi siber yang sudah dijalankan oleh negara lain.

1.2.2 Batasan Waktu

Batasan waktu dalam suatu penulisan ilmiah ditujukan untuk menegaskan rentan waktu peristiwa atau objek yang dianalisis. Batasan waktu tersebut diperlukan agar peristiwa atau objek yang dikaji tetap dalam lingkup waktu yang relevan dengan fokus pembahasan karya tulis ilmiah. Batasan waktu yang ditentukan dalam karya ilmiah ini dimulai sejak tahun 2014 sampai tahun 2017. Relevansi batasan waktu dipilih karena bertepatan dengan dimulainya maraknya fenomena kejahatan siber di Indonesia sejak tahun 2014. Mulai dari kejahatan pembajakan situs web, pencurian data negara yang disimpan secara *online*, hingga fenomena *international cyber terorist* yang menggunakan jaringan internet untuk menyebar teror dan mengancam keamanan sekaligus kestabilan negara. Pada tahun 2017 Indonesia terindikasi menjadi salah satu negara penyumbang terbanyak pelaku tindak kriminal di dunia siber (Bohang 2018). Kasus-kasus yang muncul tersebut membuat lembaga negara terkait yang utamanya yaitu

Kementerian Pertahanan dan Keamanan serta Kementerian Luar Negeri memberikan tindakan dengan menyusun strategi untuk menghadapi serta memberikan perlawanan dari Indonesia untuk konstelasi siber global.

1.3 Rumusan Masalah

Perumusan masalah diperoleh dari sebuah latar belakang penelitian. Dari latar belakang tersebut, kemudian muncul permasalahan yang harus dicari penyelesaiannya melalui proses penelitian, sehingga pada akhirnya diperoleh sebuah kesimpulan untuk menjawab permasalahan tersebut. Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka penulis merumuskan permasalahan sebagai berikut: **bagaimana strategi yang dilakukan Indonesia untuk menghadapi konstelasi siber global?**

1.4 Tujuan Penelitian

Dalam penelitian ini penulis berupaya untuk menjawab rumusan masalah dengan menggabungkan fakta-fakta yang kemudian dianalisis untuk memastikan kedudukan argumen. Secara spesifik tujuan penelitian ini menjelaskan proses dan langkah-langkah yang diambil oleh Indonesia di bidang siber dalam menghadapi konstelasi siber global.

1.5 Kerangka Konseptual

Suatu penelitian yang bersifat ilmiah memerlukan adanya teori ataupun konsep yang berfungsi sebagai instrumen analisa. Fungsi dari adanya instrumen analisa tersebut yakni sebagai acuan yang membantu penulis untuk menyederhanakan realita permasalahan yang kompleks berdasarkan definisi para ahli. Dalam menganalisa permasalahan pada penelitian ini, penulis menggunakan teori sekuritisasi karena berkaitan langsung dengan dampak yang akan ditimbulkan di bidang pertahanan nasional Indonesia dengan adanya fenomena siber global. Selain itu, penulis menggunakan konsep keamanan nasional untuk memperdalam analisa terhadap langkah strategi yang dilakukan oleh Indonesia dalam menghadapi gelombang perkembangan siber yang terjadi secara global sebagai studi kasus penelitian.

1.5.1 Konsep Strategi Keamanan

Strategi oleh John P. Lovell diartikan sebagai serangkaian langkah atau keputusan yang dirancang sebelumnya dalam situasi kompetitif. Pengertian tersebut dapat diperluas artinya bahwa strategi menjadi cara yang digunakan untuk mencapai suatu tujuan atau kepentingan dengan menggunakan *power* yang tersedia, termasuk juga kekuatan militer (Mas'oed, 1989: 90). Dalam konteks keamanan, strategi merupakan pola perencanaan yang digunakan oleh para pembuat keputusan untuk mencapai rasa aman, tentram, dan tertib dengan disertai usaha pencegahan atau penanggulangan terhadap suatu ancaman. Para pembuat keputusan menempatkan strategi sebagai alat untuk mendapatkan atau memaksimalkan apa yang diperoleh untuk negara atau bangsanya dengan menelaah berbagai alternatif tindakan yang dinilai berdasarkan analisis dari apa yang dikeluarkan dan hasil apa yang diperoleh (Mas'oed, 1989: 91).

Kajian strategi dan keamanan dalam studi Hubungan Internasional identik terhadap sesuatu yang berujung pada aspek militer. Dimana kata strategi sendiri adalah suatu hal atau bahkan sebuah usaha untuk mencapai tujuan dan pada awalnya strategi dikenal erat berhubungan dengan aspek militer karena sering digunakan untuk menghadapi sebuah peperangan. Berakhirnya *Cold War* dan munculnya era globalisasi, hubungan yang saling ketergantungan, dan semakin kompleksnya hubungan antar negara membawa studi kajian strategi untuk tidak hanya terpaku pada strategi berperang, namun memiliki subtansi perkembangan ilmu yang semakin meluas ke berbagai bidang, baik dalam bidang ekonomi maupun politik. Strategi mendorong terciptanya suatu perencanaan mengenai hal-hal yang harus dilakukan dalam rangka mengamankan lintasan menuju tujuan, sekaligus dalam implementasi perencanaan tersebut. Pada kelanjutannya studi strategi memberikan perhatian pada aktor yang dalam hal ini adalah berkaitan dengan keputusan-keputusan apa yang akan diambil untuk memecahkan sebuah permasalahan.

Era globalisasi membawa perkembangan teknologi yang begitu pesat. Salah satu perkembangan teknologi yang sangat berpengaruh besar pada kehidupan manusia adalah kemunculan internet yang mampu membentuk ruang

maya yang disebut dengan dunia siber. Dunia siber dengan segala fenomenanya tidak hanya memiliki sisi positif, namun juga memiliki sisi negatif yang secara langsung dirasakan oleh manusia sebagai makhluk sosial yang bermasyarakat dan bernegara. Maka secara otomatis dampak negatif kemunculan dunia siber yang berupa ancaman siber menjadi masalah baru bagi suatu negara, mengingat sistem pemerintahan suatu negara saat ini juga turut memanfaatkan keberadaan dunia siber. Hal tersebut mendorong suatu negara harus memiliki sebuah usaha untuk mencapai tujuan atau strategi untuk memelihara keamanan dari munculnya dunia siber. Keadaan ini yang membuat konsep strategi tidak lagi berkutat pada aspek militer, namun juga bisa diimplementasikan terhadap adanya dampak negatif dari perkembangan teknologi, dalam hal ini adalah internet.

Berkaitan dengan studi kasus pembahasan mengenai strategi yang diambil oleh Pemerintah Indonesia dalam menghadapi fenomena siber global, konsep strategi keamanan menjadi instrumen dasar penjelasan. Penyusunan strategi sebagai langkah penanggulangan kejahatan siber maupun pemanfaatan dunia siber yang bisa diperuntukkan untuk pertahanan nasional. Penyusunan strategi diperlukan guna kesiapan Indonesia menghadapi konstelasi siber global seperti *cyber crime*, *cyber terrorist*, maupun kejahatan pencurian data-data negara yang disimpan secara digital. Penggunaan dunia siber kenyataannya saat ini sangat luas dan universal. Dunia siber bisa digunakan dengan bijak, yaitu memanfaatkan keberadaan dunia siber sebagai media pengolahan, pengiriman, maupun penyimpanan data internal negara dengan sistem baru yang lebih cepat. Sedangkan di sisi lain dunia siber digunakan secara negatif dan tidak bertanggung jawab. Adanya sistem pengolahan data siber memicu para pelaku kejahatan membentuk sebuah model kejahatan baru yaitu kejahatan siber. Kasus kejahatan siber yang sudah terjadi yaitu pencurian, pemalsuan, serta pembajakan data. Hal itu terjadi dalam lingkup internasional. Konstelasi siber tersebut membuat negara-negara di dunia harus menyiapkan strategi untuk menghadapinya, baik mengamankan sekaligus menanggulangi kemungkinan-kemungkinan kejahatan siber yang akan terjadi dan dihadapi oleh negara maupun internasional. Oleh karena itu, konsep strategi keamanan mampu memberikan penjelasan dan menjadi

dasar analisa. Sebab penjelasan strategi yang sedang dilakukan Indonesia memiliki korelasi pada stabilitas keamanan Indonesia sendiri.

1.5.2 Konsep Keamanan Nasional

Keamanan Nasional dapat dimaknai baik sebagai kondisi maupun sebagai fungsi. Sebagai fungsi, Keamanan Nasional akan memproduksi dan menciptakan rasa aman dalam pengertian luas, yang di dalamnya tercakup rasa nyaman, damai, tenteram dan tertib. Kondisi keamanan semacam ini merupakan kebutuhan dasar umat manusia disamping kesejahteraan. Pemahaman terhadap makna dan substansi yang terkandung di dalamnya akan bervariasi tergantung kepada tata nilai, persepsi dan kepentingan (Darmono, 2010: 15). Strategi dan sistem keamanan sebuah negara sangat dipengaruhi oleh dinamika lingkungan yang terus berkembang dan terus berubah. Laju arus globalisasi, kemajuan teknologi dan arus informasi yang begitu cepat menjadi faktor-faktor yang secara langsung maupun tidak langsung memaksa banyak negara untuk kembali menata ulang strategi dan sistem keamanannya. Perubahan strategi dan kebijakan keamanan itu ditujukan untuk meraih keamanan nasionalnya.

Keamanan ditempatkan sebagai barang publik yang berhak dinikmati oleh setiap warga baik individu, kelompok, maupun sebagai bangsa dengan menempatkan kewajiban negara untuk mengatur dan mengelolanya. Dengan demikian, keamanan kini tidak hanya dimonopoli negara atau aktor-aktor keamanan tetapi masyarakat sipil juga memiliki ruang untuk mengkaji dan membahas berbagai isu tentang keamanan (A'raf, 2015: 28). Persoalan keamanan dengan menjelaskan mengenai sekilas perkembangan konsep keamanan dan kompleksitas ancaman yang berkembang dan juga memaparkan tentang tata kelola sektor keamanan di Indonesia pada masa kini.

Ada banyak terminologi dan interpretasi yang dihubungkan dengan konsep keamanan siber. Karena dunia siber merupakan ruang virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi. Teknologi yang dimaksud ialah teknologi informasi dan komunikasi (Sitompul, 2012: 15). Maka konsep keamanan siber tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadi ancaman terhadap keamanan nasional. Sebelumnya, permasalahan tentang

keamanan nasional sangat jarang dihubungkan dengan teknologi. Namun, seiring dengan meningkatnya ancaman serangan siber terhadap suatu negara yang bersifat domestik dan intenasional pada infrastruktur publik, pemerintahan, dan swasta, maka muncul kesadaran untuk mempopulerkan bahwa keamanan dunia siber bukanlah sekedar persoalan proteksi *password* yang sederhana. Keamanan siber lebih jauh membutuhkan serangkaian strategi karena menyangkut keamanan nasional. Perkembangan teknologi informasi juga telah memberikan perubahan signifikan mengenai konsep keamanan, kini ruang interaksi tidak bisa hanya dibatasi seara fisik tapi juga meluas ke dunia maya (siber). Konsekuensinya, negara harus beradaptasi dengan perkembangan ini dan konsep keamanan dunia siber (cyber *security*) sudah saatnya ditetapkan sebagai salah satu wilayah negara yang sistem penjagaan keamanannya ditangani sebagaimana kewajiban negara mengamankan teritorialnya. Apalagi, serangan siber tidak hanya terjadi pada institusi publik saja, namun juga menyerang institusi pemerintah.

Berkaitan dengan studi kasus pembahasan mengenai langkah dan strategi yang diambil oleh Indonesia dalam menghadapi fenomena siber global, konsep keamanan nasional menjadi konsep yang bisa menjadi acuan penjelasan. Sebab Indonesia memang sudah harus berperan lebih dengan menghadapi berbagai bentuk tindak kejahatan dunia siber yang bersifat nasional maupun internasional. Penyusunan strategi penanggulangan kejahatan siber maupun pemanfaatan dunia siber yang bisa diperuntukkan untuk pertahanan nasional. Pemerintah Indonesia memproduksi dan menciptakan rasa aman bagi negara, hal ini sangat jelas bahwa konsep keamanan nasional sebagai fungsi sedang dijalankan oleh Pemerintah Indonesia. Tata kelola di sektor keamanan dengan menyusun strategi penanggulangan kejahatan siber maupun pemanfaatan dunia siber yang bisa diperuntukkan untuk pertahanan nasional dapat dimaknai sebagai aktualisasi konsep keamananan yang telah dilakukan oleh Indonesia dalam menghadapi fenomena siber global.

1.6 Argumen Utama

Indonesia menyusun kebijakan strategis guna menciptakan sekaligus memelihara keamanan nasional dalam menghadapi gelombang fenomena siber global yang mencakup kejahatan di dunia siber. Penyusunan kebijakan strategi mengacu pada konsep strategi keamanan dan konsep keamanan nasional yang menjelaskan mengenai proses dan tujuan yang akan dicapai. Kebijakan strategi keamanan siber tersebut merupakan reaksi dan tindakan yang dilakukan oleh Pemerintah Indonesia untuk menciptakan rasa aman bagi masyarakat dan negara.

1.7 Metode Penelitian

Metodologi yaitu tentang prosedur bagaimana pengetahuan tentang fenomena itu diperoleh. Teknik dan metode penelitian yaitu tentang cara-cara penelitian apa yang diterapkan untuk memperoleh pengetahuan itu (Mas'oed, 1994: 3). Penelitian ini menggunakan metode penelitian kualitatif untuk menjelaskan strategi yang sedang dilakukan Indonesia untuk menghadapi konstelasi siber global yang berimplikasi pada bidang pertahanan nasional. Penelitian ini menggunakan data sekunder yang didapat dari berbagai referensi seperti buku, jurnal, surat kabar artikel artikel-artikel yang relevan.

1.7.1 Teknik Pengumpulan Data

Pada karya ilmiah ini, penulis menggunakan teknik penelitian studi pustaka (*Literature Research*). Data yang diperoleh berupa data sekunder atau dengan kata lain peneliti tidak terjun langsung ke lapangan untuk mendapatkan data sekaligus menelitinya. Pengumpulan data yang digunakan lebih difokuskan pada informasi yang berasal dari buku, jurnal dan surat kabar baik cetak maupun elektronik, dan data yang bersumber dari internet atau *website* yang terkait dengan topik yang dianalisisis. Selain itu, sebagai data pendukung penelitian data hasil penelitian yang dilakukan seorang pakar, akademisi maupun pihak terkait yang berhubungan dengan pembahasan karya ilmiah ini.

