UPAYA PEMERINTAH SHINZO ABE DALAM MENINGKATKAN KEAMANAN NASIONAL JEPANG DARI ANCAMAN KEJAHATAN DUNIA MAYA

(*THE EFFORTS OF SHINZO ABE'S GOVERNMENT IN IMPROVING JAPAN'S NATIONAL SECURITY FROM CYBER CRIME THREAT*)

SKRIPSI

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

Oleh
Puspaningrum
100910101040

JURUSAN ILMU HUBUNGAN INTERNASIONAL
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS JEMBER
2015

UPAYA PEMERINTAH SHINZO ABE DALAM MENINGKATKAN KEAMANAN NASIONAL JEPANG DARI ANCAMAN KEJAHATAN DUNIA MAYA

(*THE EFFORTS OF SHINZO ABE'S GOVERNMENT IN IMPROVING JAPAN'S NATIONAL SECURITY FROM CYBER CRIME THREAT*)

SKRIPSI

Oleh
Puspaningrum
100910101040

JURUSAN ILMU HUBUNGAN INTERNASIONAL
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS JEMBER
2015

PERSEMBAHAN

Skripsi ini saya persembahkan untuk:

1. Kedua orang tua tercinta saya, Ibunda Lilik Ayuliningsih dan Ayahanda Made Permadi;
2. Guru-guru saya sejak taman kanak-kanak sampai dengan Perguruan Tinggi;
3. Almamater.

MOTTO

Sesungguhnya bersama kesulitan ada kemudahan[*)]

*) Alquran. QS. As-Syarh: 6. Hlm. 596.

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Puspaningrum

NIM : 100910101040

Menyatakan dengan sesungguhnya bahwa karya ilmiah yang berjudul "Upaya Pemerintah Shinzo Abe dalam Meningkatkan Keamanan Nasional Jepang dari Ancaman Kejahatan Dunia Maya" adalah benar-benar hasil karya sendiri, kecuali kutipan yang sudah saya sebutkan sumbernya, belum pernah diajukan pada institusi mana pun, 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 mana pun serta bersedia mendapat sanksi akademik jika ternyata di kemudian hari pernyataan ini tidak benar.

Jember, 20 Maret 2015

Yang menyatakan

Puspaningrum
NIM. 100910101040

SKRIPSI

UPAYA PEMERINTAH SHINZO ABE DALAM MENINGKATKAN KEAMANAN NASIONAL JEPANG DARI ANCAMAN KEJAHATAN DUNIA MAYA

Oleh

Puspaningrum
100910101040

Pembimbing

Dosen Pembimbing Utama : Agus Trihartono, S. Sos.,M.A.,Ph.D.
Dosen Pembimbing Anggota : Adhiningasih P., S. Sos.,M.Si.

PENGESAHAN

Skripsi berjudul "Upaya Pemerintah Shinzo Abe dalam Meningkatkan Keamanan Nasional Jepang dari Ancaman Kejahatan Dunia Maya" telah diuji dan disahkan pada:

hari : Jumat
tanggal : 27 Maret 2015
waktu : 13.30 WIB
tempat : Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jember

Tim Penguji:

Ketua

Drs. Bagus Sigit Sunarko, M.Si.,Ph.D.
NIP. 196802291998031001

Sekretaris I

Agus Trihartono, S.Sos.,M.A.,Ph.D.
NIP. 196908151995121001

Sekretaris II

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

Anggota I

Drs. M. Nur Hasan, M. Hum.
NIP. 195904231987021001

Anggota II

Drs. Agung Purwanto, M.Si.
NIP. 196810221993031002

Mengesahkan
Dekan Fakultas Ilmu Sosial dan Ilmu Politik,
Universitas Jember

Prof. Dr. Hary Yuswadi, M.A.
NIP. 195207271981031003

RINGKASAN

"Upaya Pemerintah Shinzo Abe dalam Meningkatkan Keamanan Nasional Jepang dari Ancaman Kejahatan Dunia Maya"; Puspaningrum, 100910101040; 2015: 95 halaman; Jurusan Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jember.

Jepang merupakan salah satu negara dengan pengguna teknologi dan internet tertinggi di dunia. Internet telah memberikan banyak kemudahan dalam hidup manusia, seperti berkomunikasi, melakukan transaksi, mencari hiburan, memperoleh informasi dan masih banyak lagi manfaat-manfaat yang dirasakan oleh manusia. Pada perkembangannnya, ternyata penggunaan internet berpotensi menimbulkan kejahatan yaitu sebagai kejahatan dunia maya *(cyber crime)*. Sejak kecanggihan kejahatan dunia maya menyerang perusahaan kontraktor terbesar di Jepang yaitu Mitsubishi Heavy Industries Ltd, keamanan dunia maya telah menjadi bagian penting dari agenda keamanan nasional negara itu. Pemerintah Jepang melalui Perdana Menteri Shinzo Abe menyatakan bahwa Kabinet Perdana Menteri Shinzo Abe akan lebih berperan aktif dalam meningkatkan keamanan dunia maya, dan mengungkapkan kekhawatiran mengenai peningkatan kejahatan dunia maya internasional. Oleh karena itu, penelitian ini bertujuan untuk mengetahui upaya Pemerintah Shinzo Abe dalam meningkatkan keamanan dunia maya di Jepang.

Metode yang digunakan dalam penulisan karya tulis ilmiah ini adalah metode pengumpulan data dan teknik analisis data. Teknik pengumpulan data adalah studi pustaka *(library research)* untuk memperoleh data sekunder. Data tersebut kemudian dianalisis melalui metode deskriptif.

Hasil penelitian menunjukkan bahwa upaya yang dilakukan untuk menjaga dan meningkatkan keamanan dunia maya pada Pemerintahan Shinzo Abe adalah pembuatan strategi keamanan dunia maya pada tahun 2013; pembentukan unit khusus yang bertanggung jawab untuk menjaga keamanan dunia maya khususnya keamanan Departemen Pertahanan Jepang atau *Japanese Ministry of Defense (JmoD)* dan Pasukan Pertahanan Jepang atau *Self Defense Forces (SDF)* yaitu Unit Pertahanan Dunia Maya *(Cyber Defense Unit)*, dan kolaborasi antara negara Jepang dan negara-negara yang mempunyai fokus yang sama dalam masalah keamanan dunia maya. Upaya tersebut menunjukkan bahwa Pemerintah Jepang sangat serius menanggapi kejahatan dunia maya melalui peningkatan pertahanan diri negara terhadap serangan dunia maya nasional dan internasional.

PRAKATA

Puji syukur kepada Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **"Upaya Pemerintah Shinzo Abe dalam Meningkatkan Keamanan Nasional Jepang dari Ancaman Kejahatan Dunia Maya"**. Skripsi ini disusun untuk memenuhi salah satu syarat menyelesaikan pendidikan strata satu (S1) pada jurusan Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jember.

Penyusunan skripsi ini tidak lepas dari bantuan berbagai pihak. Oleh karena itu, penulis menyampaikan terima kasih kepada:

1. Bapak Agus Trihartono, S.Sos.,M.A.,Ph.D., selaku Dosen Pembimbing Utama dan Ibu Adhiningasih P.,S.Sos.,M.Si., selaku Dosen Pembimbing Anggota yang telah meluangkan waktu, pikiran, perhatian, dan bimbingan dalam penulisan skripsi ini;
2. Bapak Drs. Joko Susilo, M.Si., selaku Dosen Pembimbing Akademi atas dorongan dan bimbingannya selama penulis menjadi mahasiswa;
3. Bapak dan Ibu dosen di Jurusan Ilmu Hubungan Internasional FISIP Universitas Jember yang telah memberikan ilmu dan bimbingan selama penulis menjadi mahasiswa;
4. Kedua orang tua penulis, bapak Made Permadi dan Ibu Lilik Ayuliningsih, serta satu-satunya kakak tercinta penulis, Purwoko. Terimakasih untuk setiap dukungan dan pengorbanan yang telah diberikan demi kelancaran studi penulis;
5. Motivator dan orang yang tidak henti-hentinya ada disamping penulis, mendukung penulis dari awal hingga akhir untuk tidak patah semangat dengan hambatan-hambatan yang muncul saat penulisan skripsi ini, tidak lain adalah tunangan penulis M. Aziz Al Basid. Terimakasih untuk motivasi dan semangat yang selalu mas Basid berikan selama ini;

6. Sahabat sekaligus saudari tercinta penulis yang setia menemani penulis dari awal hingga akhir menyelesaikan studi, Fani, Sheny, dan Fitri. *Can't imagine my life without you girls*;
7. Nadia, Debby, Annisa, dan semua teman-teman di Jurusan Ilmu Hubungan Internasional FISIP Universitas Jember angkatan 2010 yang tidak mungkin penulis sebutkan satu-persatu. Terima kasih telah menjadi teman untuk berbagi dan diskusi dalam penyelesaian skripsi ini;
8. Semua pihak yang tidak dapat disebutkan satu per satu atas bantuannya dalam penyelesaisn 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 bermanfaat.