1.7.2 Teknik Analisis Data

Teknik analisis data yang digunakan oleh penulis menggunakan teknik analisis deskriptif kualitatif. Data Kualitatif bersifat menggambarkan, menjelaskan, dan memaparkan suatu fenomena secara riil dan apa adanya (Kartono, 1990: 7). Pada karya ilmiah ini data sekunder yang digunakan berasal dari ulasan berita media massa, pendapat dan hasil penelitian dari pengamat. Berdasarkan data-data yang diperoleh, penulis mendeskripsikan data dengan merelevansikannya pada studi kasus yaitu strategi Indonesia yang disusun dalam menghadapi konstelasi siber global. Kemudian dari analisa yang didapat akan ditarik sebuah kesimpulan tentang langkah-langkah yang diambil oleh Indonesia di bidang siber dalam menghadapi konstelasi siber global serta implikasinya terhadap pertahanan nasional Indonesia sendiri.

1.8 Sistematika Penulisan

Sistematika penulisan ini dibagi menjadi 5 bab. Sebagaimana uraian diatas:

Bab 1 Pendahuluan

Dalam bab ini penulis membahas tentang latar belakang, ruang lingkup pembahasan yang meliputi batasan materi dan batasan waktu, rumusan masalah, tujuan penelitian, manfaat penelitian, kerangka teori, hipotesis atau argumen utama, metode penelitian yang mencakup metode pengumpulan data dan metode analisis data, dan yang terakhir sistematika penulisan.

Bab 2 Konstelasi Siber Global

Bab ini berisi tentang penjelasan dan pembahasan mengenai konstelasi siber global. Penjelasan mengenai kemunculan dunia siber sebagai aspek kehidupan baru yang ada di masyarakat. Bab ini juga menjelaskan tentang gambaran besar penggunaan dunia siber. Pembahasan selanjutnya dalam bab ini yaitu mengenai kendala yang terjadi dalam penggunaan dunia siber sebagai sistem baru kehidupan dan harapan masyarakat internasional. Penyalahgunaan dunia siber sebagai alat untuk melakukan kejahatan

(*cyber crime, cyber terrorist*) dan keberadaan norma siber internasional juga menjadi pokok pembahasan dalam bab ini. Penjelasan mengenai hal-hal di atas dikategorikan melalui ruang lingkup kejadian pada umumnya.

Bab 3 Dinamika Siber di Indonesia

Bab ini berisi tentang penjelasan dan pembahasan mengenai dinamika siber di indonesia. Penjelasan mengenai kemunculan dunia siber sebagai aspek kehidupan baru yang ada di masyarakat Indonesia. Kemunculan dunia siber menimbulkan sistem baru yang ada di masyarakat dan negara. Bab ini juga menjelaskan tentang gambaran besar penggunaan dunia siber yang ada di Indonesia yang membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti-sosial dan perilaku kejahatan yang selama ini dianggap tidak mungkin terjadi namun ternyata telah terjadi. Penjelasan mengenai hal-hal di atas dikategorikan melalui ruang lingkup kejadian nasional (Indonesia).

Bab 4 Strategi Keamanan Siber di Indonesia

Bab ini berisi tentang penjelasan dan pembahasan mengenai langkah yang sudah dilakukan oleh Indonesia dengan menyusun strategi untuk menghadapi konstelasi siber global. Proses strategi yang sudah dilakukan oleh Pemerintah Indonesia untuk menyikapi dunia siber secara bijak. Tidak hanya menyebutkan strategi Indonesia saja, namun penulis juga akan mengkaji dengan lebih rinci dari setiap strategi yang sudah dan akan dilakukan Indonesia dalam menghadapi dan berperan aktif secara bijak pada konstelasi siber global yang akan terus terjadi dan berkembang.

Bab 5 Kesimpulan

Bab ini memuat kesimpulan yang diambil oleh penulis dari pembahasan pada bab-bab sebelumnya dan sekaligus merupakan penutup dari serangkaian dalam karya ilmiah ini.

BAB 2. KONSTELASI SIBER GLOBAL

2.1 Kemunculan Dunia Siber

Kemajuan di bidang teknologi, informasi, dan komunikasi yang begitu cepat menghasilkan internet sebagai fenomena dalam kehidupan umat manusia. Internet, yang didefinisikan oleh *The U.S. Supreme Court* sebagai *International Network of Interconnected Computers* (Gema, 2000), yang berarti jaringan internasional dari komputer-komputer yang saling berhubungan telah menghadirkan kemudahan-kemudahan bagi setiap orang. Internet telah mengahadirkan realitas kehidupan baru kepada umat manusia. Realitas kehidupan yang penuh dengan perubahan dengan adanya teknologi. Perubahan yang membuat keseluruhan sisi kehidupan menjadi lebih cepat daripada sebelumnya. Namun perubahan tersebut pasti memiliki dua sisi, bisa dimanfaatkan dengan benar ataupun dengan tanpa tanggung jawab.

Internet telah mengubah jarak dan waktu menjadi tidak terbatas. Manusia dapat melakukan transaksi bisnis, berbicara, belajar, bertukar pikiran dan melakukan berbagai aktivitas lain di dalam internet layaknya aktivitas dalam kehidupan nyata. Manusia seakan-akan mendapati suatu dunia baru yang dinamakan dengan dunia siber (Indrajit, 2011: 7). Internet telah membuat manusia-manusia sebagai penggunanya mampu menjelajah ruang maya ke mana saja, berkomunikasi dengan beragam informasi global, memasuki jagad perbedaan, dan lintas etnis, agama, politik, budaya, dan lain sebagainya. Manusia diajak bercengkerama, berdialog, dan mengasah ketajaman nalar dan psikologisnya dengan alam yang hanya tampak pada layar, namun sebenarnya mendeskripsikan realitas kehidupan manusia.

Pada saat ini penggunaan internet hampir merata bukan hanya di Indonesia melainkan hampir di semua belahan dunia sudah menggunakan internet. Dapat dikatakan bahwa internet adalah sebuah kebutuhan yang hampir sama dengan kebutuhan primer, ini dapat diartikan bahwa setiap orang pasti akan membutuhkan informasi yang dapat diakses dengan cepat serta mudah. Dengan

menggunakan internet manusia dapat memantau perkembangan dunia dengan mudah mulai dari perkembangan ekonomi hingga politik dunia.

Tentu saja internet memilki sisi positif dan negatifnya. Semua itu tergantung dari pengguna tersebut apakah akan memanfaatkan internet dengan baik atau tidak. Sebagai contoh dari penggunaan internet dalam segi positif dengan menggunakan dunia maya ini tentu saja menambah perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Namun dampak negatif pun tidak bisa dihindari. Internet telah menjadi bagian yang tidak dapat dipisahkan dari kehidupan manusia sebagai masyarakat. Keadaan yang demikian membuat diperlukannya berbagai macam upaya untuk meningkatkan kesadaran, pengetahuan, dan keterampilan agar tetap menggunakan internet dengan aman.

Dunia siber yang bersifat maya dan dengan memanfaatkan teknologi ini membuat manusia bisa melakukan apa saja yang biasa dilakukan di kehidupan sosial sehari-harinya dengan cara yang baru. Dunia siber sebenarnya merupakan sebuah dunia komunikasi yang berbasis teknologi virtual atau maya. Kemunculan dunia siber seperti itu menimbulkan sistem baru yang ada di masyarakat dan negara. Konstelasi siber global telah mampu memunculkan fenomena-fenomena baru di dunia Internasional. Dunia siber dimanfaatkan sebagai media baru untuk kepentingan suatu negara. Oleh karena itu, peluang kejahatan yang terjadi dan serangan terhadap hal tersebut akan terbuka lebar. Sistem strategi harus disusun dan segera dilakukan guna meminimalisir celah dan ancaman yang akan dimanfaatkan untuk kegiatan yang tidak bertanggung jawab seperti *cyber crime* maupun *cyber terorrism*.

2.2 Ancaman Dunia Siber

Kemajuan teknologi dan informasi yang ditandai dengan kemunculan internet, menimbulkan ancaman baru di ruang siber yakni kejahatan siber. Dunia siber sebagai sesuatu yang sangat berharga menjadikan sebuah fenomena ataupun dunia siber memiliki banyak ancaman. Tingkat dinamika yang begitu pesat dengan ditandai oleh jumlah pengguna internet di dunia yang setiap hari semakin bertambah membuat peluang ancaman semakin besar. Terus bertambahnya jumlah

pengguna internet diiringi dengan aktivitas di dunia siber yang semakin banyak, maka akan ada banyak hal yang dibuat, diperjual-belikan, dan disebarkan di dunia siber. Aktivitas-aktivitas yang demikian yang membuat dunia siber semakin memiliki nilai yang pastinya menjadi tempat untuk melancarkan aksi kriminal baru bagi para pelaku kejahatan. Seperti kejahatan peretasan situs, perampokan uang virtual, pencurian barang dan dokumen, penyebaran konten negatif, penyerangan negara dan banyak lagi kejahatan lainnya. Kejahatan yang dijalankan oleh individu, kelompok, maupun sebuah negara.

Keterbukaan yang tanpa kontrol dalam dunia siber dan ini akan menggiring pada keadaan anarkisme yang dapat membawa manusia pada situasi *chaos*. Ketika di dalam ruang dunia siber telah sama sekali hilang kontrol sosial (oleh institusi pemerintah, undang-undang, agama, atau masyarakat) maka yang terbentuk adalah semacam kematian sosial (Soluka, 2000: 11). Perubahan dalam konteks kemajuan terjadi karena ada penyesuaian pada pemanfaatan teknologi yang memang harus dikembangkan dalam bidang sosial, budaya, dan humanisme pada umumnya. Karena dasar dari perkembangan budaya itu sendiri adalah nilai-nilai yang berkembang di masyarakat secara tradinsional maupun bersumber dari ajaran agama. Teknologi yang tidak dikembangkan dalam konteks nilai-nilai dalam masyarakat cenderung menimbulkan gejolak budaya bahkan agama yang akan mengacaukan keseimbangan dalam masyarakat (Soluka, 2000: 23).

Ancaman siber yang lebih terstruktur dan pasti dilakukan oleh sekelompok orang ataupun organisasi adalah ketika para pelaku sengaja untuk membuat internet tidak berfungsi stabil dan normal. Keadaan tersebut membuat terjadinya kegagalan fungsi sebagai mana mestinya. Celah tersebut yang akan dimanfaatkan oleh pelaku untuk mencuri transaksi, mengambil alih akses informasi, mengganggu sekaligus merusak prosedur administrasi pemerintahan dan lain sebagainya. Aspek-aspek penting dalam kehidupan berbangsa dan bernegara menjadi yang paling penting dijaga keamanannya mengingat hal tersebut menjadi sasaran besar para pelaku kejahatan siber.

Secara rinci dan pengelompokan, menurut pendapat McDonnell dan Sayers, ancaman siber terdiri atas tiga jenis (Kementerian Pertahanan Republik Indonesia, 2014), yaitu:

a) Ancaman Perangkat Keras (*Hardware Threat*)

   Ancaman ini merupakan ancaman yang disebabkan oleh pemasangan perangkat tertentu yang berfungsi untuk melakukan kegiatan tertentu didalam suatu sistem, sehingga peralatan tersebut merupakan gangguan terhadap sistem jaringan dan perangkat keras lainnya.

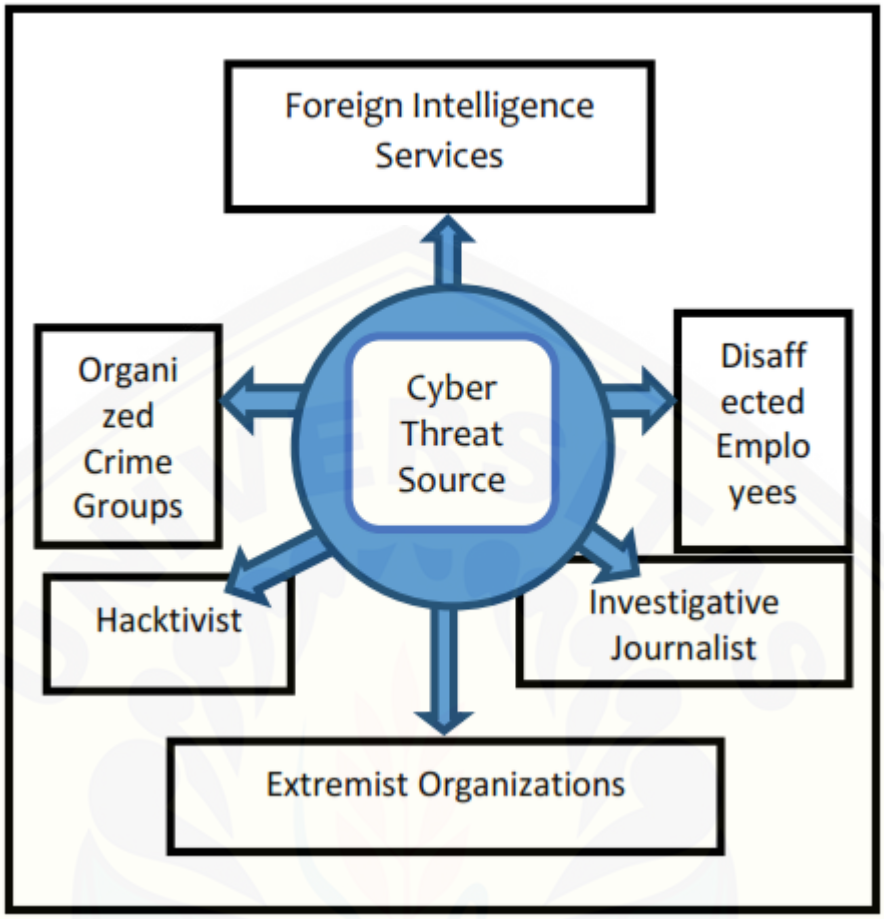
b) Ancaman Perangkat Lunak (*Software Threat*)

   Ancaman ini merupakan ancaman yang disebabkan masuknya perangkat lunak tertentu yang berfungsi untuk melakukan kegiatan pencurian, perusakan, dan manipulasi informasi.

c) Ancaman Data/Informasi (*Data/Information Threat*)

   Ancaman ini merupakan ancaman yang diakibatkan oleh penyebaran data/informasi tertentu yang bertujuan untuk kepentingan tertentu.