Jember,

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR DIAGRAM

DAFTAR SINGKATAN

AJCT	= *ASEAN-Japan Counter-Terrorism*
CDU	= *Cyber Defense Unit*
CEPTOAR	= *Capability for Engineering of Protection, Technical Operation, Analysis and Response*
CERT-In	= *Computer Emergency Response Team India*
C4SC	= *the Command, Control, Communication, Computer, System Command*
CSIRTs	= *Computer Security Incident Response Teams*
DII	= *Defense Information Infrastructure*
GSOC	= *Government Security Operation Coordination team*
ICT	= *Information and Communication Technology*
IHI	= *Ishikawajima-Harima Industries*
ICS	= *Industrial Control System*
ISMS	= *Information Security Management System*
ISPC	= *Information Security Policy Council*
ISPs	= *Internet Service Providers*
JAXA	= *Japan Aerospace Exploration Agency*
JASPER	= *Japan-ASEAN Security Partnership*
JGSDF	= *Japan Ground Self-Defense Force*
JMoD	= *Japanese Ministry of Defense*
MCIT	= *Ministry for Communication and Information Technology*
METI	= *Ministry of Economy, Trade, and Industry*
MHI	= *Mitsubishi Heavy Industries*
MIC	= *Ministry of Internal Affairs and Communication*
NATO	= *North Atlantic Treaty Organization*
NISC	= *National Informastion Security Center*
NPA	= *National Police Agency*
ODA	= *Overseas Development Assistance*
OECD	= *Organisation for Economic Co-operation and Development*
PRACTICE	= *Proactive Response Against Cyber-attacks Through International Collaborative Exchange*
SDF	= *Self Defense Forces*
SOMTC	= *Senior Officials Meeting on Transnational Crime*
TI	= Teknologi Informasi
UNODC	= *United Nations Office on Drugs and Crime*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan informasi yang demikian cepat, membawa dampak yang cukup besar dalam kehidupan manusia. Salah satunya adalah jaringan internet yang memungkinkan pertukaran informasi tanpa mengenal batas ruang dan waktu. Selain itu, adanya jaringan internet membuat setiap kegiatan manusia menjadi berkembang semakin cepat, juga membuat dunia menjadi saling berhubungan dan saling terkait. Tercatat lebih dari 360 juta pengguna internet pada akhir tahun 2000 di seluruh dunia dan terus mengalami peningkatan sekitar 741% sehingga menjadi lebih dari 3 miliar pengguna pada tahun 2014.[1]

Tidak bisa dipungkiri bahwa internet telah mengubah dunia. Internet telah memberikan banyak kemudahan dalam hidup manusia, seperti berkomunikasi, melakukan transaksi, mencari hiburan, memperoleh informasi dan masih banyak lagi manfaat-manfaat yang dirasakan oleh manusia. Namun demikian, pada perkembangannnya ternyata penggunaan internet tersebut juga memiliki sisi negatif. Hal itu, membuat internet berpotensi menimbulkan kejahatan di dalamnya. Kejahatan yang timbul sebagai dampak negatif dari perkembangan aplikasi internet ini sering disebut sebagai kejahatan dunia maya *(cyber crime)*. Kejahatan dunia maya atau *cyber crime* merupakan kejahatan yang sangat cepat pertumbuhannya. Semakin banyak tindak kejahatan kriminal yang memanfaatkan kecepatan, kemudahan dan sifat anonimitas internet yang tidak mengenal batas tersebut. Selain itu, kejahatan dunia maya juga menimbulkan kerusakan yang lebih besar terhadap masyarakat daripada kejahatan tradisional dan lebih sulit untuk diselidiki, karena pelaku kejahatan dunia maya dapat melakukan aksi kejahatan di lokasi yang berbeda dengan korbannya. Korban dari aksi kejahatan dunia maya mengalami kerugian baik material maupun non material.

[1]Internet World Stats. 2014. *World Internet Users and Population Stats*. Diakses dari http://www.internetworldstats.com/stats.htm. Diakses pada tanggal 6 Juli 2014.

Kejahatan dunia maya juga terjadi di Jepang sehingga Pemerintah Jepang melakukan upaya pada masa Pemerintahan Shinzo Abe dalam meningkatkan keamanan nasionalnya dari ancaman kejahatan dunia maya. Studi sebelumnya mengenai upaya Pemerintah Jepang dalam menghadapi ancaman kejahatan dunia maya sudah dilakukan oleh Profesor Takato Natsui dari fakultas hukum Universitas Meiji Jepang. Profesor Takato Natsui menulis jurnal tentang kejahatan dunia maya di Jepang pada tahun 2003.[2] Pada tulisan milik Takato Natsui, kejahatan dunia maya diteliti melalui sudut pandang hukum. Dalam jurnalnya, Takato Natsui menjelaskan tentang kejahatan dunia maya yang terjadi di Jepang pada tahun 1990-an sampai tahun 2000-an. Penelitian Profesor Takato tersebut lebih fokus pada undang-undang terkait kejahatan dunia maya dan pengaplikasiannya terhadap kasus-kasus kriminal dunia maya di Jepang pada masa itu. Sedangkan dalam karya ilmiah ini membahas tentang peningkatan keamanan nasional Jepang terhadap ancaman kejahatan dunia maya di bawah Perdana Menteri Shinzo Abe dan berbeda dengan studi yang dilakukan oleh Profesor Takato. Pemerintah Jepang melalui Perdana Menteri Shinzo Abe telah menyatakan bahwa Kabinet Perdana Menteri Shinzo Abe akan lebih berperan aktif dalam meningkatkan keamanan dunia maya, dan Shinzo Abe juga mengungkapkan kekhawatiran mengenai peningkatan kejahatan dunia maya internasional.[3]

Sejak kecanggihan kejahatan dunia maya menyerang perusahaan kontraktor terbesar di Jepang yaitu Mitsubishi Heavy Industries Ltd, keamanan dunia maya telah menjadi bagian penting dari agenda keamanan nasional negara itu. Perusahaan kontraktor Mitsubishi Heavy Industries Ltd pernah mengalami serangan dunia maya yang dipublikasikan pada bulan Agustus tahun 2011. Pada perusahaan tersebut ditemukan virus pada sistem komputer di 11 lokasi di seluruh

---

[2] Takato Natsui. 2003. *Cybercrime in Japan: Recent Cases, Legislations, Problems and Perspectives*. Diakses dari http://www.netsafe.org.nz/Doc_Library/netsafepapers_takatonatsui_japan.pdf. Diakses pada tanggal 21 Agustus 2014.

[3]Halo Jepang. 2014. *Kabinet Abe Tingkatkan Peran Tangani Kejahatan Dunia Maya*. Diakses dari http://www.halojepang.com/kabarutama/7837-kabinet. Diakses pada tanggal 5 Juli 2014.

negara Jepang. Sekitar 45 server dan 38 PC yang terinfeksi oleh setidaknya delapan jenis virus ketika karyawan tanpa sadar membuka email yang berisi *malware.*[4]

Kasus lain diberitakan oleh *The New York Times* bahwa serangan dunia maya juga terjadi terhadap JAXA (*Japan Aerospace Exploration Agency*) pada tahun 2012 di Jepang. Serangan tersebut diduga menyebabkan eksfiltrasi, yang berarti adanya rilis data yang tidak sah dari komputer atau jaringan terhadap informasi yang berkaitan dengan Epsilon dan prototipe roket berbahan bakar padat yang juga digunakan oleh militer. Hal itu menunjukkan bahwa serangan yang ditargetkan tersebut dimungkinkan merupakan bagian dari spionase dunia maya.

Spionase dunia maya adalah tindakan yang dilakukan untuk memperoleh data rahasia dari pemegang informasi (individu, kelompok dan pemerintah) yang bertujuan untuk mendapatkan keuntungan ekonomi, politik, maupun militer dengan menggunakan metode jaringan atau komputer. Salah satunya dengan cara menggunakan virus berbahaya seperti *trojan horse*[5] dan *spyware*.[6]

Serangan dunia maya yang terjadi di Jepang masih banyak dan rata-rata serangan tersebut ditujukan untuk lembaga-lembaga pemerintahan dan perusahaan-perusahaan Industri utama yang ada di Jepang. Hal itu membuktikan bahwa Jepang adalah "zona panas" dari perspektif keamanan informasi, dan merupakan target dari aksi spionase dunia maya. Kepentingan strategis negara ini dalam percaturan internasional dan kekayaan intelektual Industri yang dimiliki

---

[4] Paul Kalender Umezu. 2012. *Japan Takes Action Against Complex Cyber Threats*. Diakses dari http://www.defensenews.com/article/20121009/C4ISR01/310090010/Japan-Takes-Action-Against-Complex-Cyber-Threats. Diakses pada tanggal 6 Juli 2014.

[5] *Trojan horse* adalah salah satu dari beberapa jenis malware yang mungkin ditemukan di komputer 'korban' setelah adanya serangan virus. Trojan merupakan program jahat yang melakukan tindakan tanpa persetujuan pengguna. Tindakan tersebut dapat mencakup: penghapusan data, pemblokiran data, pemodifikasian data, penyalinan data, dan mengganggu kinerja komputer atau jaringan komputer. Untuk penjelasan lebih lengkap mengenai *trojan horse* dapat dilihat di http://www.pctools.com/security-news/what-is-a-trojan-virus/

[6] *Spyware* adalah jenis malware yang diinstal pada komputer tanpa sepengetahuan pemilik yang bertujuan untuk mengumpulkan informasi pribadi pemilik. *Spyware* sering tersembunyi dari pengguna untuk mengumpulkan informasi tentang interaksi internet, *keystrokes* (perekaman penekanan tombol keyboard), password, dan data berharga lainnya Untuk penjelasan lebih lengkap mengenai *spyware* dapat dilihat di http://www.pctools.com/security-news/what-is-spyware/

oleh Jepang menjadi alasan yang cukup masuk akal atas serangan dunia maya tersebut.

Serangan dunia maya yang menimpa Pemerintah Jepang yang semakin meningkat membuat Perdana Menteri Shinzo Abe mengadakan rapat tim ahli di kantor Perdana Menteri pada Mei 2014. Rapat tersebut membahas jaminan keamanan dunia maya yang merupakan tantangan sangat penting di lihat dari sudut pandang keamanan nasional dan manajemen krisis. Pemerintah Jepang berupaya menangani isu tersebut secara lebih agresif.[7]

Sudah terdapat empat Kementerian bertanggung jawab atas keamanan dunia maya seperti Badan Kepolisian Nasional atau *National Police Agency (NPA)* yang bekerja untuk meningkatkan perjuangannya melawan kejahatan dunia maya; Kementerian Ekonomi, Perdagangan dan Industri atau *Ministry of Economy, Trade, and Industry (METI)* yang mengambil inisiatif untuk kerjasama dalam hal berbagi informasi tentang keamanan dunia maya atau dikenal dengan *Cyber Security Information sharing Partnership Japan (J-CSIP)* dan berhubungan dengan infrastruktur. Selain itu, lembaga Pemerintah Jepang yang bertanggung jawab atas keamanan dunia maya adalah Departemen Dalam Negeri dan Komunikasi atau Ministry of Internal Affairs and Communications *(MIC).* Departemen tersebut bertanggung jawab untuk kebijakan komunikasi dan jaringan seperti keamanan *smartphone* dan Departemen Pertahanan bertanggung jawab atas keamanan berbagi informasi secara nasional.[8] Namun demikian, masih ada ancaman terbaru untuk keamanan dunia maya yang lebih besar, lebih maju dan lebih rumit dan itu membuat Jepang harus mengambil langkah-langkah lebih lanjut guna mengurangi ancaman dunia maya.

Kejahatan dunia maya yang dihadapi oleh Pemerintah Jepang telah membuktikan bahwa kejahatan dunia maya bukan hanya merupakan masalah

---

[7]Kabinet Abe Tingkatkan Peran Tangani Kejahatan Dunia Maya. 2014. Diakses dari http://www.halojepang.com/kabarutama/7837-kabinet. Diakses pada tanggal 6 Juli 2014.

[8] Yoko Nitta. *Japan's Approach Towards International Strategy on Cyber Security Cooperation.* Diakses dari http://lsgs.georgetown.edu/sites/lsgs/files/Japan_edited%20v2.pdf_for_printout.pdf. Diakses pada tanggal 6 Juli 2014.

kriminal semata. Namun, kejahatan dunia maya termasuk masalah keamanan yang dapat mengganggu stabilitas negara. Oleh karena itu, Pemerintah Jepang menempatkan isu kejahatan dunia maya sebagai suatu agenda penting yang harus segera ditanggapi dan diselesaikan dengan mengambil langkah-langkah, baik itu strategi nasional maupun kerjasama internasional.

Dari penjelasan di atas dapat dilihat adanya peningkatan respon dan upaya yang dilakukan oleh Pemerintah Jepang melalui Perdana Menteri Shinzo Abe untuk memerangi tindak kejahatan dunia maya dalam rangka mewujudkan keamanan nasional di Jepang. Hal tersebut menarik untuk diteliti. Terdapat relevansi dalam masalah kejahatan dunia maya yang menjadi suatu agenda keamanan dengan mata kuliah di dalam studi Hubungan Internasional, yaitu mata Studi Keamanan dan Strategi. Dengan alasan tersebut, maka skripsi ini mengambil judul : **"UPAYA PEMERINTAH SHINZO ABE DALAM MENINGKATKAN KEAMANAN NASIONAL JEPANG DARI ANCAMAN DUNIA MAYA"**

1.2 Ruang Lingkup Pembahasan

Dalam melakukan analisa pada studi hubungan Internasional, pembatasan ruang lingkup menjadi amat penting. Hal ini bertujuan untuk membatasi masalah agar pembahasan tidak berkembang luas maupun keluar dari pokok permasalahan. Ruang lingkup pembahasan terbagi dua yakni batasan materi dan batasan waktu.

1.2.1 Batasan Materi

Penulis membatasi pada upaya Pemerintah Jepang di masa Pemerintahan Shinzo Abe yang difokuskan pada permasalahan kejahatan dan keamanan dunia maya di Jepang. Batasan ini digunakan agar penelitian yang dilakukan dapat menjadi lebih fokus pada pokok permasalahan yang ada. Dalam karya ilmiah ini, penulis membahas tentang upaya Pemerintahan Shinzo Abe dalam meningkatkan keamanan dunia maya di Jepang. Pada pembahasannya, skripsi ini meliputi beberapa aspek, seperti gambaran umum kejahatan dunia maya, kerugian yang

disebabkan oleh serangan dunia maya, ancaman-ancaman kejahatan dunia maya yang mengancam keamanan nasional negara Jepang, dan upaya Pemerintah Shinzo Abe untuk meningkatkan keamanan dunia maya di Jepang.

1.2.2 Batasan Waktu

Penulis mengkaji upaya peningkatan keamanan nasional dari ancaman kejahatan dunia maya oleh Pemerintah Jepang dengan memberikan batasan waktu, yaitu dimulai sejak Shinzo Abe menjabat sebagai Perdana Menteri Jepang periode kedua tahun 2012 sampai sekarang yaitu tahun 2015. Walaupun penulis sudah menetapkan ruang lingkup pembahasan, namun tidak menutup kemungkinan bagi penulis untuk memasukkan berbagai variabel dan fenomena yang terjadi di luar lingkup pembahasan yang sudah ditetapkan. Hal ini dimaksudkan untuk menjelaskan permasalahan secara terperinci dan komprehensif, sehingga dengan demikian fenomena di luar pembahasan merupakan sebuah latar belakang dan penjelas bagi analisa yang dilakukan.

1.3 Rumusan Masalah

Rumusan permasalahan yang akan dikaji dalam karya ilmiah ini adalah:

"Bagaimana upaya Pemerintah Shinzo Abe dalam meningkatkan keamanan nasional Jepang dari ancaman kejahatan dunia maya?"

1.4 Tujuan Penelitian

Penulisan skripsi ini bertujuan untuk:

- Untuk memberi gambaran yang obyektif tentang kejahatan dunia maya di Jepang;
- Untuk memberi gambaran tentang ancaman-ancaman kejahatan dunia maya terhadap keamanan nasional di Jepang;
- Untuk mengetahui tentang upaya-upaya yang dilakukan Pemerintah Shinzo Abe dalam meningkatkan keamanan dunia maya di Jepang.

1.5 Landasan Konseptual

Dalam penulisan karya ilmiah diperlukan landasan pemikiran yang digunakan sebagai dasar dari arah penulisan. Landasan pemikiran bisa berupa teori maupun konsep. Teori membantu kita menjelaskan dan meramalkan fenomena politik dan dengan demikian juga membantu pembuatan keputusan praktis.[9] Secara lebih spesifik, *McCain* dan *Segal* mendefinisikan teori sebagai berikut:

> "Serangkaian *statement* yang saling berkaitan...(yang terdiri dari):
> 1)Kalimat-kalimat yang memperkenalkan istilah-istilah yang mengacu pada konsep-konsep dasar teori itu; 2) kalimat-kalimat yang menghubungkan konsep-konsep dasar satu sama lain; 3) kalimat-kalimat yang menghubungkan beberapa *statement* teoritik itu dengan sekumpulan kemungkinan obyek pengamatan empirik (yaitu argumen utama)".[10]

Sedangkan konsep menurut Mochtar Mas'oed adalah abstraksi yang mewakili suatu objek, sifat suatu objek atau fenomena tertentu,[11] sehingga dapat menyerdehanakan apa yang menjadi permasalahan. Dalam skripsi ini, penulis membahas mengenai langkah-langkah Pemerintahan Shinzo Abe dalam meningkatkan keamanan dunia maya di Jepang. Oleh karena itu, penulis menganalisis dengan menggunakan konsep kejahatan dunia maya dan konsep keamanan non tradisional.

1.5.1 Konsep Kejahatan Dunia Maya *(Cyber Crime)*

Perkembangan teknologi dan komputer telah melahirkan jaringan internet yang memberi kemudahan bagi manusia untuk berkomunikasi dan mendapat informasi tanpa mengenal batas ruang dan waktu. Selain itu, internet bisa mempermudah kegiatan manusia, seperti melakukan kegiatan bisnis, belanja, dan berinteraksi melalui dunia maya. Namun, seiring dengan berbagai manfaat yang telah dirasakan manusia internet pun telah melahirkan berbagai aksi-aksi negatif

---

[9] Mochtar Mas'oed. 1990. *Ilmu Hubungan Internasional*. Jakarta: LP3ES. Hlm. 186.
[10] Ibid. hlm. 187.
[11] Mochtar Mas'oed. 1990. *Ilmu Hubungan Internasional: Disiplin dan Metodologi*. Jakarta: LP3ES. Hlm. 93-94.

melanggar hukum yang tidak pernah terpikirkan akan bisa terjadi. Kejahatan yang muncul sebagai dampak negatif dari perkembangan aplikasi internet ini sering disebut sebagai kejahatan dunia maya atau *cyber crime*.

Awalnya, kejahatan dunia maya dilakukan hanya oleh individu dan kelompok-kelompok kecil saja. Namun, seiring dengan perkembangan jaman, telah banyak organisasi kriminal besar yang secara profesional melakukan serangan dunia maya untuk membiayai kegiatan ilegal lainnya dari organisasi mereka. Jaringan kriminal dunia maya atau *cyber criminal*, pada saat ini, bahkan telah mampu menyatukan individu yang berada dalam organisasi yang sama namun ada di tempat yang berbeda-beda untuk melakukan aksi kejahatan dalam skala yang cukup besar.