Kajian Strategis Keamanan Siber Nasional, mendefinisikan ancaman siber sebagai setiap kondisi dan situasi serta kemampuan yang dinilai dapat melakukan tindakan atau gangguan atau serangan yang mampu merusak atau segala sesuatu yang merugikan sehingga mengancam kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersedian (*availability*) sistem dan informasi (Rahmawati, 2017). Ancaman siber dapat terjadi karena adanya kepentingan dari berbagai individu atau kelompok tertentu dalam aspek kehidupan masyarakat dapat menimbulkan berbagai ancaman fisik, baik nyata ataupun yang tidak nyata dengan menggunakan kode-kode komputer (*software*) untuk melakukan pencurian informasi, kerusakan sistem, manipulasi informasi atau perangkat keras (*hardware*) untuk melakukan gangguan terhadap sistem ataupun penyebaran data dan informasi tertentu untuk melakukan kegiatan propaganda.



Gambar 2.1 Sumber-sumber Ancaman Siber

Sumber: International Telecommunication Unit (ITU). 2012. National Cybersecurity Strategy Guide, 12 November 2012

Sumber-sumber ancaman siber dapat berasal dari berbagai sumber, seperti intelejen negara, kekecewaan para pegawai, investigasi jurnalis, organisasi ekstremis, aktivitas para peretas (*hacker*), dan kelompok kejahatan terorganisir. Klasifikasi sumber-sumber ancaman siber pada gambar tersebut menjelaskan bahwa hal-hal negatif yang terjadi di dunia siber sangat kompleks. Tidak hanya berdasar pada kepentingan politik, ekonomi, sosial, dan budaya yang digerakkan oleh segelintir orang maupun kelompok, namun ada juga yang berasal dari sisi manusiawi seperti kekecewaan para pegawai yang disebutkan di atas. Dengan demikian, sumber-sumber ancaman siber sudah seperti arus yang bila ingin dihentikan hanya bisa dengan suatu sistem yang terstruktur dan bersifat massal.

2.3. *Cyber Crime*

Cyber crime adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital (Wahid dan Labib, 2005: 40). Definisi ini sangat jelas menerangkan bahwa instrumen utama dalm melakukan kejahatan siber adalah teknologi, dalam hal ini adalah internet. Pengertian tersebut sejalan dengan pengertian versi lain dari para ahli yang menyebutkan bahwa hanya dengan internet dan melalui komputer, segala bentuk kejahatan akan terjadi secara kompleks dan melemahkan seluruh sistem dalam kehidupan bermasyarakat. Seperti yang dikatakan oleh Peter Stephenson:

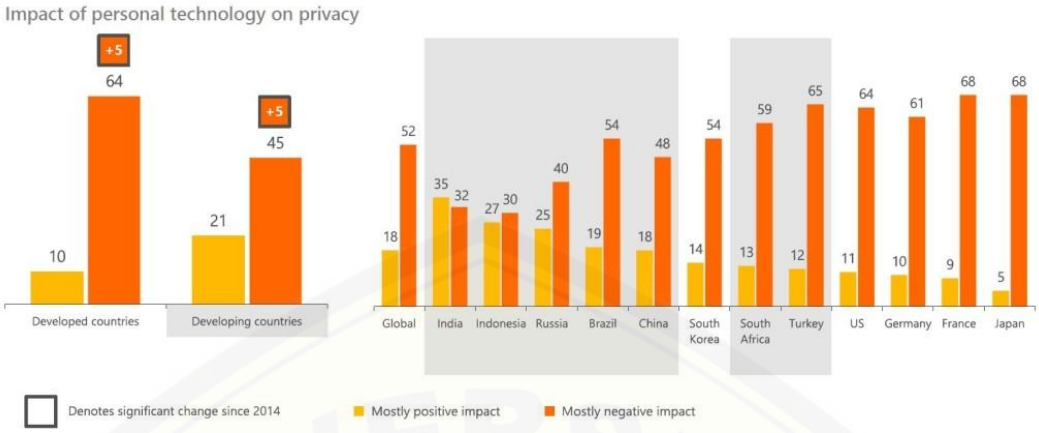
> *"The easy definition of cyber crime is crimes directed at a computer or a computer system. The nature of cyber crime, however, is far more complex. As we will see later, cyber crime can take the form of simple snooping into a computer system for which we have no authorization. It can be the feeing of a computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system."* (Stephenson, 2000: 56)

Sementara dua dokumen Kongres PBB yang dikutip oleh Barda Nawawi Arief, mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian kejahatan siber, yaitu *cyber crime* dan *computer related crime* (Arief, 2007: 24). Dalam *back ground paper* untuk lokakarya Kongres PBB X/2000 di Wina Austria, istilah *cyber crime* dibagi dalam dua kategori. Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) disebut *computer crime*. Kedua, *cyber crime* dalam arti luas (*in a broader sense*) disebut *computer related crime* (Arief, 2007). Lengkapnya sebagai berikut:

1. *Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed byh them.*
2. *Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network.*

Perkembangan dan kemajuan teknologi, informasi, dan komunikasi menjadikan dunia siber semakin kompleks juga jenis serangan ataupun gangguan yang terjadi di dalamnya. Istilah *hacker* dan *cracker* yang merujuk pada suatu individu dengan kemampuan dan aktivitasnya mampu memasuki tanpa izin komputer & jaringan lain, bahkan sampai merusaknya. Tujuannya pun beraneka ragam, seperti pemberontakan, pencurian, pembajakan, hingga merusak sistem pertahanan politik suatu negara. Tidak hanya individu sebagai pelaku, namun juga ada mesin maupun sistem yang dirancang sebagai sesuatu yang fungsi kerjanya sama dengan *hacker* dan *cracker*. Lebih parah lagi, mesin dan alat yang dimaksud bahkan mampu menjalankan fungsi penyusupan dengan teknik-teknik intelijen buatan (Indrajit, 2011). Pada intinya, serangan yang berbasis teknologi, informasi, dan komunikasi di dunia siber telah masuk pada kategori kriminal. Entah dilakukan secara individu, kelompok, maupun organisasi, dan bersifat pidana atau perdata.

Kemajuan teknologi informasi ternyata memiliki konsekuensi yang tidak bisa disepelekan begitu saja. Kenyamanan serta kecanggihan itu semua ternyata menjadi faktor utama keamanan siber yang sedikit dipedulikan oleh para pengguna internet. Penjelajah dunia siber dapat dengan mudah melakukan transaksi keuangan, bertukar informasi, penyimpanan dan pengiriman data, serta banyak aktivitas lainnya hanya dengan melalui internet. Hal tersebut merupakan sebuah kenyamanan yang tentu mampu melindungi aspek privasi masing-masing orang. Setiap orang di dunia siber dapat memiliki ruang privasi masing-masing sesuai yang diinginkan. Namun demikian mereka melakukan itu tanpa menyadari risiko yang akan terjadi. Grafik di bawah ini menggambarkan bagaimana dampak dari kemajuan teknologi yang dilihat dari aspek privasi.



Gambar 2.2 Dampak Teknologi Sebagai Privasi

Sumber: Charlie Cottrell. 2017. Personal Technology on Privacy. We Are Social UK. 28 Juli 2017

Grafik 2.2 tersebut menunjukkan bahwa dampak negatif yang terjadi di dunia, yaitu kejahatan dalam penggunaan teknologi ternyata lebih tinggi dari dampak positif. Data penggunaan teknologi yang disajikan dalam grafik berdasar pada negara dengan jumlah penduduk paling banyak dalam menggunakan internet. Data tersebut menunjukkan penggunaan teknologi secara pribadi, bukan untuk perusahaan atau instansi pemerintahan. Data itu juga menunjukkan bahwa tingkat jumlah populasi dari suatu negara yang besar, maka pengguna internetnya pun juga akan semakin banyak. Maka semakin banyak pengguna internet akan memunculkan dampak penggunaannya, baik positif maupun negatif.

Seiring dengan kemajuan teknologi informasi, ternyata teknologi juga memiliki dampak yang negatif. Salah satunya adalah perkembangan kejahatan siber yang semakin hari semakin meningkat. Hal ini ditandai dengan seringnya terjadi serangan terhadap sistem dan server di dunia. Kasus kejahatan seperti ini semakin hari semakin meningkat. Kasus kejahatan di dunia siber berbeda dengan kasus kejahatan di dunia nyata. Kejahatan yang dilakukan merupakan kejahatan maya/tidak bisa dilihat, dipegang, sehingga perlakuan investigasi terhadap kejahatanpun membutuhkan orang-orang khusus yang memiliki pengetahuan lebih mengenai keamanan siber (*cyber security*).

Go-Gulf, sebuah perusahaan teknologi web berbasis di Dubai, mengeluarkan pernyataan mengenai statistik kejahatan yang terjadi dalam rentang waktu satu tahun. Dalam data yang diberi nama *Yearly Cyber Crime Victim Count Estimate*; tercatat sebanyak 556 juta korban per tahun, lebih dari 1.5 juta korban per hari, 18 korban per detik, dan keseluruhan korban dengan identitas yang tidak terungkap (Go-Gulf, 2018). Statistik ini menunjukkan betapa berkembangnya kejahatan yang terjadi di dunia siber. Hal tersebut mengindikasikan bahwa pengguna internet masih belum memahami apa itu kejahatan siber serta dampak yang ditimbulkan.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi internet ini dikelompokkan dalam beberapa bentuk sesuai modus operasi yang ada (Suara Merdeka, 2002), yaitu:

a. *Unauthorized Access to Computer System and Service*

   Kejahatan yang dilakukan dengan memasuki/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 (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi Internet dan juga intranet.

b. *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, 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.

c. *Data Forgery*

Merupakan kejahatan dengan memalsukan data pada dokumendokumen penting yang tersimpan sebagai *scripless 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 karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan.

d. *Cyber Espionage*

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

e. *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.

f. *Offense against Intellectual Property*

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh, 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.

g. *Infringements of Privacy*

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.

Pelaku *cyber crime* adalah mereka yang memiliki keahlian tinggi dalam ilmu komputer. Pelaku *cyber crime* umumnya menguasai algoritma dan pemrograman computer unutk membuat *script* atau *malware code* (Basariyadi 2017). Mereka dapat menganalisa cara kerja system komputer dan jaringan, dan mampu menemukan celah pada sistem dan kemudian akan menggunakan kelemahan tersebut untuk dapat masuk sehingga tindakan kejahatan seperti pencurian data dapat berhasil dilakukan.

Seluruh jenis dan bentuk kejahatan siber tersebut menyentuh semua aspek kehidupan manusia dalam bermasyarakat. Secara otomatis pasti akan bersinggungan langsung dengan kehidupan bernegara. Akibat keberadaannya, maka akan selalu terjadi banyak perubahan secara dinamis di bidang politik, ekonomi, sosial, dan budaya. Masyarakat dan pemerintah menjadi satu kesatuan yang dijadikan sebagai sasaran utama dalam aksi kejahatan siber atau *cyber crime*.

2.4 *Cyber Terorrism*

Pendefinisian *cyber terorrism* hingga saat ini masih tidak ada yang baku. Sama halnya dengan terorisme sendiri, pendefinisian yang dijadikan sebagai acuan arti secara bahasa masih tidak ada. Acuan yang digunakan untuk menggambarkan suatu tindak kejahatan terorisme hingga saat ini hanya berdasarkan pada skala kejahatan yang dilakukan dan tujuan dari kejahatan itu sendiri. Hal tersebut hanya melahirkan makna secara terminologi dari tindakan terorisme dan *cyber terorrism* itu sendiri. Dorothy E. Denning, dalam sebuah pernyataan mendefinisikan *cyber terorrism* sebagai:

> *"unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."* (Denning, 2000)

Istilah *cyber terrorism* telah diperkenalkan sejak tahun 1997 oleh Barry Collin, seorang peneliti senior pada Institute *for Security and Intellegence* di California, Amerika Serikat. Dalam pandangan Collin, komputerisasi dalam berbagai bidang kehidupan manusia menciptakan kerentanan baru. Kerentanan itu dapat dieksploitasi untuk aksi terorisme baik melalui perusakan (*destruction*), pengubahan (*alteration*), dan akusisi dan retransmisi (*acquisition* dan *retransmission*), yang tujuannya untuk menimbulkan kekacauan dan teror (Denning, 2009: 7).

Pelaku *cyber terorrism* disebut dengan *cyber terorrist* atau teroris siber. Secara etimologi, kosakata mengenai teroris siber adalah penjahat yang menggunakan teknologi komputer dan Internet, terutama untuk menyebabkan ketakutan dan gangguan. Beberapa teroris siber menyebar virus komputer, dan lain-lain mengancam orang secara elektronik. Beberapa peneliti berpendapat bahwa kegiatan terorisme yang demikian dianggap sebagai *cyber terorrism* (Yunus dan Ahmad, 2012: 149).

Terdapat beberapa pengertian mengenai *cyber terrorism* dari berbagai sumber (Samad, 2014: 30), yaitu:

1. *Cyber terrorism* adalah tindakan kriminal yang dilakukan melalui komputer dan berkibat kejahatan, kematian dan/atau kehancuran, dan menimbulkan teror untuk tujuan memaksa pemerintah untuk mengubah kebijakan.
2. *Cyber terrorism* adalah penggunaan jaringan komputer sebagai alat untuk mematikan infrastruktur nasional yang penting (seperti energi, transportasi, kegiatan pemerintah) atau untuk memaksa atau mengintimidasi pemerintah atau populasi sipil.
3. *Cyber terrorism* seperti tindakan terorisme yang lainnya, merupakan tindakan kejahatan yang dilakukan dengan perencanaan yang hati-hati dengan sedikit upaya, biasanya sulit untuk diindentifikasi atau ditangkap, yang dipergunakan untuk mencampuri berfungsinya mayarakat sipil.

Beberapa pengertian di atas bisa dijadikan sebagai acuan untuk menyimpulkan bahwa *cyber terorrism* adalah tindakan melawan hukum yang dilakukan oleh individu, sekelompok orang, atau organisasi yang menggunakan sistem jaringan komputer dan internet, artinya yaitu dunia siber sebagai media dan juga sasaran aksi kejahatan yang menyebabkan kekerasan atau mengintimidasi pemerintah atau masyarakat secara umum untuk tujuan politik, sosial, ekonomi atau kerusakan pada infrastruktur suatu negara.