Salah satu contoh jaringan kriminal yang juga bekerja melalui dunia maya adalah suatu geng dari Cina bernama Triad. Triad merupakan suatu perkumpulan para pelaku kriminal yang terkenal karena perdagangan senjata dan narkoba, penipuan kartu kredit, kejahatan dunia maya, pembajakan perangkat lunak *(software)*, dan penyelundupan manusia, hewan dan tumbuhan.[12] Triad terdiri dari kelompok-kelompok kecil yang bekerja secara independen dengan lebih dari 1,5 juta orang diperkirakan terlibat dalam kejahatan terorganisir di Cina.[13]

Secara sederhana, kejahatan dunia maya atau *cyber crime* merupakan tindak pidana kriminal yang terjadi di dunia maya atau internet dengan menggunakan komputer sebagai media untuk melakukan aksi tersebut. Sangat sedikit instrumen hukum yang secara jelas menjabarkan tentang pengertian kejahatan dunia maya, salah satunya adalah menurut Departemen Keadilan di Amerika Serikat atau yang dikenal sebagai *U.S. Department of Justice* dalam Institusi Nasional Keadilan (*National Institute of Justice*). Dalam salah satu materinya yang membahas tentang kejahatan dunia maya, berjudul "*Computer Crime : Criminal Justice Resource Manual"* menjelaskan bahwa kejahatan dunia

[12] *Asia's most notorious gangs.* 2015. Diakses dari http://team-yellow.com/tag/yamaguchi-gumi/. Diakses pada tanggal 3 Maret 2015.
[13] Ibid.

maya atau kejahatan komputer adalah segala bentuk pelanggaran hukum pidana yang melibatkan dan memanfaatkan pengetahuan teknologi komputer untuk melancarkan aksi jahat, penyelidikan, atau penuntutan (protes) di dunia maya.[14]

Selain itu, sangat sedikit negara-negara yang mengutip kata kejahatan dunia maya *(cyber crime)* dalam perundang-undangan nasional mereka. Undang-undang tersebut lebih sering menggunakan kata kejahatan komputer *(computer crime)* dalam *Malaysia, Computer Crimes Act 1997* dan *Sri Lanka, Computer Crime Act 2007*; komunikasi elektronik *(electronic communications)* dalam *Albania, Electronic Communications in the Republic of Albania, Law no.* 9918 2008 dan *Tonga Communications Act 2000*; teknologi informasi *(information technologies)* dalam *India, The Information Technology Act 2000* dan *Saudi Arabia, IT Criminal Act 2007*; atau kejahatan berteknologi tinggi *(high-tech crime)* dalam *Serbia, Law on Organization and Competence of Government Authorities for Combating High-Tech Crime 2010*.[15] Namun, banyak bagian yang ada dalam perundang-undangan tersebut yang termasuk dalam konsep kejahatan dunia maya, seperti akses tidak sah ke sistem komputer *(unauthorized access to a computer system)*, atau gangguan sistem komputer atau data *(interference with a computer system or data).*[16]

Badan Kepolisian Internasional atau *International Criminal Police Organization (Interpol)* juga memberikan gambaran mengenai kejahatan dunia maya. Kejahatan dunia maya merupakan kejahatan yang berkembang dengan sangat pesat.[17] Semakin banyak pelaku kejahatan dunia maya yang memanfaatkan kecepatan, kemudahan dan anonimitas dari internet untuk melakukan beragam

---

[14] Donn B. Parker. 1989. *Computer Crime: Criminal Justice Resource Manual*. Diakses dari https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf. Diakses pada tanggal 16 Juli 2014.
[15] UNODC. 2013. *Comprehensive Study on Cybercrime*. Diakses dari http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Diakses pada tanggal 25 Februari 2015. Hlm. 12.
[16] Ibid.
[17] Interpol. *Cybercrime.* Diakses dari http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime. Diakses pada tanggal 5 Juli 2014.

kegiatan kriminal yang tidak mengenal batas, baik fisik maupun virtual.[18] Menurut Badan Kepolisian Internasional kejahatan-kejahatan dalam dunia maya terbagi menjadi tiga bidang, yaitu:[19]

1. Serangan terhadap perangkat keras dan perangkat lunak komputer, misalnya, *botnet*[20], *malware*[21] dan intrusi jaringan;
2. Kejahatan keuangan, seperti penipuan online, penetrasi layanan keuangan online dan *phishing*[22];
3. Pelecehan atau penyalahgunaan, terutama terhadap anak-anak dan remaja, dalam bentuk eksploitasi komersial seks atau yang disebut *sexploitation*[23].

Dari beberapa penjelasan diatas dapat disimpulkan bahwa kejahatan dunia maya juga dapat disebut kejahatan komputer atau kejahatan yang berhubungan dengan teknologi. Kejahatan dunia maya merupakan bentuk kejahatan pidana yang menggunakan media pengetahuan teknologi komputer untuk melakukan serangan di dunia maya berupa aksi jahat, penyelidikan, atau penuntutan (protes). Aksi kriminal dalam dunia maya ini telah berkembang pesat dengan

---

[18] Ibid.
[19] Interpol, *Cybercrime.* Diakses dari http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime. Diakses pada tanggal 5 Juli 2014.
[20] *Botnet* adalah suatu jaringan yang mendistribusikan perangkat lunak berbahaya. Program tersebut dapat bekerja kapan saja sesuai keinginan si pelaku yang tujuannya untuk mengganggu atapun merusak suatu jaringan atau sistem operasi komputer yang berpotensi melumpuhkan jaringan internet secara luas Untuk penjelasan lebih lengkap mengenai *botnet* dapat dilihat di http://us.norton.com/botnet/
[21] *Malware* adalah singkatan dari *malicious software* yang berarti perangkat lunak berbahaya. *Malware* adalah jenis perangkat lunak yang tidak diinginkan terinstal pada sistem komputer. Program *malware* menyebabkan adanya invasi komputer dan kerusakan (misalnya, mencuri password dan data atau menginfeksi komputer lain pada jaringan).Untuk penjelasan lebih lengkap mengenai *malware* dapat dilihat di http://www.pctools.com/security-news/what-is-malware/
[22] *Phishing* adalah metode penipuan email dimana pelaku mengirimkan email dalam upaya untuk mengumpulkan informasi pribadi dan keuangan dari penerima. Selain mencuri data pribadi dan keuangan, pelaku dapat menginfeksi komputer dengan virus. Kebanyakan orang mengasosiasikan *phishing* dengan pesan email yang menipu, atau menyerupai bank, perusahaan kartu kredit atau bisnis lain seperti Amazon dan eBay. Pesan ini terlihat otentik dan berusaha untuk mendapatkan korban untuk mengungkapkan informasi pribadi mereka. Untuk penjelasan lebih lengkap mengenai *phishing* dapat dilihat di http://computer.howstuffworks.com/phishing.htm
[23] *Sexploitation* atau eksploitasi seks secara komersial merupakan eksploitasi seks pidana dimana korbannya adalah anak-anak. Jaringan internet dapat digunakan untuk memfasilitasi akses, penyimpanan, perdagangan anak; untuk mendukung pertukaran informasi antara jaringan pedofilia; dan untuk membantu organisasi kegiatan ilegal seperti prostitusi anak. Kegiatan-kegiatan tersebut dapat dilakukan secara rahasia. Untuk penjelasan lebih lengkap mengenai *sexploitation* dapat dilihat di http://www.bcmj.org/article/commercial-sexual-exploitation-children-and-youth

memanfaatkan kecepatan, kenyamanan, dan anonimitas internet tanpa mengenal batas.

1.5.2 Konsep Keamanan Non Tradisional

Konsep keamanan telah bertransformasi oleh dua kejadian utama, akhir dari Perang Dingin dan serangan terorisme di Amerika Serikat tahun 2001.[24] Berakhirnya Perang Dingin telah membuka era baru dalam pemahaman tentang keamanan. Dalam studi Hubungan Internasional, kajian tentang konsep keamanan Internasional telah berlangsung sejak lama, apalagi sejak berakhirnya Perang Dingin. Berakhirnya Perang Dingin diwarnai dengan meredanya konflik antara Amerika Serikat dan Uni Soviet mengakibatkan berkurangnya perhatian akan ancaman militer sebagai sumber ancaman terhadap keamanan suatu negara. Namun di sisi lain, justru muncul berbagai ancaman keamanan baru yang tidak muncul dari entitas berupa negara bangsa (*nation-state*). Hal ini melahirkan kajian keamanan nontradisional. Ancaman dalam kajian keamanan nontradisional menurut Terry Terriff, *et al*. memiliki empat karakteristik umum. Pertama, sebagian besar bagian dari masalah ini tidak bersifat *state-centred*, tetapi lebih berdasarkan pada faktor atau aktor non negara. Kedua, ancaman keamanan tidak memiliki suatu wilayah geografis tertentu. Ketiga, ancaman tersebut tidak mampu diselesaikan hanya dengan mengandalkan kebijakan keamanan tradisional. Keempat, sasaran ancaman adalah individu dan negara.[25]

Ada kesepakatan umum diantara para analis konsep keamanan sebagai implikasi dari akhir Perang Dingin terhadap bidang kajian konsep keamanan, yaitu :

1. Peran dari kekuatan militer diteliti kembali. Akhir dari Perang Dingin telah meningkatkan kerjasama multilateral sebagai alat dari tata negara yang baru. Bagi beberapa pihak hal ini berarti bahwa ancaman militer telah mengalami

[24] Craig A. Snyder. 2008. *Contemporary Security and Strategy*. New York: Palgrave Macmillan. Hlm. 1.
[25] Terry Terriff, et.al. 1999. *Security Studies Today.* Cambridge: Polity Press. Hlm. 115-116

penurunan, dan untuk beberapa pihak yang lain alat militer menjadi tidak berguna

2. Keharusan untuk meneliti kembali cara kita berpikir tentang konsep keamanan. Bagi beberapa pihak, hal ini merupakan hasil dari perubahan fundamental lingkungan pasca Perang Dingin, dan untuk beberapa pihak yang lain adalah kegagalan kajian strategis untuk memprediksi akhir dari Perang Dingin.
3. Keharusan untuk memperluas tentang arti keamanan *(security)*. Bagi beberapa pihak memperluas definisi dengan memasukkan efek dari isu-isu domestik pada agenda keamanan nasional suatu negara, dan untuk beberapa pihak yang lain hal itu berarti menangani ancaman non-militer harus sebaik menangani ancaman militer.[26]

Konsep isu keamanan non tradisional muncul pasca Perang Dingin. Konsep tersebut menekankan bahwa keamanan hendaknya juga dipandang dari sisi lain. Sisi individu, manusia atau warga negara juga dipandang sebagai obyek keamanan. Ancaman tidak hanya berasal dari negara namun juga dari aktor-aktor non negara lainnya. Isu keamanan harus mencakup berbagai dimensi lainnya. Artinya perubahan dalam kajian keamanan ini juga harus mencerminkan adanya permasalahan kemanusiaan.[27] Oleh karena itu, ada perluasan bidang keamanan disamping keamanan militer.

Aspek-aspek selain aspek militer yang menjadi ancaman keamanan termasuk objek ancaman non militer. Ancaman non militer memiliki karakteristik yang berbeda dengan ancaman militer, yaitu tidak bersifat fisik serta bentuknya tidak terlihat seperti ancaman militer. Adapun ancaman-ancaman yang berasal dari militer maupun non militer[28], yaitu:

---

[26] Craig A. Snyder. *Op.cit*. Hlm. 7.
[27] Landry Haryo Subianto. 2002. Konsep Human Security: Tinjauan dan Prospek. *Analisis CSIS vol. 31 no. 1*. Jakarta: CSIS. Hlm. 104.
[28] T. May Rudy. 2002. *Studi Strategis dalam Transformasi Sistem Internasional Pasca Perang Dingin*. Bandung: Refika Aditama. Hlm.33-35.

1. Militer

   Ancaman militer telah menjadi hal yang paling menakutkan dalam sejarah sebuah bangsa. Tidak hanya unsur-unsur vital yang akan hancur, namun pula unsur-unsur ekosistem serta unsur kehidupan sosial politik akan mengalami akibat yang lebih fatal. Pencegahan ancaman militer sampai saat ini masih merupakan prioritas setiap negara, mengingat tentu saja mereka tidak ingin apa-apa yang telah di raih rakyatnya dalam bidang seni budaya, industri, teknologi dan seluruh aktivitas yang telah ditekuni, musnah karena peperangan. Tingkat ancaman militer terhadap suatu negara bervariasi, tergantung dari apa yang menyebabkan terjadinya konflik tersebut. Hal tersebut mulai dari pelanggaran batas territorial, hukuman, perebutan batas territorial negara, invasi, sampai ancaman pembumi-hangusan sebuah negara dengan adanya *blockade* pengeboman. Tujuannya juga beragam, mulai dari persoalan minor seperti pelanggaran batas laut teritorial, sampai perbedaan paham yang dianut negara lain.

2. Politik

   Ancaman politik lebih mengarah kepada stabilitas organisasi pemerintah. Tujuannya bisa untuk menekan pemerintah yang berkuasa dalam kebijakan yang diambil, menggulingkan pemerintah, atau menciptakan intrik politik yang mampu mengganggu jalannya pemerintahan sehingga pula melemahkan kekuatan militernya. Ancaman politik merupakan ancaman umum yang terdapat di semua bangsa-bangsa di dunia tanpa melihat besar atau kecilnya suatu negara maupun kekuatan yang dimilikinya.

   Biasanya ancaman politik dari luar berkaitan erat dengan ideologi. Banyaknya paham ideologi yang masih dianut oleh rakyat sebuah negara, tentunya menyimpan bom waktu yang siap meledak setiap saat dan ancaman politik dari dalam negeri pun sama bahayanya dengan ancaman politik yang datang dari luar.

3. Sosial

   Perbedaan antara ancaman politik dan ancaman sosial yang dapat terjadi di sebuah negara sangat tipis. Ancaman sosial biasanya terjadi sebagai imbas dari

ancaman militer dan politik. Diskriminasi serta perbedaan tingkat sosial kehidupan merupakan faktor penting dalam terjadinya ancaman sosial dalam sebuah negara sebelum akhirnya menjadi ancaman politik di jajaran elit pemerintahan.

4. Ekonomi

Ancaman ekonomi merupakan ancaman yang paling sulit diatasi dalam kaitannya dengan keamanan nasional. Bukan saja hal ini dapat berarti kokoh atau tidaknya sebuah bangsa, namun keberhasilannya pun ditentukan oleh banyak faktor. Negara dalam hal ini hanya salah satu aktor yang berperan dalam perekonomian dunia. Kelemahan dalam bidang ekonomi dapat menjadi jalan bagi bangsa asing untuk mengontrol jalannya pemerintahan melalui bantuan ekonomi. Jika negara tersebut tidak mampu segera bangkit dari aspek struktural tersebut, maka keruntuhan sebuah negara tinggal menunggu waktu.

Hubungan antara ekonomi dan kemampuan kemiliteran saling berkaitan. Kemampuan kemiliteran suatu negara bukan hanya terletak pada persediaan dari strategi peralatan tetapi juga pada barang yang di hasilkan suatu industri yang mampu mendukung pasukan bersenjata. Untuk kekuatan utama, artinya sebuah perusahaan industry mampu menghasilkan beraneka macam senjata masa kini.

5. Lingkungan

Ancaman lingkungan bagi keamanan nasional ibarat ancaman militer dan ekonomi yang dapat menghancurkan bentuk dasar suatu negara. Secara tradisional, ancaman lingkungan bisa dilihat sebagai ketidaksengajaan, bagian dari kehidupan kondisi alam, dan suatu persoalan dari pokok persoalan bagi agenda keamanan nasional.

Beberapa aspek *non* militer, seperti aspek politik, ekonomi, sosial, dan lingkungan dapat menjadi ancaman bagi suatu negara sama halnya seperti aspek militer. Namun, selain aspek-aspek tersebut terdapat suatu ancaman baru di jaman globalisasi seperti ancaman yang berasal dari teknologi dan dunia maya. Masalah teknologi dan dunia maya yang bersifat inheren sebagai sumber ketergantungan

individu, masyarakat bahkan negara juga dapat menjadi ancaman bagi keamanan negara.

Kejahatan dunia maya telah menjadi fokus keamanan suatu negara sebagaimana dibuktikan oleh pembentukan beberapa institusi yaitu Komisi Perlindungan Infrastruktur Penting *(the Commission on Critical Infrastructure Protection)* yang dibentuk oleh Presiden Clinton pada tahun 1996, formulasi strategi Presiden Bush untuk melindungi dunia maya *(the National Strategy to Secure Cyberspace)* pada tahun 2003, pembentukan pusat pertahanan dunia maya di Estonia yang didukung oleh NATO pada tahun 2008,[29] dan yang terbaru adalah pembentukan lembaga-lembaga yang berwenang untuk menjaga keamanan dunia maya dan informasi di Jepang.

Penulis juga mengutip dokumen yang dikeluarkan oleh Dewan Kebijakan Keamanan Informasi Jepang yang bertujuan untuk mengamankan dunia maya, sebagai berikut:

> ”Perubahan lingkungan keamanan informasi yang sangat cepat, resiko menjadi semakin serius, lebih menyebar dan lebih mengglobal. Serangan dunia maya terhadap lembaga pemerintah dan infrastruktur penting menjadi kenyataan dan termasuk isu keamanan nasional dan isu-isu manajemen krisis. Saat ini, pengenalan langkah-langkah terbaik untuk melindungi lembaga-lembaga pemerintah dan infrastruktur penting telah menjadi penting *(the information security environment changes extremely quickl, risks have become increasingly serious, more diffuse and more globalized. 'Cyber attacks' against government institutions and critical infrastructures have become a reality and have become both 'national security' and 'crisis management' issues. At present, the introduction of the best possible measures for protecting the government institutions and critical infrastructures has become essential)".*[30]

Dari isi dokumen dapat disimpulkan bahwa lingkungan keamanan informasi yang telah berubah mampu menyebabkan gangguan bagi infrastruktur,

---

[29]Lene Hansen and Helen Nissenbaum. 2009. *Digital Disaster, Cyber Security, and the Copenhagen School*. Diakses dari www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf. Diakses pada tanggal 9 Agustus 2014.

[30] Informastion Security Policy Council. 2013. *Cybersecurity Strategy*. Diakses dari www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf. Diakses pada tanggal 21 Juli 2014.

ekonomi, atau keamanan nasional Jepang. Jadi tidak masuk akal untuk membedakan masalah keamanan dunia maya dengan masalah keamanan lainnya. Selanjutnya, Yould berasumsi bahwa teknologi informasi mungkin menjadi dasar umum dimana semua sektor keamanan bertemu *(it appears that IT may be the common underlying factor upon which all security sectors are destined to converge)*[31].

Respon yang diberikan oleh pemerintah suatu negara, organisasi regional maupun Internasional terhadap kejahatan dunia maya, dapat disimpulkan bahwa dunia maya merupakan media penting dimana sebagian besar aktivitas manusia di dunia dilakukan melalui dunia maya. Jadi tantangan untuk memastikan keamanan dunia maya telah menjadi salah satu isu penting yang dihadapi masyarakat global dan menjadi agenda penting internasional.

1.5.3 Konsep Kerjasama Internasional

Kerjasama internasional adalah kerjasama yang dilakukan oleh dua negara atau lebih untuk mencapai tujuan-tujuan tertentu yang berlandaskan kepentingan nasional. Negara-negara yang melakukan kerjasama internasional mempunyai tujuan bersama atau kepentingan bersama, karena ketidakberadaan kepentingan bersama di dalam kerjasama merupakan sesuatu hal yang mustahil.[32]

Selain itu, negara-negara berusaha untuk memecahkan dua tipe dasar masalah sosial, ekonomi, dan politik melalui kerjasama internasional.[33] Tipe yang pertama menyangkut kondisi-kondisi di lingkungan internasional yang apabila tidak diatur akan mengancam negara-negara yang terlibat. Sedangkan tipe yang kedua mencakup keadaan sosial, ekonomi, dan politik domestik tertentu yang

---

[31] Rachel E. Yould. 2003. *Beyond the American Fortress: Understanding Homeland Security in the Information Age. In Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, edited by Robert Latham. New York: The New Press. Hlm. 78.

[32] Robert O Keohane. 1989. *Neoliberal institutionalsm: a Perspektif in World Politics, in Internasional Institutions and State Power.* Boulder: Westview Press. Hlm. 3.

[33] William D. Coplin. 2003. *Pengantar Politik Internasional: Suatu Telaah Teoritis*. Edisi Kedua (Terjemahan: Marsedes Marbun). Bandung: Sinar Baru. Hlm. 283.

dianggap membawa konsekuensi luas terhadap sistem internasional sehingga dipersepsi sebagai masalah internasional bersama.