Cyber terorrism memiliki makna berbeda dengan *cyber crime*. Walaupun pada dasarnya kedua jenis aktivitas tersebut memiliki kesamaan pada usaha untuk mengacaukan sistem keteraturan yang ada di dunia siber. Hal yang membedakan antara *cyber terorrism* dan *cyber crime* adalah pada jenis kejahatan yang dilakukan. *Cyber crime* merupakan kejahatan di dunia siber yang dilakukan untuk lingkup kepentingan pribadi seseorang atau golongan. Berbeda dengan *cyber crime*, *cyber terorrism* adalah aktivitas kejahatan di dunia siber yang lebih terorganisir dan dalam bentuk yang lebih ekstrim. Karena para pelaku *cyber terorrism* merupakan organisasi bentukan yang terlatih dan tidak hanya profesional, namun juga mereka melakukan aksi-aksi kejahatan untuk kepentingan ataupun tujuan politis. Aktivitas kejahatan di dunia siber yang dilakukan oleh para pelaku *cyber terorrism* bertujuan untuk melakukan serangan yang membuat sistem suatu negara mengalami ketidak-stabilan atau kelumpuhan, sehingga ada celah yang digunakan untuk menyerang sistem politik suatu negara.

Cyber terorrism sebenarnya memiliki konsep yang tidak jauh berbeda dengan tindakan terorisme di dunia yang sebenarnya. Hanya saja pada hal ini para pelaku kejahatan maupun teror memasukkan unsur keberadaan dunia siber. Melalui artikel *a Dynamic Cyber-terrorism Framework* yang ditulis oleh Zahri Yunus dan Rabiah Ahmad, konsep kerangka *cyber terrorism* mencakup beberapa hal (Yunus dan Ahmad, 2012: 167) sebagai berikut:

a. Target

   Dalam melakukan tindakan *cyber terrorism* menggabungkan target tertentu dengan khalayak yang lebih luas. Dengan ini, sistim komputer dan masyarakat sipil merupakan target yang menarik bagi *cyber terrorist*.

Misalnya, dengan menyerang seluruh jaringan *Critical National Information Infrastructure* (CNII) atau menyerang layanan sistim komputer yang menggunakan *Supervisory Control dan Data Acquisition* (SCADA) yang telah terhubung dengan internet dan dikendalikan secara jarak jauh. Selain berfokus pada infrastruktur yang berbasis Teknik Informasi dan Komunikasi, *cyber terrorism* juga menargetkan masyarakat sipil. Serangan terhadap infrastruktur yang penting dari suatu negara dapat menyebarkan ketakutan dan membahayakan masyarakat yang tidak bersalah dapat dikategorikan sebagai *cyber terrorism*.

b. Motif

Motif dari *cyber terrorism* bersifat sosial, politik dan keyakinan terhadap suatu paham atau ideologi. Dengan motif ini *cyber terrorist* dapat menyerang jaringan informasi suatu negara demi kepentingan mereka.

c. Metode Penyerangan

Metode penyerangan *cyber terrorism* menggunakan operasi jaringan komputer.

- Komputer dan jaringan internet sebagai senjata atau alatuntuk melakukan serangan siber.
- Menjadi penyedia layanan informasi baik media elektronik maupun cetak. Dengan menjadi penyedia informasi, para *cyber terrorist* mampu untuk mengontrol tingkah laku atau respon dari orang-orang yang menerima informasi tersebut.
- Menyebarkan propaganda lewat media informasi. Seiring berkembangnya zaman kondisi penyebaran informasi menjadi semakin cepat, sehingga hal ini dimanfaatkan oleh *cyber terrorist* untuk melakukan propaganda tentang kegiatan teroris mereka.

d. Domain

Cyber terrorism adalah konvergensi dari dunia siber dan terorisme. Dunia siber, baik diakses melalui sistem komputer atau perangkat lain, adalah media bagi *cyber terrorists* melakukan serangan siber.

e. Tindakan Pelaku

Cyber terrorist melakukan tindakan melawan hukum dengan terencana untuk mengintimidasi atau memaksa pemerintah atau orang-orang dengan tujuan politik, sosial atau tujuan ideologi yang dipaham oleh mereka.

f. Dampak atau Akibat

Cyber terroism dilakukan untuk menyebabkan kerusakan serius pada infrastruktur suatu negara maupun keamanan dalam skala internasional. Ketika *cyber terrorism* berhasil dilakukan terhadap infrastuktur suatu negara atau pada jaringan komputer, hal ini akan berdampak pada stabilitas suatu negara dan membahayakan masyarakat, selain itu akan berdampak terhadap keamanan internasional.

Karakteristik *cyber terorrism* yaitu memiliki sistem dalam segala aktivitasnya dan semua hal dilakukan secara terstruktur organisasi. Tindakan teror yang dilakukan dalam koridor dunia siber tersebut melakukan penyerangan terhadap suatu sistem. Baik itu jaringan komputer, internet, dan basis informasi dalam skala pribadi hingga data penting kenegaraan. Tindak kejahatan terorisme di dunia siber sangat erat kaitannya dengan bidang politik kenegaraan. Sasaran terbesarnya adalah pengacauan pada sistem politik yang telah disusun oleh pemerintahan suatu negara. Para teroris siber bisa dikategorikan sebagai pemberontak yang menentang suatu sistem atau rezim yang berlaku di suatu negara. Oleh karena itu, kepentingan atau motif utama yang dilakukan dalam tindak kejahatan *cyber terorrism* merupakan kepentingan suatu kelompok atau organisasi tertentu yang tidak menghendaki adanya suatu sistem negara yang sedang berlangsung.

2.5 Hukum Siber

Dunia siber menyediakan ruang atau tempat yang digunakan untuk melakukan berbagai macam interaksi antar manusia. Berbagai macam aktivitas terjadi di dunia siber selama jaringan internet terus ada dan berkembang. Walaupun dunia siber merupakan ruang maya yang tidak bisa dijangkau dengan fisik manusia secara langsung, namun keberadaannya mampu membuat manusia sebagai *user* menjalankan sebagian aktivitas kehidupan di dalamnya. Sebuah

konsep norma ataupun hukum dapat ditempatkan di dunia siber agar tercipta keteraturan dan pencegahan terhadap tindak kejahatan yang tidak diinginkan.

Cara pandang mengenai perlunya sebuah konsep norma atau hukum di dunia siber berpijak pada pemikiran Lawrence Lessig yang mengatakan bahwa hukum siber adalah seperangkat aturan/*code* melalui algoritma program komputer yang ditujukan untuk mengatur bagaimana manusia berinteraksi dengan komputer dan dengan sesama pengguna komputer (Lessig, 2006: 83). Keberadaan norma atau hukum siber adalah gagasan yang diadakan untuk mengiringi laju perkembangan teknologi internet. Laju perkembangan yang semakin waktu semakin cepat rentan terhadap adanya ketidak-teraturan di dalamnya bila tidak diiringi dengan keberadaan norma atau hukum siber yang berlaku. Ada 2 pendekatan untuk memahami dan mengatur dunia siber (Dalimi, 2017: 1), yaitu:

1. Hukum adalah teknologi

   Dalam pendekatan ini, ketika ada teknologi yang baru, maka akan dibuatkan/terbitkan hukum yang baru untuk mengatur teknologi baru tersebut.

2. Teknologi adalah hukum

   Dalam pendekatan ini, teknologi itu sendiri dianggap sudah menjadi hukum, yang artinya setiap ada teknologi yang baru, tidak perlu diciptakan hukum yang baru, melainkan cukup menggunakan hukum/aturan yang sudah ada.

Perlu dibedakan bahwa konsep norma atau hukum siber adalah hukum yang berlaku ketika sebuah kejahatan siber, yang pastinya terkait dengan pemanfaatan teknologi informasi dalam hal ini adalah jaringan internet. Bukan semata-mata didefinisikan sebagai hukum pidana yang berlaku untuk kejahatan yang hanya menggunakan alat, sebab alat tersebut yang dimaksud masih belum tentu alat dalam kategori jaringan teknologi, informasi, dan komunikasi. Artinya, di sini ada klasifikasi baru dalam definisi alat pada hukum pidana, karena tidak semua alat dapat terhubung ke dalam jaringan Internet. Perlu adanya pemahaman konsep pendefinisian mengenai norma ataupun hukum siber yang berlaku.

Penegasan konsep dalam mendefinisikan norma atau hukum siber dikembangkan secara rinci agar tidak menjadi rancu terhadap definisi hukum kejahatan yang menggunakan alat. Oleh karena itu, muncul istilah lain yang juga digunakan adalah hukum Teknologi Informasi (*Law of Information Techonology*) Hukum Dunia Maya (*Virtual World Law*) dan Hukum Mayantara. Istilah-istilah tersebut lahir mengingat adanya kegiatan internet dan pemanfaatan teknologi informasi berbasis virtual semakin kompleks (Ramli, 2006: 12).

Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global dengan memanfaatkan teknologi informasi berbasis sistem komputer yang yang merupakan sistem elektronik yang dapat dilihat secara virtual. Belum adanya peraturan perundang-undangan tersebut disebabkan oleh fakta bahwa pengaturan dunia siber memerlukan kajian-kajian yang cermat dan mendalam agar dapat benar-benar tepat sasaran sesuai dengan tingkat perkembangan perilaku kehidupan masyarakat agar implementasinya tidak menimbulkan keadaan yang pasif. Para penegak hukum akan menghadapi kesulitan jika harus membuktikan suatu persoalan yang diasumsikan sebagai sesuatu yang maya atau yang tidak terlihat dan semu.

Hukum siber merupakan konsep dan bidang baru di ranah hukum. Hukum siber diciptakan dari buah inovasi teknologi yang makin berkembang pesat. Keberadaannya mengiringi kemajuan teknologi, informasi, dan komunikasi sebagai pelindung bagi para *user* yang ada di dunia siber. Secara konseptual, berbagai isu-isu hukum baru di dunia siber akan dikembalikan kepada prinsip hukum sektoralnya. Misalnya terkait isu kekayaan intelektual, persaingan usaha, perlindungan konsumen, pidana siber dan sebagainya. Artinya, hukum siber adalah tempat untuk menentukan posisi suatu peristiwa hukum yang penyelesaiannya memerlukan bantuan bidang hukum sektoral terkait. Meskipun demikian, tidak dapat dipungkiri daya rusak dan efek kelanjutannya dari suatu peristiwa hukum di dunia siber lebih tinggi dibandingkan dengan di dunia nyata. Agar hukum siber bekerja secara optimal, maka kekuatan hukum sektoral menjadi

penting agar dapat bekerja membantu menjawab masalah hukum di ruang siber (Pratama, 2017: 7).

Secara luas hukum siber bukan hanya meliputi tindak kejahatan yang ada di internet, namun juga aturan yang melindungi para pelaku aspek hak cipta, aspek merek dagang, aspek fitnah dan pencemaran nama baik, aspek privasi (Ramli, 2006: 34).

a. Aspek Hak Cipta

   Hak cipta yang sudah diatur dalam Undang-undang Hak Cipta. Aplikasi internet seperti *website* dan *e-mail* membutuhkan perlindungan hak cipta. Publik beranggapan bahwa informasi yang tersedia di internet bebas untuk diunduh, diubah, dan diperbanyak. Ketidak-jelasan mengenai prosedur dan pengurusan hak cipta aplikasi internet masih banyak terjadi.

b. Aspek Merek Dagang

   Aspek merek dagang ini meliputi identifikasi dan membedakan suatu sumber barang dan jasa, yang diatur dalam Undang-undang Merek.

c. Aspek Fitnah dan Pencemaran Nama Baik

   Hal ini meliputi gangguan atau pelanggaran terhadap reputasi seseorang, berupa pertanyaan yang salah, fitnah, pencemaran nama baik, mengejek, dan penghinaan. Walau semua tindakan tadi dilakukan dengan menggunakan aplikasi internet, namun tetap tidak menghilangkan tanggung jawab hukum bagi pelakunya. Jangan karena melakukan fitnah atau sekedar mengoolok-olok seseorang di *e-mail* atau *chat room* maka kita bebas melenggang tanpa rasa bersalah. Ada korban dari perbuatan kita yang tidak segan-segan menggambil tindakan hukum.

d. Aspek Privasi

   Banyak negara maju yang menjadikan komputer dan internet sudah bisa diaskes oleh mayoritas warganya, maka bila seperti itu privasi menjadi masalah tersendiri. Semakin seseorang menggantungkan pekerjaannya kepada komputer, semakin tinggi pula privasi yang dibutuhkannya. Ada beberapa persoalan yang bisa muncul dari hal privasi ini. Baik itu dari informasi personal dan juga informasi pekerjaan orang yang

menggantungkan pekerjaanya dengan menggunakan komputer dan jaringan internet.

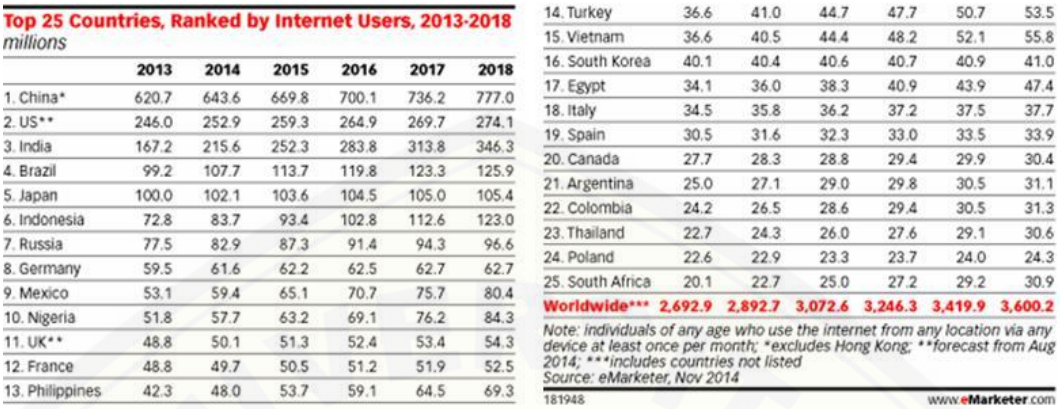
BAB 3. DINAMIKA SIBER DI INDONESIA

3.1 *Trend* Siber di Indonesia

Kemajuan teknologi adalah sesuatu yang tidak bisa dihindari dalam kehidupan ini, karena kemajuan teknologi akan berjalan sesuai dengan kemajuan ilmu pengetahuan. Setiap inovasi diciptakan untuk memberikan manfaat positif bagi kehidupan manusia. Teknologi juga memberikan banyak kemudahan, serta sebagai cara baru dalam melakukan aktivitas manusia. Manusia juga sudah menikmati banyak manfaat yang dibawa oleh inovasi-inovasi teknologi yang telah dihasilkan. Indonesia adalah salah satu negara yang mengalami perkembangan pesat di bidang teknologi informasi dan komunikasi. Banyak jenis dan model teknologi baru yang diterima oleh masyarakat Indonesia, terutama dalam hal ini adalah internet. Tidak hanya menerima, masyarakat Indonesia juga turut menggunakan hingga mengembangkan berbagai macam kegunaan ataupun fungsi dari internet itu sendiri. Berbagai macamnya aktivitas masyarakat Indonesia pengguna internet itu membuat Indonesia menjadi salah satu dari negara di dunia yang terus mengalami peningkatan besar dalam hal jumlah pengguna internet.

Jumlah pengguna internet di Indonesia begitu banyak dan pertumbuhannya sangat pesat setiap tahunnya. Faktor utama yang menyebabkan hal tersebut terjadi adalah jumlah penduduk Indonesia yang terhitung banyak, sekaligus adanya infrastruktur dan kemudahan untuk mengakses Internet di Indonesia. Data jumlah pengguna internet di Indonesia telah disampaikan oleh Kementerian Komunikasi dan Informatika Republik Indonesia (KOMINFO) pada tahun 2014. Melalui lembaga riset pasar *e-Marketer*, KOMINFO menyatakan populasi pengguna internet di Indonesia mencapai 83,7 juta orang pada tahun 2014. Angka tersebut menjadikan Indonesia sebagai negara peringkat ke-6 terbesar di dunia dalam hal jumlah pengguna internet (Kementerian Komunikasi dan Informatika Republik Indonesia, 2014).

Tabel 3.1 Daftar 25 Negara dengan Jumlah Pengguna Internet Terbanyak



Top 25 Countries, Ranked by Internet Users, 2013-2018
millions

	2013	2014	2015	2016	2017	2018
1. China*	620.7	643.6	669.8	700.1	736.2	777.0
2. US**	246.0	252.9	259.3	264.9	269.7	274.1
3. India	167.2	215.6	252.3	283.8	313.8	346.3
4. Brazil	99.2	107.7	113.7	119.8	123.3	125.9
5. Japan	100.0	102.1	103.6	104.5	105.0	105.4
6. Indonesia	72.8	83.7	93.4	102.8	112.6	123.0
7. Russia	77.5	82.9	87.3	91.4	94.3	96.6
8. Germany	59.5	61.6	62.2	62.5	62.7	62.7
9. Mexico	53.1	59.4	65.1	70.7	75.7	80.4
10. Nigeria	51.8	57.7	63.2	69.1	76.2	84.3
11. UK**	48.8	50.1	51.3	52.4	53.4	54.3
12. France	48.8	49.7	50.5	51.2	51.9	52.5
13. Philippines	42.3	48.0	53.7	59.1	64.5	69.3
14. Turkey	36.6	41.0	44.7	47.7	50.7	53.5
15. Vietnam	36.6	40.5	44.4	48.2	52.1	55.8
16. South Korea	40.1	40.4	40.6	40.7	40.9	41.0
17. Egypt	34.1	36.0	38.3	40.9	43.9	47.4
18. Italy	34.5	35.8	36.2	37.2	37.5	37.7
19. Spain	30.5	31.6	32.3	33.0	33.5	33.9
20. Canada	27.7	28.3	28.8	29.4	29.9	30.4
21. Argentina	25.0	27.1	29.0	29.8	30.5	31.1
22. Colombia	24.2	26.5	28.6	29.4	30.5	31.3
23. Thailand	22.7	24.3	26.0	27.6	29.1	30.6
24. Poland	22.6	22.9	23.3	23.7	24.0	24.3
25. South Africa	20.1	22.7	25.0	27.2	29.2	30.9
Worldwide* **	**2,692.9**	**2,892.7**	**3,072.6**	**3,246.3**	**3,419.9**	**3,600.2**

*Note: individuals of any age who use the internet from any location via any device at least once per month; *excludes Hong Kong; **forecast from Aug 2014; ***includes countries not listed*
Source: eMarketer, Nov 2014

181948 www.eMarketer.com

Sumber: KOMINFO. 2014. Negara dengan Jumlah Pengguna Internet Terbanyak. kominfo.go.id. 12 September 2014.

Tabel 3.1 menunjukkan negara-negara yang jumlah pengguna internetnya terhitung banyak. Dalam gambar tersebut juga ditunjukkan pertumbuhan jumlah pengguna dari tahun 2013 hingga tahun 2018. Dari data ini pula, KOMINFO juga menyatakan bahwa pada tahun 2017 diperkirakan pengguna internet di Indonesia akan mencapai 112 juta orang, mengalahkan Jepang di peringkat kelima yang pertumbuhan jumlah pengguna internetnya lebih lamban. Kenyataannya sangat benar, jumlah pengguna internet di Indonesia pada tahun 2017 melebihi angka prediksi yang dikeluarkan oleh KOMINFO.

Melalui Siaran Pers No. 53/HM/KOMINFO/02/2018 yang dikeluarkan pada tanggal 19 Februari 2018 tentang peningkatan jumlah pengguna internet 2017, KOMINFO menyatakan jumlah pengguna internet tahun 2017 telah mencapai 143,26 juta jiwa atau setara dengan 54,68 persen dari total jumlah penduduk Indonesia. Jumlah tersebut menunjukan kenaikan sebesar 10,56 juta jiwa dari hasil survei pada tahun 2016 (Kementerian Komunikasi dan Informatika Republik Indonesia, 2018). Pertumbuhan ataupun kenaikan besar pengguna internet menunjukkan bahwa masyarakat Indonesia sangat antusias dengan teknologi internet. Terhubungnya masyarakat Indonesia melalui internet sebagai

sarana bersosialisasi, berbisnis, dan berbagai macam lainnya ini menjadikan internet sebagai sebuah *trend* tersendiri bagi masyarakat Indonesia.

Gambar 3.2 Penetrasi Pengguna Internet di Indonesia

Sumber: Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). 2017. Indonesia Alami Lonjakan Pengguna Internet. Apjii.id. 22 Maret 2017.

Lebih dari separuh penduduk Indonesia merupakan masyarakat pengguna internet aktif. Gambar 3.2 menunjukkan bahwa dari populasi 262 juta jiwa penduduk Indonesia, 143,26 juta jiwa menggunakan internet secara aktif dan sehari-hari. Jumlah tersebut adalah hasil lonjakan yang cukup signifikan dibandingkan dengan tahun sebelumnya yang tercatat sebanyak 132,7 juta jiwa penduduk indonesia pengguna internet. Artinya, ada kenaikan sejumlah 10,56 juta jiwa dari hasil survey di tahun sebelumnya (Buletin Asosiasi Penyelenggara Jasa Internet Indonesia, 2018: 3). APJII juga telah memprediksikan di tahun-tahun yang akan datang jumlah lonjakan masyarakat pengguna internet terus bertambah dengan jumlah yang sama bahkan lebih, dan tidak akan mengalami penurunan jumlah bila infrastruktur internet akan terus dikembangkan di Indonesia.

Kenaikan jumlah pengguna internet di Indonesia yang begitu besar ini terjadi akibat dari faktor pembangunan infrastruktur yang semakin mempermudah masyarakat mengakses layanan internet dan juga mudahnya masyarakat memiliki perangkat internet. Perilaku pengguna internet Indonesia menunjukkan bahwa 70 persen dari pengguna internet di Indonesia mengakses internet dari perangkat bergerak atau *mobile gadget* (Buletin Asosiasi Penyelenggara Jasa Internet Indonesia, 2018: 3). Hal ini menunjukkan bahwa penggunaan internet *mobile* cukup tinggi, sedangkan penggunaan internet rumah cukup rendah. Hasil survey Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) juga menyebutkan bahwa sebagian besar pengguna internet Indonesia menggunakan internet untuk mengakses media sosial dan hiburan. *Facebook* menjadi tujuan sebagian besar pengguna internet Indonesia kemudian diikuti oleh Instagram. Pengguna internet Indonesia juga mulai percaya bahwa bertransaksi *online* aman, dengan menggunakan ATM untuk bertransaksi. Barang dan jasa utama yang dibeli melalui toko *online* seperti kebutuhan peralatan rumah tangga dan tiket suatu acara ataupun perjalanan.

Bukan hanya dari segi akses yang terus meningkat, tetapi juga dari durasi menggunakan internet. Pengguna internet di Indonesia menempati peringkat keempat dunia dengan durasi rata-rata menggunakan internet selama 8 jam 51 menit setiap harinya. Indonesia hanya "kalah" dari Thailand yang memiliki durasi 9 jam 38 menit, kemudian Filipina 9 jam 29 menit dan Brazil dengan 9 jam 14 menit. Peringkat Indonesia ini melampaui negara-negara maju seperti Singapura yang memiliki rata-rata durasi 7 jam 9 menit, Tiongkok 6 jam 30 menit, Amerika Serikat 6 jam 30 menit dan Jerman 4 jam 52 menit (Ramadhan 2018). Dengan demikian, masyarakat Indonesia pengguna internet menggantungkan sebagian besar aspek kehidupan sehari-harinya kepada internet. *Trend* ini cukup membanggakan, karena dengan kondisi tersebut menunjukkan bahwa masyarakat telah dapat menikmati perkembangan teknologi informasi untuk dipergunakan dalam kehidupannya sehari-hari. Namun hal ini juga mengkhawatirkan karena dengan *trend* pengguna internet di Indonesia yang begitu besar dan banyak ini

akan menimbulkan ancaman kejahatan siber, mengingat internet digunakan sebagai sarana aktivitas bagi manusia di dunia siber.

Internet telah memunculkan berbagai macam aplikasi yang dapat dimanfaatkan oleh penggunanya untuk berkomunikasi, mencari berita dan berbisnis. Perkembangan teknologi informasi dan komunikasi ini tentu saja menambah *trend* perkembangan teknologi dunia dengan segala bentuk kreativitas manusia. Perkembangan teknologi ini semakin meluas ke berbagai bidang, dimana masyarakat dengan cepat dapat mendapatkan informasi yang dibutuhkannya setiap saat. *Trend* penggunaan internet di masyarakat Indonesia tidak mengenal batas usia, kalangan, maupun status sosial. Mulai dari anak kecil hingga orang dewasa di Indonesia sudah dengan mudah untuk menggunakan internet. Pelajar, mahasiswa, dan karyawan setiap hari juga mengakses internet dengan mudahnya. Masyarakat dari kalangan atas, menengah, hingga bawah menggunakan internet sebagai salah satu aspek dalam kehidupan sehari-hari. Keadaan yang demikian akan semakin memperjelas fakta sekaligus prediksi bahwa jumlah pengguna internet yang ada di Indonesia akan terus bertambah dari tahun ke tahun. Jumlah pertambahannya akan selalu dalam sebuah presentase yang sangat besar.

Perkembangan teknologi informasi seperti mata uang koin yang memiliki dua sisi. Satu sisi dapat memberikan manfaat, mempermudah dan mempercepat akses informasi yang kita butuhkan dalam segala hal serta dapat mengubah model perekonomian dan model berbisnis. Namun demikian di sisi lainnya dapat menimbulkan dampak negatif yang tidak bisa dihindari. Indonesia sebagai negara dengan jumlah pengguna internet yang begitu besar sudah pasti akan terkena dampak (postif/negatif) tersebut secara langsung. Sebuah gambaran kondisi tentang adanya kemajuan teknologi (berupa internet) yang bisa dimanfaatkan oleh jumlah pengguna yang begitu banyak ini menjadi tantangan bagi pemerintah negara untuk mengawasi dan menanggulangi segala kemungkinan yang akan terjadi.

Masyarakat pengguna internet di Indonesia yang begitu banyak jumlahnya menimbulkan kerentanan. Seiring perkembangan teknologi internet dengan jumlah pengguna yang semakin banyak, maka akan menyebabkan munculnya kejahatan baru yang disebut dengan c*yber crime* dan *cyber terrorism* melalui jaringan internet. Seperti yang sudah dan sedang terjadi berulang-ulang yaitu munculnya beberapa kasus kejahatan siber di Indonesia, seperti penipuan, *hacking*, penyadapan data orang lain, *spaming e-mail* atau pemberian konten *e-mail* yang tidak diinginkan secara terus menerus, dan manipulasi data dengan program komputer untuk mengakses data milik orang lain. Kejahatan-kejahatan yang ditimbulkan oleh pelaku *cyber crime* telah merugikan dalam jumlah besar bagi korbannya serta perekonomian dan martabat bangsa Indonesia di mata dunia. Untuk penanggulangan permasalahan kejahatan internet ini diperlukan Lembaga-lembaga khusus, baik milik pemerintah maupun *Non-Government Organization* (NGO).

3.2 Pemanfaatan Dunia Siber di Indonesia

Perkembangan teknologi informasi yang terjadi pada hampir setiap negara sudah merupakan ciri global yang mengakibatkan hilangnya batas-batas negara. Negara yang sudah mempunyai infrastruktur jaringan informasi yang lebih memadai tentu telah menikmati hasil pengembangan teknologi informasinya, negara yang sedang berkembang dalam pengembangannya akan merasakan kecenderungan timbulnya neo-kolonialisme dalam hal baru. Hal tersebut menunjukan adanya pergeseran paradigma dimana jaringan informasi merupakan infrastruktur bagi perkembangan suatu negara (Golose, 2006: 31). Tanpa penguasaan dan pemahaman akan teknologi informasi ini, tantangan globalisasi akan menyebabkan ketergantungan yang tinggi terhadap pihak lain dan hilangnya kesempatan untuk bersaing karena minimnya pemanfaatan teknologi informasi.

Tentunya tidak dapat dipungkiri dengan kemajuan teknologi internet akan membawa pengaruh yang besar bagi perkembangan kehidupan manusia. Hal itu tentunya akan membawa dampak baik itu dari segi positif maupun negatif. Dari segi positif kemajuan teknologi patut disyukuri keberadaannya karena dengan

keberadaannya tentunya akan bisa dipergunakan untuk mempermudah dan memperlancar pekerjaan manusia. Internet telah banyak digunakan di berbagai bidang kehidupan dari bidang pendidikan, perbankan, bisnis maupun pemerintahan. Hal itu sesuai dengan klasifikasi pemanfaatan teknologi internet menurut Eoghan Casey dalam aspek kehidupan manusia (Casey, 2001: 16), yang mencakup:

a. *e-education* dalam bidang pendidikan
b. *e-banking* dalam bidang Perbankan
c. *e-commerce* dalam bidang ekonomi dan bisnis
d. *e-goverment* dalam bidang Pemerintahan

Klasifikasi manfaat dalam penggunaan internet tersebut menunjukkan bahwa dengan perkembangan dunia siber akan membawa banyak manfaat positif yang dapat dinikmati oleh manusia. Kemudahan-kemudahan dalam melakukan transaksi di dunia pendidikan, perbankan, transaksi penjualan ataupun pembelian dalam dunia bisnis, serta kemudahan dalam mengakses bidang pemerintahan, dan mungkin masih banyak lagi manfaat-manfaat yang akan dirasakan dalam bidang-bidang lainnya.