Kehidupan negara-negara yang saling berjalin semakin erat membuat kerjasama internasional menjadi sarana utama untuk memecahkan masalah domestik maupun internasional. William D. Coplin menjelaskan bahwa terdapat dua asumsi yang menjadi motivasi terbentuknya kerjasama antarnegara. Asumsi pertama adalah orang sering mengira bahwa suatu masalah sama sekali tidak bisa diselesaikan jika tidak terjadi suatu bentuk kerjasama internasional.[34] Dalam skripsi ini Pemerintah Jepang melakukan suatu kerjasama dengan negara lain untuk mengatasi kejahatan yang dilakukan melalui dunia maya. Kejahatan tersebut merupakan suatu masalah yang tidak bisa diselesaikan sendiri karena bentuk kejahatan baru tersebut dapat terjadi lintas negara. Oleh karena itu, diperlukan suatu bentuk kerjasama internasional. Contoh mengenai kerjasama internasional bisa ditemukan dalam kerjasama internasional antara Pemerintah Jepang dan Amerika Serikat untuk meningkatkan keamanan nasional dari kejahatan dunia maya. Kerjasama tersebut memungkinkan kedua negara saling bertukar informasi mengenai ancaman serangan dunia maya terhadap keamanan nasional dua negara tersebut dan memperkuat aliansi antar dua negara tersebut khususnya mengenai dunia maya dan teknologi. Asumsi kedua yang merangsang perilaku kerjasama internasional adalah bahwa penyatuan sumber daya akan menghilangkan penggandaan usaha yang sia-sia serta meningkatkan efisiensi umum pelaksanaannya dalam bidang apapun, bahkan dalam bidang yang kompleks seperti kerjasama internasional.[35] Penyatuan sumber daya tersebut merupakan suatu stimulus utama bagi kerjasama internasional yang luas.

1.6 Argumen Utama

Argumen utama di dalam sebuah penelitian merupakan jawaban sementara yang kebenarannya perlu diuji secara empirik. Jadi argumen utama merupakan jawaban terhadap masalah penelitian yang secara teoritis dianggap paling

[34] Ibid. Hlm. 284.
[35] Ibid.

mungkin atau tinggi tingkat kebenarannya. Menurut *Lanberg*, argumen utama adalah suatu dalil atau perumusan perjanjian atau prinsip yang diterima tapi tanpa mempercayainya dan atas dasar itu perlu dites dan disesuaikan dengan kenyataan-kenyataan. Dari pendapat tersebut, maka dapat disimpulkan bahwa Argumen Utama adalah :

a. Sesuatu yang masih kurang dari sebuah kesimpulan
b. Sebuah kesimpulan yang belum final karena masih harus dibuktikan kebenarannya.
c. Jawaban duga yang dianggap besar kemungkinannya untuk menjadi jawaban benar.[36]

Menarik kaitan antara permasalahan dan konsep yang digunakan di atas, maka dapat diambil argumen utama sementara di dalam penelitian ini, yaitu:

Peningkatan ketergantungan masyarakat Jepang terhadap internet diiringi dengan meningkatnya kejahatan dunia maya di negara tersebut. Kejahatan dunia maya meningkat menjadi isu keamanan seiring dengan serangan yang menimpa perusahaan-perusahaan besar di Jepang dan institusi pemerintahan. Hal itu, dikhawatirkan akan mengganggu kestabilan negara itu karena serangan dunia maya yang terjadi di Jepang dapat menyebabkan gangguan bagi ekonomi, keamanan nasional, dan infrastruktur penting. Dalam pendekatannya Perdana Menteri Shinzo Abe melakukan langkah-langkah yang lebih mendalam dalam hal peningkatan keamanan dunia maya melalui pertahanan diri Pemerintah Jepang dari kejahatan dunia maya lintas batas dan lebih proaktif menjaga keamanan dunia maya internasional. Oleh karena itu, Pemerintah Shinzo Abe melakukan upaya untuk meningkatkan pertahanan diri guna melindungi keamanan nasional Jepang dari kejahatan dunia maya dengan cara:

1. Membentuk Strategi Keamanan Dunia Maya
2. Membentuk Unit Pertahanan Dunia Maya
3. Mengadakan kerjasama dengan negara-negara lain terkait keamanan dunia maya internasional.

---

[36] Bohar Soeharto. 1996. *Menyiapkan Penelitian dan Penulisan Karya Ilmiah.* Bandung: Tarsito. Hlm. 134-135.

1.7 Metode Penelitian

Dalam penelitian karya ilmiah, metode merupakan salah satu syarat untuk melakukan penelitian. Penerapan metode bermanfaat untuk mendapatkan kerangka berpikir dan data-data yang dibutuhkan dengan tujuan agar karya tulis menjadi ilmiah, sistem dan kronologis.

Agar suatu penelitian dapat terarah dan mendapatkan hasil yang optimal dan sesuai dengan apa yang diharapkan, maka diperlukan metode yang tepat.

Menurut The Liang Gie metodologi adalah sebagai berikut :

> "Cara atau langkah yang berulang kali sehingga menjadi pola untuk menggali pengetahuan tentang suatu gejala pada ujung awalnya. Ini merupakan cara atau langkah untuk mengumpulkan data-data,sedangkan pada ujung akhirnya untuk meluruskan kebenaran pernyataan yang disebut mengenai gejala tersebut".[37]

Metode yang digunakan dalam penulisan tentang karya tulis ilmiah ini ada dua kategori yaitu metode pengumpulan data dan metode analisa data.

1.7.1 Metode Pengumpulan Data

Penulis melakukan penelitian dengan menggunakan data-data sekunder yang berarti data-data pengamatan terhadap objek yang diteliti tidak diperoleh secara langsung, tetapi didapatkan melalui buku-buku terbitan, artikel atau buletin dan pemberitaan oleh media massa serta informasi-informasi yang ada di internet. Dengan demikian metode pengumpulan data yang dilakukan adalah metode penelitian perpustakaan atau *library research*.

Tempat-tempat yang menjadi sumber data dalam penelitian ini adalah :

1. Perpustakaan Pusat Universitas Jember
2. Perpustakaan FISIP Universitas Jember

---

[37] The Liang Gie. 1984. *Ilmu Politik: Suatu Pembahasan tentang Pengertian, Kedudukan dan Metodologi*. Yogyakarta: Gajah Mada university Press. Hlm. 81.

Sumber literatur yang digunakan berasal dari:

1. Internet
2. Buku
3. Jurnal

1.7.2 Metode Analisis Data

Penelitian harus mengunakan proses berpikir yang baik untuk mendapatkan hasil yang baik juga. Berpikir adalah suatu proses mencari korelasi di antara berbagai ilmu pengetahuan untuk mengorganisasikan dan mereorganisasikan sehingga dapat menginstruksikan yang terdapat dalam tataran tertentu dan nantinya dapat dikembangkan kembali.

Penulis menggunakan cara berpikir deduktif untuk menganalisis data yang bertujuan untuk menyederhanakan sehingga mudah ditafsirkan. Metode deduktif adalah metode yang digunakan untuk menganalisa sesuatu yang spesifik, yang dihasilkan dan unit eksplanasi yang lebih tinggi. Unit eksplanasi yang digunakan dalam penelitian ini adalah ancaman dunia maya yang terjadi di Jepang yang menjadi agenda keamanan sehingga diperlukan adanya respon yang intensif untuk menanggapi ancaman tersebut. Metode penelitian secara deduksi merupakan penelitian yang dilakukan berupa penerapan teori, berangkat dari teori yang sudah ada, yang selanjutnya menjadi pegangan untuk membuat argumen utama dan akhirnya akan diuji kebenarannya melalui observasi fakta empiris.[38]

Penulis juga menggunakan metode deskriptif dalam menganalisa data. Deskriptif adalah upaya untuk menjawab pertanyaan siapa, apa, di mana, kapan, atau berapa; jadi merupakan upaya melaporkan apa yang terjadi.[39] Berangkat dari konsep keamanan menurut perspektif keamanan non tradisional yang penulis gunakan, penulis mencoba membuat argumen utama tentang upaya yang dilakukan oleh Pemerintah Shinzo Abe dalam menanggulangi kejahatan dunia maya di Jepang, yang difungsikan sebagai acuan dalam analisa terhadap kasus yang telah ditetapkan.

---

[38] Mochtar Mas'oed. 1990. *Ilmu Hubungan Internasional, Disiplin dan Metodologi.* Jakarta: LP3ES. Hlm. 117.
[39] Ibid. hal. 68.

1.8 Sistematika Penulisan

Penulisan skripsi ini dibagi dalam lima bab yang diuraikan lagi lebih dalam, yaitu:

BAB I: PENDAHULUAN

Bab ini berisi tentang latar belakang masalah, ruang lingkup pembahasan, rumusan masalah, kerangka konseptual, argumen utama, metode penelitian, tujuan penelitian, dan sistematika penulisan.

BAB II: GAMBARAN UMUM KEJAHATAN DUNIA MAYA DI JEPANG

Bab ini berisi tentang gambaran umum kejahatan dunia maya yang terjadi di Jepang. Gambaran umum yang akan dijelaskan dalam bab ini adalah motif-motif dan tipe serangan dunia maya yang terjadi di Jepang. Selain itu, penyebaran pengguna internet di Jepang, kasus-kasus kejahatan dunia maya yang sering terjadi dan kerugian yang menimpa perusahaan dan organisasi di Jepang serta modus operandi yang dilakukan oleh pelaku kejahatan dunia maya di negara tersebut.

BAB III: ANCAMAN-ANCAMAN KEJAHATAN DUNIA MAYA TERHADAP KEAMANAN NASIONAL DI JEPANG

Bab 3 berisi tentang beberapa ancaman serangan dunia maya yang menimpa beberapa infrastruktur dari dimensi keamanan nasional di Jepang. Kejahatan dunia maya menjadi *referent objects* terkait dengan ancaman yang ditimbulkannya terhadap individu dan negara secara langsung dan mempengaruhi keamanan negara.