E-education di Indonesia lebih dikenal dengan istilah *e-learning*. Sistem *e-learning* di Indonesia tidak bisa dipastikan awal kemunculannya. Tidak ada sumber penelitian ataupun dan referensi kapan dimulainya sistem ini. Namun sistem e-learning di Indonesia sudah berada di tahap yang cukup bagus. Sudah cukup banyak atau nahkan hampir seluruh perguruan tinggi yang ada di Indonesia melakukan inovasi pembelajaran menggunakan teknologi informasi dan komunikasi. Sistem inovasi pembelajaran *e-learning* juga sudah mulai diterapkan di tingkat pendidikan di bawah universitas, yaitu di tingkat Sekolah Menengah Atas (SMA), Sekolah Menengah Pertama (SMP), dan Sekolah Dasar (SD). Sistem pembelajaran *e-learning* memungkinkan semua data dalam proses kegiatan belajar mengajar dikumpulkan, disimpan, dan dibagikan secara digital dan terhubung dengan koneksi internet. Pemanfaatan teknologi ini sangat bermanfaat untuk efisiensi kecepatan dan koordinasi antara pengajar dan siswa.

E-banking merupakan sistem perbankan berbasis digital yang dijalankan secara *online* atau terhubung ke internet. Perbankan Indonesia memasuki era baru sejak sekitar tahun 2000 di saat beberapa bank di Indonesia (baik milik swasta dan pemerintah) mulai mengimplementasikan sistem elektronik banking atau *e-banking*. *E-banking* sendiri bertujuan untuk memudahkan para nasabah bank yang menyediakan layana ini dengan hanya berperantara koneksi internet (BINUS University 2014). Dalam *e-banking* seorang nasabah dapat melakukan berbagai transaksi perbankan misalnya cek saldo, transfer dana, dan membayar tagihan-tagihan bulanan seperti listrik, PAM, telepon, cicilan kendaraan, dan lain-lain. Dalam pembahasan *e-banking* tidak akan lepas dari pembahasan internet *banking*. Internet banking adalah layanan perbankan melalui perangkat komputer/PC/laptop/tablet/smartphone via *web* yang dapat di akses oleh nasabah kapanpun dan di manapun selama mempunyai koneksi dengan internet. Saat inipun, seluruh perbankan yang ada di Indonesia menggunakan sistem *e-banking* untuk memanjakan nasabahnya. Keuntungan dari pihak perbankan sendiri dalam menggunakan sistem ini adalah adanya kecepatan dan kemudahan untuk mengakses arus lalu lintas data transaksi yang dilakukan oleh pihak bank dan pihak nasabah.

E-commerce merupakan sebuah sistem perdagangan yang dilakukan secara digital dan membutuhkan sebuah koneksi internet. *E-commerce* diperkenalkan pada tahun 1994 saat pertama kali *banner* elektronik digunakan untuk tujuan promosi dan periklanan di suatu halaman *website*. Pada saat yang bersamaan, para pelaku bisnis di Indonesia merespon dengan memunculkan sebuah model bisnis konvensional yang dialihkan pada sistem penjualan melalui *website* (Adhi, 2016). Oleh karena itu muncul banyak model *e-commerce* di Indonesia yang membuat masyarakat Indonesia menikmati keberadaanya hingga saat ini. Ekosistem *e-commerce* yang terus berkembang juga mendorong diluncurkannya beraneka macam layanan pembayaran. Ketika aktivitas jual beli dilakukan secara digital, proses pembayarannya pun menyesuaikan. Muncul juga layanan uang elektronik sebagai bentuk inovasi dan adaptasi yang terus bergulir.

E-goverment adalah penggunaan teknologi informasi dan telekomunikasi dalam pengolahan data yang terhubung dengan koneksi internet untuk mengolah administrasi pemerintahan yang efisien dan efektif, serta memberikan pelayanan yang transparan dan memuaskan kepada masyarakat (Bastian, 2003). Semua organisasi pemerintahan akan terpengaruh oleh perkembangan *e-government* ini. *E-government* dapat digolongkan dalam empat tingkatan dalam penerapannya. Tingkat pertama adalah pemerintah mempublikasikan informasi melalui *website*. Tingkat kedua adalah interaksi antara masyarakat dan kantor pemerintahan melaui *e-mail*. Tingkat ketiga adalah masyarakat pengguna dapat melakukan transaksi dengan kantor pemerintahan secara timbal balik. Level terakhir adalah integrasi di seluruh kantor pemerintahan, di mana masyarakat dapat melakukan transaksi dengan seluruh kantor pemerintahan yang telah mempunyai pemakaian *data base* bersama (Badan Perencanaan Pembangunan Nasional, 2013). Sistem *e-government* di Indonesia tidak hanya digunakan di lingkungan pemerintahan pusat saja, pemeritahan pusat juga memberikan perintah pada pemerintahan daerah-daerah di Indonesia untuk mengelola pemerintahan dengan sistem tersebut.

3.3 Kejahatan Siber di Indonesia

Kejahatan siber terjadi karena beberapa sebab, antara lain adanya pelaku kejahatan, modus kejahatan, kesempatan untuk melakukan kejahatan, korban kejahatan, reaksi sosial atas kejahatan, dan hukum. Rata-rata yang menjadi pelaku kejahatan adalah mereka yang lebih menguasai teknologi ini dan menggunakan kemampuannya itu untuk melakukan akses yang tidak sah ke jaringan komputer orang lain. Menurut Eoghan Casey, ada 4 kategori kejahatan siber (Casey, 2001: 12), yaitu:

1. *a computer can be the object of crime*
2. *a computer can be a subject of crime*
3. *the computer can be used as the tool for conducting for planning a crime*
4. *the symbol of computer it self can be used to intimidate or deceive*

Pelaku kejahatan siber adalah mereka yang paham dan mahir dalam dunia siber ini. Kejahatan siber dapat menembus ruang dan waktu, tidak ada batas negara, tidak mengenal yurisdiksi, dan dapat dilakukan dari mana saja dan kapan saja. Selain itu, kejahatan siber tidak hanya terjadi pada lingkup global, tetapi juga dalam lingkup kenegaraan.

Indonesia juga turut merasakan salah satu dampak dari konstelasi siber global yaitu kejahatan siber ini sendiri. Serangan kejahatan siber di Indonesia meningkat dari tahun ke tahun, dengan tipe dan variasi serangan yang berbeda dari tahun sebelumnya, namun ada juga yang masih sama. Jumlah serangan siber di Indonesia semakin meningkat, dari 28,430,843 pada tahun 2015 meningkat menjadi 135.672.984 pada tahun 2016. 47% dari keseluruhan kasus yang terjadi merupakan serangan *malware*, 44% merupakan penipuan, sedangkan sisanya berbentuk kejahatan siber lainnya, seperti *website defacement*, dan aktivitas manipulasi data dan kebocoran data. *Trend* peningkatan kejahatan siber dalam bentuk penyebaran konten ilegal, *hate speech* dan sejenisnya (Id-SIRTII/CC, 2017).

Beragam jenis aksi kejahatan siber terjadi di Indonesia. Mulai dari kejahatan terhadap perangkat keras (*hardware*), kejahatan terhadap perangkat lunak (*software*), hingga pencurian data dan informasi. Bila dikategorikan menurut kategori yang sudah dijelaskan oleh Eoghan Casey, maka kejahatan terhadap perangkat keras masuk dalam kategori *a computer can be the object of crime*, sementara kejahatan terhadap perangkat lunak masuk dalam kategori *a computer can be the subject of crime*, dan pencurian data dan informasi masuk dalam kategori *the symbol of computer it self can be used to intimidate or deceive*. Sumber dari aksi-aksi tersebut bukan hanya untuk kepentingan pribadi seseorang, namun juga bersumber dari kepentingan kelompok/organisasi/golongan tertentu, serta kepentingan negara lain. Tidak bisa dipungkiri bahwa kejahatan siber juga menarget dan menyerang unit-unit vital negara secara efektif dan masif.

Badan bentukan Kementerian Komunikasi dan Informatika Republik Indonesia yang bertugas sebagai badan pengamanan dan pemanfaatan jaringan telekomunikasi berbasis protokol internet di Indonesia, *Indonesia Security*

Incident Response Team on Internet and Infrastructure/Coordination Center (Id-SIRTII/CC) merilis laporan kondisi keamanan internet Indonesia selama tahun 2017. Hasilnya, dalam laporan yang diterbitkan itu, Id-SIRTII/CC mengungkap bahwa ada sekitar 205.502.159 serangan ke Indonesia. Serangan paling banyak berasal dari *malware* dengan 36.423.773 aktivitas sepanjang tahun 2017 (Damar, 2017). Data tersebut menggambarkan bahwa Indonesia adalah salah satu dari negara di dunia yang sangat rentan sekali terhadap serangan kejahatan siber. Secara individu, pengguna internet di Indonesia yang sangat aktif menjadi sasaran langsung serangan kejahatan siber. Hal itu sangat berbahaya, namun yang lebih membahayakan lagi, dikhawatirkan banyaknya serangan itu akan mengincar akses kenegaraan yang memunculkan kemungkinan stabilitas keamanan negara terancam oleh serangan kejahatan siber.

Data yang dihasilkan oleh Id-SIRTI/CC juga bisa memberi gambaran keadaan tentang lambatnya Indonesia merespon atau bereaksi terhadap arus kemajuan teknologi. Indonesia termasuk negara yang lambat mengikuti perkembangan teknologi komunikasi modern. Indonesia tidak memiliki prioritas pada strategi pengembangan dan penguasaan teknologi. Kemudian yang terjadi, transfer teknologi yang berasal dari negara maju tidak serta merta diikuti dengan penguasaan teknologi oleh negara berkembang seperti Indonesia. Indonesia merupakan negara yang memiliki kesenjangan digital yang cukup besar. Kesenjangan digital ini dapat diartikan sebagai adanya jurang diantara mereka yang mampu mengakses teknologi komunikasi dan yang tidak mampu (Staubhaar dan Rose, 2000: 9). Hal itu terjadi akibat adanya ketimpangan untuk menggunakan teknologi komunikasi digital tidak merata di Indonesia.

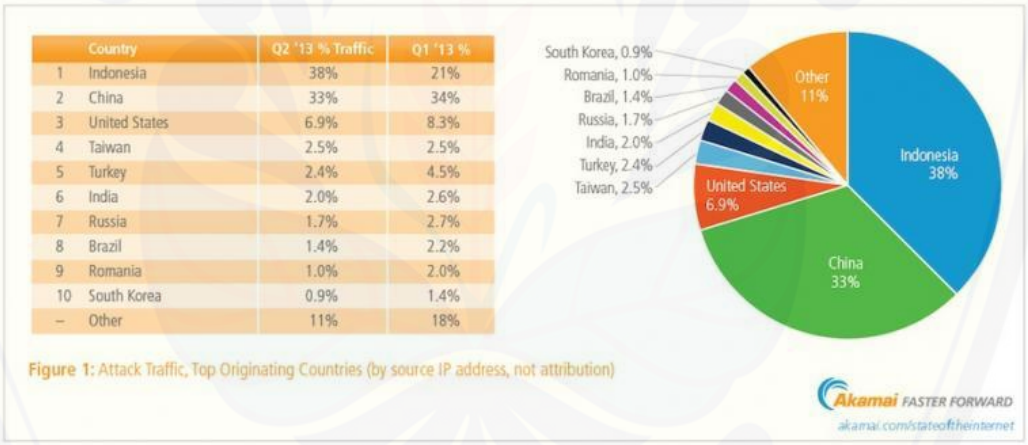
Para pelaku kejahatan siber menganggap Indonesia sebagai negara dengan pasar potensial untuk diserang karena melihat dari jumlah pengguna internet dan besaran jumlah pasar secara ekonomi. Bukti bahwa Indonesia masih menjadi pasar potensial bagi para pelaku kejahatan siber untuk melancarkan aksinya adalah saat kepolisian Indonesia yang bekerja sama dengan kepolisian China pada bulan Juli 2017 mengungkap kejahatan dengan modus pembelian barang dengan kartu kredit palsu atau kartu kredit orang lain yang telah diakses secara ilegal oleh

pelaku. Pihak kepolisian Indonesia mengungkap kejahatan tersebut sering terjadi di empat lokasi di Indonesia menjadi titik sindikat asal China dan Taiwan ini melakukan kejahatannya yakni Surabaya, Jakarta, Bali dan Batam (Purnama 2017).

Selain aksi kejahatan siber berbentuk pencurian dengan metode *digital hacking*, Indonesia adalah negara yang rentan dengan kejahatan siber berbentuk penyebaran *illegal contents*. *Illegal contents* sendiri 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, 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.

Kebebasan berbicara, berpendapat, dan menyebar-luaskan kabar di Indonesia menjadi salah satu faktor terkuatnya. Apalagi, dunia siber telah memberikan macam-macam aplikasi media sosial. Jaringan media yang sangat mudah dan praktis untuk diakses kapan saja, di mana saja, dan oleh siapa saja. Hal itu yang membuat sebuah konten berita sangat mudah diputar dan dibalikkan faktanya, hingga menjadi sebuah kejahatan siber berbentuk *illegal contents*. Pada dasarnya, aksi kejahatan siber *illegal content* bentuknya bermacam-macam. Namun yang sering terjadi di Indonesia yaitu, penyebaran kabar pembohongan publik (hoax), penyebaran konten pornografi, aksi persekusi (*bullying*) yang dilakukan di berbagai media sosial (Saputra, 2016). Ketiga aksi kejahatan siber tersebut menjadi aksi kejahatan siber yang sering terjadi di Indonesia, baik dilakukan oleh masyarakat dalam negeri sendiri dan juga masyarakat luar negeri. Tentunya ketika kejahatan siber dalam bentuk apapun dilakukan, dampaknya akan membuat kegaduhan di tengah-tengah masyarakat. Hal itu yang memicu adanya ketidak stabilan keamanan masyarakat bila terus menerus dilakukan dan terjadi. Padahal pemerintah negara memiliki fungsi menciptakan rasa aman bagi seluruh masyarakat dan keadaan negara.