BAB IV: UPAYA PEMERINTAH SHINZO ABE DALAM MENINGKATKAN KEAMANAN NASIONAL JEPANG DARI ANCAMAN DUNIA MAYA

Bab ini berisi tentang langkah-langkah yang dilakukan oleh Pemerintahan Shinzo Abe dalam meningkatkan keamanan dunia maya yang terjadi di Jepang. Langkah-langkah yang akan dijabarkan pada bab 4 adalah upaya yang dilakukan Pemerintah Jepang dalam lingkup nasional dan internasional. Dalam lingkup internasional, Jepang melakukan kerjasama bilateral dan multilateral terkait keamanan dunia maya.

BAB V: KESIMPULAN

Bab ini berisi tentang kesimpulan dari permasalahan diatas.

BAB II

KEJAHATAN DUNIA MAYA DI JEPANG

Kejahatan dunia maya atau yang disebut dengan *cyber crime* merupakan segala bentuk pelanggaran hukum pidana yang terjadi di dunia maya dengan melibatkan dan memanfaatkan pengetahuan teknologi komputer untuk melancarkan aksi jahat, penyelidikan, atau penuntutan mereka.[40] Bab ini menjelaskan tentang beberapa hal yang terkait dengan kejahatan dunia maya yang terjadi di Jepang, beberapa kasus kejahatan dunia maya yang menimpa beberapa perusahaan besar dan instansi-instansi di Jepang, peningkatan dan motif aksi kejahatan dunia maya yang terjadi di Jepang, serta kerugian yang dialami akibat aksi kejahatan dalam dunia maya tersebut. Pada akhirnya, hal-hal tersebut di atas menjadi suatu pengantar alasan Pemerintah Jepang melalui Perdana Menteri Shinzo Abe melakukan upaya untuk lebih berperan aktif meningkatkan keamanan dunia maya.

2.1 Gambaran Umum Kejahatan Dunia Maya di Jepang

Komunikasi informasi telah menyediakan dasar bagi semua kegiatan di luar bidang teknologi, seperti ekonomi, sosial, ataupun budaya. Maka dari itu, dunia maya atau *cyber space* telah menjadi *platform* penting untuk mendukung pertumbuhan nasional. Sejak tahun 1970-an, elektronik pengolahan data dan sistem komputer telah diperkenalkan dalam area bisnis di Jepang.[41] Beberapa perusahaan swasta telah mulai menggunakan sistem jaringan yang berdiri sendiri atau sistem jaringan internal. Namun, di beberapa daerah penting sistem jaringan

[40] Donn B. Parker. 1989. *Computer Crime: Criminal Justice Resource Manual*. Diakses dari https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf. Diakses pada tanggal 21 Agustus 2014.

[41]Takato Natsui. 2003. *Cybercrimes in Japan: Recent Cases, Legislations, Problem and Perspectives*. Diakses dari www.netsafe.org.nz/Doc_Library/netsafepapers_takatonatsui_japan.pdf. Diakses pada tanggal 21 Agustus 2014. Hlm. 1.

eksternal pun telah dikembangkan dan diperkenalkan. Salah satu contoh dari sistem eksternal tersebut adalah sistem komputer bank yang terhubung satu sama lain dengan sistem jaringan untuk tujuan pengiriman uang elektronik atau transaksi elektronik lainnya. Seiring dengan perkembangan teknologi tersebut, kejahatan komputer atau kejahatan kerah putih[42] yang dilakukan dengan menggunakan sistem komputer mulai muncul.[43]

Jaringan internet di negara Jepang terus mengalami pertumbuhan sejak tahun 1995 dan telah digunakan dalam berbagai kegiatan untuk menghubungkan sistem komputer yang satu dengan yang lain.[44] Semakin tinggi ketergantungan Jepang terhadap teknologi informasi, serangan dunia maya pun menjadi semakin tinggi dan semakin kompleks serta jangkauan serangannya menjadi semakin luas. Insiden-insiden yang terjadi dalam dunia maya juga telah banyak melumpuhkan fungsi administratif dan sosial di dunia nyata.

Terdapat beberapa motivasi dibalik serangan yang terjadi di dunia maya berdasarkan skala dampak dan korban yang muncul akibat adanya aktivitas tersebut, yaitu aktivitas peretasan komputer[45] *(hacktivism)*, kejahatan dunia maya *(cyber crime)*, spionase dunia maya[46] *(cyber espionage)*, perang dunia maya[47]

---

[42] Kejahatan kerah putih merupakan kejahatan yang umumnya dilakukan di dunia bisnis atau birokrasi. Jenis kejahatan semacam itu diantaranya termasuk penggelapan, penipuan, atau korupsi. Untuk penjelasan lebih lengkap mengenai kejahatan kerah putih dapat dilihat di http://www.amazine.co/17137/apa-itu-penjahat-kerah-putih-definisi-kejahatan-kerah-putih/

[43] Takato Natsui. *Op. cit*. Hlm. 2.

[44] Ibid.

[45] *Hacktivism* adalah tindakan meretas, atau membobol sistem komputer, untuk tujuan politik atau sosial. Biasanya tindaka ini dilakukan dengan mengirim virus ke sistem komputer yang menjadi target. Untuk penjelasan lebih lengkap mengenai *hacktivism* dapat dilihat di http://searchsecurity.techtarget.com/definition/hacktivism

[46] Spionase dunia maya adalah suatu tindakan yang dilakukan untuk memperoleh data rahasia dari pemegang informasi (individu, kelompok dan pemerintah) yang bertujuan untuk mendapatkan keuntungan ekonomi, politik, maupun militer dengan menggunakan metode jaringan atau komputer. Salah satunya dengan cara menggunakan virus berbahaya seperti *Trojan horse* dan *spyware*. Untuk penjelasan lebih lengkap mengenai spionase dunia maya dapat dilihat di http://www.techopedia.com/definition/27159/digital-espionage

[47]*Cyber warfare* adalah suatu perang di dunia maya yang melibatkan tindakan oleh organisasi negara-negara atau internasional untuk menyerang dan mencoba untuk merusak sistem komputer negara lain melalui, misalnya, virus komputer atau serangan *denial-of-service*. Untuk penjelasan lebih lengkap mengenai *cyber warfare* dapat dilihat di http://searchsecurity.techtarget.com/definition/cyberwarfare

(cyber warfare).[48] Berdasarkan motif-motif dibalik penyerangan di dunia maya, serangan yang terjadi di negara Jepang beberapa waktu yang lalu sudah masuk dalam kategori spionase dunia maya. Dalam arti bahwa serangan yang dilakukan terhadap lembaga pemerintahan dan perusahaan di Jepang bertujuan untuk memperoleh data rahasia mereka demi keuntungan para pelaku kejahatan. Banyaknya serangan dunia maya yang menimpa perusahaan kontraktor besar dan lembaga Pemerintah Jepang mengindikasikan bahwa spionase dunia maya merupakan salah satu ancaman dunia maya terbesar di negara Jepang.[49] Hal itu menandakan adanya peningkatan era teknologi dimana setiap perangkat komputer memiliki komponen intelejen yang bisa dimanfaatkan.

Selain motif yang digunakan oleh para pelaku kejahatan dunia maya, ada 9 tipe serangan dunia maya yang terjadi di Jepang, yaitu orang dalam berbahaya *(malicious insiders)*[50], serangan berbasis web *(web-based attacks)*[51], virus, worm dan trojan *(viruses, worms*[52]*, trojan),* serangan *Denial of Service* (DoS)[53], botnets,

---

[48] Hackmageddon.com. 2013. *2013 Cyber Attacks Statistics*. Diakses dari http://hackmageddon.com/2013-cyber-attacks-statistics/. Diakses pada tanggal 21 Agustus 2014.

[49] Pierluigi Paganini. 2012. *Japan institutions victim of cyber espionage, is it cyber warfare?*. Diakses dari http://securityaffairs.co/wordpress/7678/hacking/japan-institutions-victim-of-cyber-espionage-is-it-cyber-warfare.html. Diakses pada tanggal 15 Desember 2014.

[50] Orang dalam berbahaya *(malicious insiders)* adalah bekas karyawan, kontraktor, atau mitra bisnis lainnya yang memiliki atau telah berwenang ke akses jaringan, sistem, atau data organisasi dan sengaja disalahgunakan dengan cara negatif yang mempengaruhi kerahasiaan, integritas, atau ketersediaan informasi organisasi atau sistem informasi. Untuk penjelasan lebih lengkap mengenai orang dalam berbahaya dapat dilihat di https://www.watchfulsoftware.com/en/news-events/blog/posts/what-is-a-malicious-insider

[51] Serangan berbasis web atau *(web-based attacks)* merupakan serangan yang biasanya melibatkan teknik yang mengarahkan browser ke situs berbahaya. Jenis serangan ini termasuk jenis yang paling umum dilaporkan oleh korban serangan dunia maya. Untuk penjelasan lebih lengkap mengenai serangan berbasis web dapat dilihat di http://www.cs.northwestern.edu/~ychen/classes/msit458-w10/WebBasedAttacks_Offense.ppt

[52] *Worms* sangat mirip dengan virus, dalam arti bahwa virus itu merupakan program komputer yang meniru salinan fungsional dari virus itu sendiri (melalui koneksi jaringan) dan seringkali, namun tidak selalu, mengandung beberapa fungsi yang akan mengganggu penggunaan normal dari komputer atau Program. Untuk penjelasan lebih lengkap mengenai *worms* dapat dilihat di http://www.kaspersky.co.uk/internet-security-center/threats/viruses-worms