Ketika Indonesia menjadi salah satu negara di dunia yang menjadi pasar potensial bagi para sindikat pelaku kejahatan siber sekaligus sebagai negara dengan tingkat kejahatan siber yang berada pada level darurat dan mengkhawatirkan, Indonesia juga ternyata tercatat sebagai negara penyumbang pelaku kejahatan siber. Menurut data yang dihasilkan oleh *State Of The Internet* pada 2013 yang menyebutkan bahwa dari 497 orang di dunia yang tertangkap karena kasus kejahatan siber 108 orang diantaranya merupakan warga negara Indonesia (KOMPAS, 2015). Bahkan banyaknya serangan siber yang berasal dari Indonesia, membuat Indonesia menduduki peringkat pertama negara yang paling banyak melakukan serangan siber. Salah satu perusahaan teknologi yang berasal dari Amerika Serikat bernama AKAMAI pada tahun 2018 merilis data sebagai berikut:



	Country	Q2 '13 % Traffic	Q1 '13 %
1	Indonesia	38%	21%
2	China	33%	34%
3	United States	6.9%	8.3%
4	Taiwan	2.5%	2.5%
5	Turkey	2.4%	4.5%
6	India	2.0%	2.6%
7	Russia	1.7%	2.7%
8	Brazil	1.4%	2.2%
9	Romania	1.0%	2.0%
10	South Korea	0.9%	1.4%
–	Other	11%	18%

Figure 1: Attack Traffic, Top Originating Countries (by source IP address, not attribution)

Akamai FASTER FORWARD
akamai.com/stateoftheinternet

Gambar 3.3 Negara Asal Serangan Siber

Sumber: AKAMAI Technologies. 2013. Negara Asal Serangan Siber. tekno.kompas.com. 17 Oktober 2013

AKAMAI Technologies merilis data 10 negara asal serangan siber terbesar. Gambar 3.3 menunjukkan bahwa Indonesia menyumbang 38 persen lalu lintas internet yang berhubungan dengan peretasan server pada kuartal kedua tahun 2013. Angka tersebut naik dari 21 persen pada kuartal pertama tahun 2013. Indonesia telah mengungguli China yang sebelumnya dikenal sebagai negara yang paling sering melakukan serangan siber. Kini China berada di peringkat kedua, yang menyumbang 33 persen dari lalu lintas aksi peretasan global. Sementara

Amerika Serikat turun menjadi 6,9 persen dan tetap berada di peringkat ketiga. Dalam penelitian ini, AKAMAI mengamati lalu lintas serangan siber di 175 negara berdasarkan alamat internet protokol atau *IP adress* (Panji, 2013).

Indonesia berada pada dua sisi, antara korban dan pelaku dalam hal adanya kejahatan siber. Satu sisi Indonesia adalah pasar potensial bagi sindikat internasional pelaku kejahatan siber karena pengguna internet di Indonesia terbilang sangat banyak dengan aktivitasnya yang bermacam-macam. Namun demikian di sisi lain, Indonesia adalah negara yang memiliki warga negara sebagai pelaku aksi kejahatan terbesar di dunia. Banyaknya pengguna internet di Indonesia membuat Indonesia mengalami kedua hal tersebut secara bersama-sama. Saat Indonesia sedang gencar untuk bereaksi melawan aksi kejahatan siber, di saat yang sama Warga Negara Indonesia (WNI) juga banyak yang tertangkap sebagai pelaku kejahatan siber dalam lingkup dalam negeri maupun internasional.

3.4 Kejahatan Terorisme Siber di Indonesia

Karakteristik aksi kejahatan terorisme siber yaitu memiliki sistem dalam segala aktivitasnya dan semua hal dilakukan secara terstruktur organisasi. Tindakan teror yang dilakukan dalam koridor dunia siber tersebut melakukan penyerangan terhadap suatu sistem. Baik itu jaringan komputer, internet, dan basis informasi dalam skala pribadi hingga data-data penting kenegaraan. Secara spesifik, sasaran sasaran aksi kejahatan terorisme siber adalah menimbulkan suatu kondisi kekerasan atau mengintimidasi pemerintah atau masyarakat secara umum melalui adanya teror untuk tujuan politik, sosial, ekonomi atau kerusakan pada infrastruktur suatu negara.

Indonesia merupakan salah satu negara yang sering diidentikan dengan aksi radikal terrorismenya oleh dunia internasional. Hal ini tidak mengherankan karena telah banyak aksi teroris yang terjadi di Indonesia dari tahun ke tahun. Indonesia memiliki banyak kemungkinan aksi terorisme siber yang bisa dilakukan dengan bebas dan meluas. Penyebab utamanya adalah regulasi tentang tindak kejahatan siber di Indonesia tidak terlalu kuat. Bahkan, belum ada regulasi khusus yang mengatur tentang terorisme siber. Pemerintah Indonesia dengan anggota

intelejennya juga belum kuat dalam penguasaan perangkat teknologi jaringan komputer dalam mendeteksi berbagai kemungkinan mengenai terorisme siber.

Aksi kejahatan terorisme siber di Indonesia terdiri dari pencurian dan penipuan kartu kredit untuk mendukung pendanaan dalam aksi terrorismenya. Ada juga yang berbentuk penyerangan/peretasan jaringan komputer atau *hacking* situs-situs milik institusi pemerintahan dan institusi swasta yang ada di Indonesia. Kemudian adanya penciptaan sebuah situs *online* yang ditujukan untuk melakukan aksi pembunuhan tanpa berada di lokasi. Meskipun pemerintah berhasil menemukannya, pemerintah masih tidak mampu mengatasinya sehingga aksi terorisme di Indonesia hingga kini terus bertambah. Indonesia sangat lemah dalam perlindungan data Internet.

Federal Beureau Investigation (FBI) secara resmi mengindikasikan bahwa kelompok ekstremis atau garis keras menggunakan identitas untuk mencuri dan melakukan penipuan kartu kredit untuk mendukung aktivitas terorisme mereka. Berdasarkan laporan media, kepolisian Indonesia meyakini bahwa pengeboman Bali tahun 2002 oleh sekelompok teroris sebagian didanai melalui penipuan kartu kredit secara online, Serangan di Bali dan beberapa negara juga kemungkinan didanai melalui pencurian kartu kredit (Rollins dan Wilson, 2007: 5). Salah satu aktor pelaku aksi pengeboman, Imam Samudra mendorong para pengikutnya dalam golongannya secara aktif mengembangkan kemampuan *hacking* agar mampu menyerang jaringan komputer Amerika Serikat. Imam Samudra menyebutkan beberapa situs dan *chat room* sebagai sumber-sumber mereka untuk meningkatkan kemampuan *hacking* mereka. Samudra mendesak remaja Muslim untuk mendapatkan angka pin kartu kreditnya dan menggunakannya untuk mendanai perjuangannya melawan Amerika Serikat dan sekutunya (Rollins dan Wilson, 2007: 18).

Menurut tim penyelidik, Samudra menggunakan laptop untuk berkomunikasi dengan kelompok ekstremis beberapa bulan sebelum melakukan pemboman. Pembicaraan mereka termasuk bagaimana secara curang menggunakan kartu kredit *online* untuk transfer uang yang digunakan sebagai dana serangan. Kepala unit kejahatan Indonesia, Kolonel Petrus Golose,

menyatakan Agung Prabowo, yang juga merupakan pembantu Imam Samudra, sebagai *hacker* professional. Agung Prabowo menciptakan sebuah situs yang digunakan untuk membunuh para warga Asing tanpa berada di lokasi serangan (VOA News, 2009). Dalam kasus lain, pada bulan Mei 2001, Laskar Jihad melakukan aksi kejahatan terorisme siber dengan meretas situs kedutaan besar Australia dan kepolisian Indonesia di Jakarta sebagai bentuk protes tertangkapnya pemimpin mereka, Ja'far Umar Thalib. Setiap akses situs keduanya, mereka mengarahkannya pada situs lainnya yang berisi peringatan kepada kepolisian Indonesia untuk membebaskan pemimpin mereka (Irwin, 2004: 83).

Pelaku terorisme siber melakukan rekrutmen anggota dan pelatihan merakit bom melalui media sosial. Selain itu, pelaku teroris juga mencari dana melalui *bitcoin* atau uang elektronik yang dijadikan sebagai acuan mata uang di dunia siber (Kementerian Komunikasi dan Informatika Republik Indonesia, 2016). Hal ini terbukti ketika pada bulan Mei 2017, Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais yang ada di Jakarta terkena serangan *ransomware* atau sebuah jenis *malware* yang dikendalikan oleh sekelompok peretas (*hacker*) menyerang komputer dengan cara mengunci semua file pada komputer korban sehingga tidak bisa diakses kembali. Kemudian kelompok peretas meminta dana tebusan agar file-file yang dibajak dengan enkripsi bisa dikembalikan dalam keadaan normal lagi. Para ahli menyebutkan dana tembusan yang diminta adalah dengan terlebih dahulu melakukan pembayaran menggunakan *bitcoin* yang setara dengan 300 dollar Amerika kepada para pelaku yang sebelumnya telah memberikan alamat *bitcoin* untuk pembayarannya (BBC News Indonesia, 2017).

Kementerian Komunikasi dan Informatika Republik Indonesia telah memastikan bahwa Indonesia merupakan salah-satu negara yang terdampak akibat serangan yang disebut sebagai terorisme siber. Aksi para pelaku terorisme siber merupakan aksi yang berbentuk adanya kepentingan suatu golongan/kelompok dan institusi kenegaraan. Kejadian-kejadian yang telah disampaikan di atas bisa membuktikan bahwa pelaku teroris di Indonesia juga telah masuk era baru dalam meluncurkan aksinya. Para pelaku teroris siber melakukan aksi di Indonesia dengan memanfaatkan dunia siber sebagai salah satu media perncanaan dan

komunikasi. Mereka terhubung dari satu negara ke negara lain dan antar jaringan organisasi yang saling berhubungan. Dunia siber yang identik dengan internet membuat para pelaku kejahatan terorisme siber semakin cepat melakukan segala aksinya karena adanya koneksi internet.

BAB 5. KESIMPULAN

Strategi yang telah disusun oleh Pemerintah Indonesia dalam menghadapi gelombang fenomena siber global adalah dengan membentuk badan dan organisasi khusus serta menjalankan program terpadu dalam bidang keamanan siber. Pemerintah Indonesia membuat BSSN dan Id-SIRTII/CC yang saling berkoordinasi untuk mengamati, mengawasi, mengedukais, dan menganalisa segala permasalahan yang muncul di dunia siber dan berdampak langsung terhadap sektor pertahanan, politik, ekonomi, dan sosial budaya di Indonesia. Kemudian Pemerintah Indonesia menyelenggarakan program *Born To Control* yang dijadikan sebagai ajang pencarian sumber daya manusia yang mampu menjadi 'tentara siber' untuk Indonesia.

Berbagai permasalahan muncul akibat konstelasi siber global yang sedang terjadi berdampak secara langsung terhadap Indonesia. Hal ini mengingat Indonesia adalah negara dengan jumlah pengguna internet yang sangat besar. Hal itu yang membuat Indonesia telah menjadi salah satu negara yang berpotensi besar sebagai sasaran kejahatan dan terorisme siber yang dilakukan oleh para pelaku maupun sindikat kejahatan siber internasional. Namun di sisi lain, banyak data yang menyebutkan bahwa Indonesia adalah negara penyumbang terbesar para pelaku dan sindikat kejahatan siber di dunia internasional yang kasusnya terus menerus terjadi. Semakin dikembangkannya infrastruktur teknologi internet di Indonesia, maka semakin rentan pula kondisi pertahanan dan keamanan Indonesia khususnya di bidang siber.

Konstelasi siber global telah membuat pemerintah Indonesia memiliki suatu dilema. Dilema yang muncul adalah, di satu sisi Indonesia sangat membutuhkan pengembangan teknologi dalam industri bisnis dan tata kelola pemerintahan. Pada sisi lainnya, sumber daya manusia yang dimiliki terbatas secara kemampuan. Pada masa yang akan datang, hal ini turut membawa masalah serius dan besar. Masalah dan ancaman yang cukup sensitif khususnya pada masalah ketahanan dan pertahanan negara dalam berbagai sektor.

Penyusunan strategi yang dibuat oleh Pemerintah Indonesia dalam menghadapi fenomena siber global merupakan aplikasi dari konsep strategi keamanan yang mengedepankan aspek penciptaan rasa aman bagi warga negara. Konsep keamanan nasional juga menjadi landasan konseptual yang mendukung kesesuaian teori sekuritisasi yang digunakan dalam penelitian ini. Sebab strategi yang disusun merupakan reaksi dari Pemerintah Indonesia dalam mengatasi permasalahan-permasalahan yang muncul akibat adanya fenomena siber global, seperti tindak kejahatan siber dan terorisme siber yang sudah dan mungkin akan terjadi di masa yang akan datang, mengingat perkembangan teknologi internet merupakan sebuah arus yang tidak bisa dianggap hanya lewat begitu saja.

DAFTAR PUSTAKA

Buku:

Arief, Barda Nawawi. 2007. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana.* Jakarta: Kencana Predana Media Group.

Casey, Eoghan. 2001. *Digital Evidence and Computer: Forensic Science, Computers and The Internet.* London: Harcourt Science and Technology Company.

Denning, Dorothy E. 2009. *Terror Webs: How The Internet Is Transforming Terrorism.* California: Willan Publishing.

Indrajit, Richardus Eko. 2011. "*Pengantar Konsep Keamanan Informasi di Dunia Siber*." Bandung: Graha Ilmu.

Irwin, Jones. 2004. *War and Virtual War: The Challenges to Communities.* Amsterdam: Rodopi.

Kartono, Kartini. 1990. *Metodologi Riset.* Bandung: CV. Mandar Maju.

Lessig, Lawrence. 2006. *Code Version 2.0.* Cambridge: Perseus Books Group.

Mas'oed, Mohtar. 1994. *Ilmu Hubungan Internasional Disiplin dan Metodologi.* Jakarta: Pustaka LP3ES Indonesia.

Mas'oed, Mochtar. 1989. *Studi Hubungan Internasional, Tingkat Analisis dan Teorisasi*. Yogyakarta: Pusat antar Universitas-studi Sosial UGM.

Ramli, Ahmad. 2006. *Cyber Law dan Haki Dalam Sistem Hukum Indonesia.* Bandung: Refika Aditama.

Soluka, Mark. 2000. *Ruang yang Hilang: Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan.* Bandung: Mizan.

Staubhaar, J., dan R. La Rose. 2000. *Media Now.* Jakarta: Salemba Empat.

Stephenson, Peter. 2000. *Investigating ComputerRelated Crime: A Hanbook For Corporate.* Washington D.C: CRC Press.

Wahid, Abdul, dan Mohammad Labib. 2005. *Kejahatan Mayantara (Cyber Crime).* Jakarta: PT. Refika Aditama.

Jurnal:

A'raf, Al. 2015. "Dinamika Keamanan Nasional." *Jurnal Keamanan Nasional Vol 1, No 1*.

Darmono, Bambang. 2010 . "Konsep Dan Sistem Keamanan Nasional Indonesia." *Jurnal Ketahanan Nasional Vol 15, No 1*.

Rahmawati, Ineu. 2017. "Analisis Manajemen Risiko Ancaman Kejahatan Siber." *Jurnal Pertahanan & Bela Negara Vol 7, No 2*.

Samad, Alfira Nurliliani. 2014 "Analisis Instrumen Cyber Terorrism Dalam Kerangka Sistim Hukum Internasional." *Jurnal Lex Crimen Vol 7, No 3*.

Soewardi, Bagus Artiadi. 2013. "Ancaman Siber dalam Perspektif Pertahanan Negara." *Jurnal Prodi Perang Asimetris Vol 4, No 2*.

Yunus, Zahri, dan Rabiah Ahmad. 2012. "A Dynamic Cyber-terrorism Framework." *Internasional Journal of Computer Science and Information Security Vol 10 No 2*.

Buletin dan Surat Kabar:

Buletin Asosiasi Penyelenggara Jasa Internet Indonesia. 2018. "Survey APJII." *Penetrasi Internet di Indonesia Capai 143 Juta Jiwa*. Bandung. APJII.

Golose, Petrus Reinhard. 2006. "Perkembangan Cyber Crime dan Upaya Penanganannya." *Buletin Hukum Perbankan dan Kebanksentralan*. Bandung. APJII.

Ida, Rachma. 2017. "Ledakan Industri Cybersecurity." Surabaya. *Jawa Pos*.

Internet:

Adhi. *Sejarah Bisnis e-Commerce di Indonesia dari Masa ke Masa.* 28 April 2016. https://www.money.id/digital/sejarah-bisnis-e-commerce-di-indonesia-dari-masa-ke-masa-160427f.html [diakses tanggal 19 Oktober 2018].

Badan Perencanaan Pembangunan Nasional. *Perkembangan E-government di Indonesia.* 14 Juni 2013. https://www.bappenas.go.id/files/8913/6508/2376/perkembangan-e-government-di-indonesia---oleh-bastian__20081223152111__1660__0.pdf [diakses tanggal 19 Oktober 2018].

Badan Siber dan Sandi Negara. *Deputi Bidang Identifikasi dan Deteksi.* 2017. https://bssn.go.id/deputi-bidang-identifikasi-dan-deteksi/ [diakses tanggal 31 Oktober 2018].

----------. *Pusat Operasi Keamanan Siber Nasional.* 2017. https://bssn.go.id/pusat-operasi-keamanan-siber-nasional/ [diakses tanggal 31 Oktober 2018].

----------. *Sejarah Persandian.* 2017. https://bssn.go.id/sejarah-persandian/ [diakses tanggal 29 Oktober 2018].

----------. *Tugas dan Fungsi BSSN.* 2017. https://bssn.go.id/tugas-dan-fungsi-bssn/ [diakses tanggal 29 Oktober 2018].

Basariyadi, Abdi. *Cyber Crime: Pengertian, Jenis-jenis dan Contohnya.* 31 August 2017. https://majalahpendidikan.com/cybercrime-pengertian-jenis-jenis-dan-contohnya/ [diakses tanggal 4 September 2018].

Bastian. *Perkembangan "E-government" di Indonesia.* 8 Maret 2003. https://www.bappenas.go.id/files/8913/6508/2376/perkembangan-e-government-di-indonesia---oleh-bastian__20081223152111__1660__0.pdf [diakses tanggal 19 Oktober 2018].

BBC News Indonesia. *Indonesia Diserang Teroris Siber, Pemerintah Meminta Masyarakat Tenang.* 13 Mei 2017. https://www.bbc.com/indonesia/39907370 [diakses tanggal 22 Oktober 2018].

BINUS University. *E-banking Perbankan Indonesia.* 14 April 2014. https://sis.binus.ac.id/2014/04/14/e-bankingperbankan-indonesia/ [diakses tanggal 19 Oktober 2018].

Bohang, Fatimah Kartini. *Berapa Jumlah Pengguna Internet di Indonesia?* 22 February 2018. https://tekno.kompas.com/read/2018/02/22/16453177/berapa-jumlah-pengguna-internet-indonesia [diakses tanggal 8 Maret 8 2018].

Chendramata, Aidil. *Kebijakan Cyber Security Dukung Nawacita, Amankan 8 Sektor Strategis.* 10 Agustus 2017. https://kominfo.go.id/content/detail/10308/kebijakan-cyber-security-dukung-nawacita-amankan-8-sektor-strategis/0/berita_satker [diakses tanggal 31 Oktober 2018].

Damar, Agustinus Mario. *Indonesia Alami 205 Juta Serangan Siber Sepanjang 2017.* 22 Desember 2017. https://www.liputan6.com/tekno/read/3203987/indonesia-alami-205-juta-serangan-siber-sepanjang-2017 [diakses tanggal 18 Oktober 2018].

Dalimi, Daya Perwira. "Mengatur Cyber Space." *Rangkuman Hukum Siber*. 21 Maret 2017. https://id.scribd.com/document/213662445/Rangkuman-Materi-Hukum-Siber [diakses tanggal 18 Oktober 2018].

Denning, Dorothy E. *Cyberterrorism.* 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html [diakses tanggal 10 September 2018].

Gema, Ari Jualiano. *Cybercrime: Sebuah Fenomena di Dunia Maya.* 30 July 2000. http://www.hukumonline.com/berita/baca/hol229/cybercrime-sebuah-fenomena-di-dunia-maya [diakses tanggal 27 Agustus 2018].

Go-Gulf. *Yearly Cyber Crime Victim Count Estimate.* 20 May 2018. http://www.go-gulf.ae/yearly-cyber-crime-victim-count-estimate [diakses tanggal 3 September 2018].

Id-SIRTII/CC. *Pengantar Strategi Keamanan Siber Indonesia.* 2017. https://idsirtii.or.id/halaman/tentang/pengantar-strategi-keamanan-siber-indonesia.html [diakses tanggal 28 Oktober 2018].

----------. *Ruang Lingkup.* 2017. https://www.idsirtii.or.id/halaman/tentang/ruang-lingkup.html [diakses tanggal 31 Oktober 2018].

----------. *Sejarah Id-SIRTII/CC.* 2017. https://www.idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html [diakses tanggal 31 Oktober 2018].

IPLURAL. *Internet, Keberagaman, dan Perdamaian Siber dalam Diplomasi Kontemporer Indonesia.* 15 August 2017. http://www.iplural.org/2017/08/internet-keberagaman-dan-perdamaian-siber-dalam-diplomasi-kontemporer-indonesia/ [diakses tanggal 6 Februari 2018].

Iza, Noor. *"Born To Control" Penjaringan 10.000 Kandidat Gladiator Cyber Security Indonesia.* 25 Januari 2017. https://kominfo.go.id/content/detail/9012/siaran-pers-no12-hmkominfo012017-tentang-born-to-control-penjaringan-10000-kandidat-gladiator-cyber-security-indonesia/0/siaran_pers [diakses tanggal 5 November 2018].

Kementerian Luar Negeri Republik Indonesia. *Kemlu Beri Perhatian Serius pada Diplomasi Siber.* 31 August 2017. https://www.kemlu.go.id/id/berita/Pages/Kemlu-Beri-Perhatian-Serius-pada-Diplomasi-Siber.aspx [diakses tanggal 9 November 2017].

Kementerian Komunikasi dan Informasi Republik Indonesia. *Jumlah Pengguna Internet 2017 Meningkat, Kominfo Terus Lakukan Percepatan Pembangunan Broadband.* 19 Februari 2018. https://kominfo.go.id/index.php/content/detail/12640/siaran-pers-no-53hmkominfo022018-tentang-jumlah-pengguna-internet-2017-meningkat-kominfo-terus-lakukan-percepatan-pembangunan-broadband/0/siaran_pers [diakses tanggal 15 Oktober 2018].

----------. *Kapolri: Ada terorisme siber, rekrutmen & pelatihan bom lewat online.* 22 Desember 2016. https://kominfo.go.id/content/detail/8523/kapolri-ada-terorisme-siber-rekrutmen-pelatihan-bom-lewat-online/0/sorotan_media [diakses tanggal 23 Oktober 2018].

----------. *Pengguna Internet Indonesia Nomor Enam Dunia.* 24 November 2014.

https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media [diakses tanggal 16 Oktober 2018].

----------. *Indonesia Butuh Penangkal Serangan "Cyber".* 21 April 2015. https://kominfo.go.id/index.php/content/detail/4787/Indonesia+Butuh+Penangkal+Serangan+%E2%80%9CCyber%E2%80%9D/0/sorotan_media [diakses tanggal 13 Maret 2018].

----------. *Penjelasan Adanya HOAX Terkait informasi viral Sistem Big Data Cyber Security dan Cybercrime Police*. 26 October 2015. https://www.kominfo.go.id/content/detail/6288/siaran-pers-no84pihkominfo102015-tentang-penjelasan-kementerian-kominfo-terkait-sistem-big-data-cyber-security-dan-cybercrime-police/0/siaran_pers [diakses tanggal 13 Maret 2018].

----------. "Program Born To Control." *Kementerian Komunikasi Dan Informatika.* 25 Januari 2017. https://web.kominfo.go.id/sites/default/files/users/3645/FAQ%20BTC.pdf [diakses tanggal 31 Oktober 2018].

Kementerian Pertahanan Republik Indonesia. *Pedoman Pertahanan Siber*. 14 Oktober 2016. https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf [diakses 29 Oktober 2019].

KOMPAS. *Indonesia Urutan Kedua Terbesar Negara Asal "Cyber Crime" di Dunia.* 12 May 2015. http://nasional.kompas.com/read/2015/05/12/06551741/Indonesia.Urutan.Kedua.Terbesar.Negara.Asal.Cyber.Crime.di.Dunia [diakses tanggal 20 Februari 2018].

----------. *Indonesia Urutan Kedua Terbesar Negara Asal "Cyber Crime" di Dunia.* 12 May 2015. http://nasional.kompas.com/read/2015/05/12/06551741/Indonesia.Urutan.Kedua.Terbesar.Negara.Asal.Cyber.Crime.di.Dunia [diakses tanggal 20 Februari 2018].

Panji, Aditya. *Serangan "Cyber" Dunia, Terbanyak dari Indonesia.* 17 Oktober 2013. https://tekno.kompas.com/read/2013/10/17/0811211/Serangan.Cyber.Dunia.Terbanyak.dari.Indonesia [diakses tanggal 21 Oktober 2018].

Pratama, Bambang. *Hukum Siber Dalam Dinamika Disruptive Innovation*. 6 Juli 2017. https://www.researchgate.net/publication/319327733_PERSPEKTIF_HUKUM_SIBER_DALAM_MENANGKAP_FENOMENA_DISRUPTIVE_INNOVATION [diakses tanggal 30 Oktober 2018].

Purnama, Dara. *Indonesia Jadi Pasar Potensial Kejahatan Siber, Apa Sih Penyebabnya?* 31 Juli 2017. https://news.okezone.com/read/2017/07/31/337/1746803/indonesia-jadi-pasar-potensial-kejahatan-siber-apa-sih-penyebabnya [diakses tanggal 20 Oktober 2018].

Purnomo, Nurmulai Rekso. *Permasalahan Virus Petya Akan Ditangani Lebih Baik Oleh BSSN.* 1 Juli 2017. http://www.tribunnews.com/nasional/2017/07/01/permasalahan-virus-petya-akan-ditangani-lebih-baik-oleh-bssn [diakses tanggal 6 Desember 2018].

Ramadhan, Bagus. *Inilah Perkembangan Digital Indonesia Tahun 2018.* 6 Februari 2018. https://www.goodnewsfromindonesia.id/2018/02/06/inilah-perkembangan-digital-indonesia-tahun-2018 [diakses tanggal 16 Oktober 2018].

Rollins, John, dan Clay Wilson. *Terrorist Capabilities for Cyberattack: Overview and Policy Issues.* 22 Januari 2007. https://fas.org/sgp/crs/terror/RL33123.pdf [diakses tanggal 23 Oktober 2018].

Saputra, Andi. *UU ITE Perubahan Berlaku, Ini 6 Konten yang Terancam Penjara.* 28 November 2016. https://news.detik.com/berita/d-3356295/uu-ite-perubahan-berlaku-ini-6-konten-yang-terancam-penjara [diakses tanggal 21 Oktober 2018].

Sekretariat Kabinet Republik Indonesia. *Perpres Direvisi, Badan Siber dan Sandi Negara Kini Berada Langsung di Bawah Presiden.* 30 December 2017. http://setkab.go.id/perpres-direvisi-badan-siber-dan-sandi-negara-kini-berada-langsung-di-bawah-presiden/ [diakses tanggal 13 Maret 2018].

Setiadi, Djoko. *Pengantar Strategi Keamanan Siber Indonesia.* Juni 2018. https://bssn.go.id/strategi-keamanan-siber-nasional/ [diakses tanggal 31 Oktober 2018].

Suara Merdeka. *Jenis-jenis Cyber Crime.* 24 July 2002. http://www.suaramerdeka.com/harian/0207/24/nas13.html. [diakses tanggal 4 September 2018].

Utama, Linardi. *Diplomasi Siber Indonesia.* 30 September 2017. https://kompas.id/baca/opini/2017/09/30/diplomasi-siber-indonesia/ [diakses tanggal 9 November 2017].

VOA News. *Indonesian Police Charge Two Suspects with Cyber-Terrorism.* 31 Oktober 2009. https://www.voanews.com/a/a-13-2006-08-23-voa32/400055.html [diakses tanggal 22 Oktober 2018].

Wibowo, Satriyo. *BSSN dan Peta Keamanan Siber Indonesia.* 5 Maret 2018. https://inet.detik.com/cyberlife/d-3899799/bssn-dan-peta-keamanan-siber-indonesia [diakses tanggal 31 Oktober 2018].

Wulan, R. Teja. *Mengkhawatirkan, Tingkat Cyber Crime di Indonesia.* 17 October 2014. http://nationalgeographic.co.id/berita/2014/10/mengkhawatirkan-tingkat-cyber-crime-di-indonesia [diakses tanggal 20 Februari 2018].