[53] Sebuah serangan *denial-of-service* (DoS) adalah jenis serangan dimana penyerang *(hacker)* berupaya mencegah pengguna yang sah untuk mengakses layanan. Dalam serangan DoS, penyerang biasanya mengirimkan pesan yang berlebihan meminta jaringan atau server untuk mengotentikasi permintaan yang memiliki alamat kembali yang tidak valid. Untuk penjelasan lebih lengkap mengenai serangan *denial-of-service* (DoS) dapat dilihat di http://www.pctools.com/security-news/what-is-denial-of-service/

kode berbahaya *(malicious code)*[54], *malware*, *phishing*, dan perangkat yang dicuri *(stolen devices)*.[55] Lembaga Ponemon *(Ponemon Institute)*[56] melakukan suatu penelitian dan membuat diagram tentang tipe serangan dunia maya yang menimpa beberapa perusahaan di Jepang dengan menggunakan 31 sampel perusahaan yang bergerak di bidang yang berbeda-beda di seluruh Jepang. Hampir semua perusahaan yang menjadi sampel mengalami serangan berupa *malware*, yaitu sebesar 97% dan menggunakan virus,worm dan trojan sebesar 100%. Selain itu, tipe serangan kode berbahaya *(malicious code)* dan *phishing* juga membuat kerugian pada perusahaan yang menjadi sampel, yaitu lebih dari separuh jumlah sampel mendapat serangan berupa kode berbahaya *(malicious code)* sebesar 58% dan *phishing* sebesar 52%. Tipe serangan lain juga banyak menimpa perusahaan-perusahaan di Jepang meskipun tidak sebanyak yang sudah disebutkan sebelumnya. Tipe serangan botnet menyerang sebanyak 48% dari total perusahaan, serangan DoS sebesar 39%, dan serangan yang berbasis web sebesar 39%. Pencurian perangkat *(stolen devices)* dan pemanfaatan orang dalam yang berbahaya *(malicious insiders)* juga menjadi cara untuk mengambil keuntungan dari perusahaan-perusahaan sampel, yaitu sebanyak 29% perusahaan mendapat serangan berupa perangkat yang dicuri *(stolen device)* dan pemanfaatan orang dalam berbahaya *(malicious insiders)* sebanyak 26% dari total jumlah perusahaan sampel.

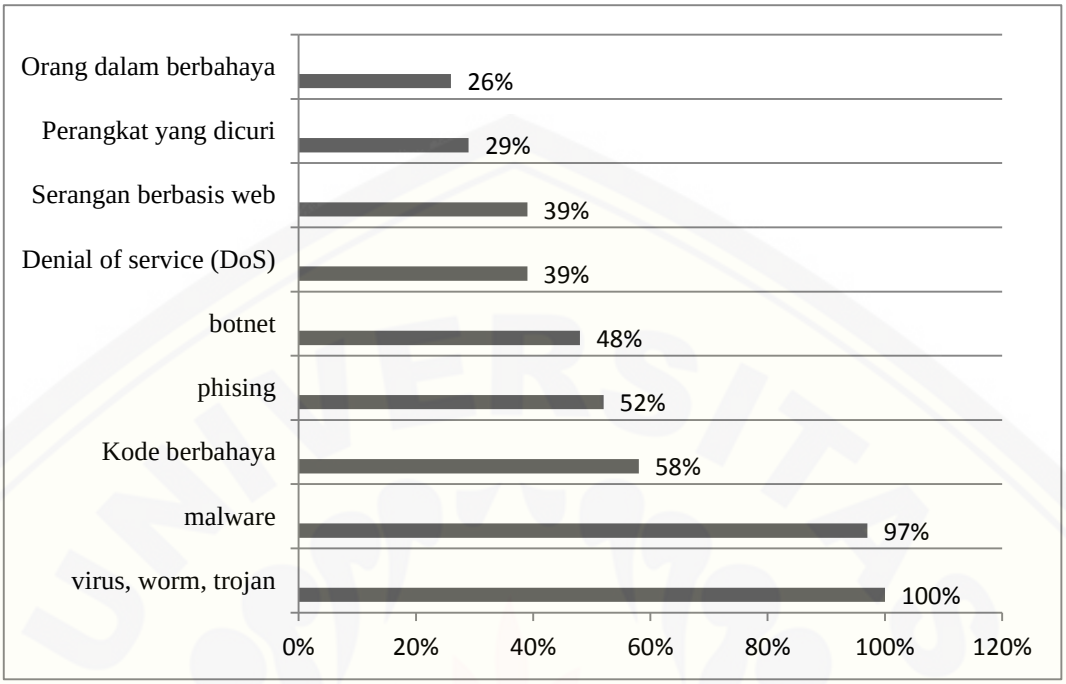
---

[54]Kode berbahaya *(malicious code)* adalah kode komputer yang menyebabkan pelanggaran keamanan untuk merusak sistem komputer. Serangan ini adalah jenis ancaman yang mungkin tidak bisa diblokir oleh perangkat lunak antivirus yang ada di sistem komputer. Untuk penjelasan lebih lengkap mengenai kode berbahaya *(malicious code)* dapat dilihat di http://usa.kaspersky.com/internet-security-center/definitions/malicious-code

[55] Ponemon Institute. 2014. *2014 Cost of Cyber Crime Study: Japan*. Diakses dari http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA5-5213JPN. Diakses pada tanggal 15 Desember 2014. Hlm. 10.

[56]Lembaga Ponemon merupakan lembaga penelitian dan pendidikan independen yang berlokasi di Amerika Serikat dan merupakan anggota dari Dewan Organisasi Penelitian Survei Amerika *(Council of American Survey Research Organizations)*. Lembaga tersebut melakukan penelitian independen, perlindungan data dan kebijakan keamanan informasi. Tujuan mereka adalah untuk memberikan pemahaman yang lebih jelas pada organisasi baik sektor swasta maupun publik dalam hal persepsi dan potensi ancaman yang dapat mempengaruhi pengelolaan dan pengamanan informasi pribadi tentang individu atau organisasi yang bersangkutan.

Diagram 2.1 Tipe serangan dunia maya di negara Jepang



Sumber : Ponemon Institute, 2014, *2014 Cost of Cyber Crime Study: Japan*, diakses dari http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA5-5213JPN, diakses pada tanggal 15 Desember 2014. Hlm. 10.

Diagram di atas menunjukkan bahwa tipe serangan dunia maya yang paling sering terjadi di Jepang adalah dengan mengirim virus,*worm*, *trojan* dan *malware* untuk meretas sistem komputer calon korban. Tipe tersebut dilakukan dengan cara mengirimkan virus berbahaya ke dalam sistem komputer korban untuk mengacaukan sistem kerja komputer tersebut. Virus ini memungkinkan untuk mencuri data atau informasi rahasia yang ada di sistem komputer, baik berupa kekayaan intelektual maupun data pribadi pengguna. Dalam beberapa tahun terakhir penggunaan *malware* meningkat sebagai senjata di dunia maya.[57]

Motif-motif dan tipe-tipe serangan dunia maya yang sering terjadi di negara Jepang menentukan langkah-langkah keamanan yang akan diambil Pemerintah Jepang sebagai upaya untuk mengatasi kejahatan dunia maya yang semakin meningkat. Seperti yang telah dijelaskan sebelumnya, aksi spionase dunia maya yang terjadi di Jepang lebih banyak menggunakan *malware* sebagai

[57] Ponemon Institute. Loc. cit.

alat untuk mencuri informasi rahasia. Hal itu terjadi pada Pembangkit Listrik Tenaga Nuklir Monju *(Monju Nuclear Power Plant)*. Pada 2 Januari 2014 salah satu dari delapan komputer di ruang kontrol Pembangkit Listrik Tenaga Nuklir Monju telah disusupi oleh peretas.[58] Para ahli keamanan yang menyelidiki insiden tersebut menyimpulkan bahwa serangan tersebut adalah serangan berbasis malware. Kemungkinan infeksi bisa berupa pembaruan perangkat lunak pada mesin yang disusupi, dan juga terdapat kode berbahaya yang mencuri beberapa data dan mengirimnya ke server yang terletak di Korea Selatan.[59] Oleh karena itu, diperlukan adanya data-data berupa tipe-tipe serangan yang sering terjadi di Jepang untuk merumuskan langkah-langkah yang diperlukan oleh Pemerintah Jepang sebagai cara untuk memerangi kejahatan dunia maya.

2.2 Penyebaran Pengguna Internet *(Internet Users)* dalam Dunia Maya di Negara Jepang

Dunia maya dan jaringan internet memungkinkan masyarakat dunia khususnya masyarakat Jepang untuk memunculkan terobosan-terobosan baru di masa depan. Selain itu, teknologi informasi, jaringan komunikasi, dan beberapa sistem serupa dapat membawa ekspansi dan penetrasi di bidang dunia maya yang lebih besar. Oleh karena itu, dunia maya diharapkan dapat menembus skala dunia sebagai kekuatan untuk mendorong pertumbuhan nasional terutama mendorong pertumbuhan ekonomi dan membuat inovasi-inovasi baru, menyelesaikan masalah, dan untuk tujuan-tujuan lainnya.

Jepang memiliki tingkat populasi pengguna internet terbesar keempat di dunia setelah negara Cina, Amerika Serikat, dan India[60]. Laporan tersebut

[58]Pierluigi Paganini. 2014. *Malware based attack hit Japanese Monju Nuclear Power Plant*. Diakses dari http://securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html. Diakses pada tanggal 16 Desember 2014.
[59] Ibid.
[60] Internet Live Stats. 2014. *Internet Users by Country (2014)*. Diakses dari http://www.internetlivestats.com/internet-users-by-country/. Diakses pada tanggal 16 Desember 2014.

dikeluarkan oleh lembaga statistik yaitu Internet Live Stats.[61] Negara Cina merupakan negara dengan populasi internat terbanyak di dunia, yaitu sebesar 21,97% dari total pengguna internet di dunia, dan Amerika Serikat sebesar 9,58%. Sedangkan India menggantikan posisi Jepang sebagai pengguna internet terbesar ketiga di dunia[62] yaitu sebesar 8,33%, dan Jepang dengan populasi pengguna interner sebesar 3,74% dari populasi pengguna internet di dunia.

Tabel 2.1 Presentase Pengguna Internet di Dunia

Rank	Country	Internet Users	1 Year Growth %	1 Year User Growth	Total Country Population	1 Yr Population Change (%)	Penetration (% of Pop. with Internet)	Country's share of World Population	Country's share of World Internet Users
1	China	641,601,070	4%	24,021,070	1,393,783,836	0.59%	46.03%	19.24%	21.97%
2	United States	279,834,232	7%	17,754,869	322,583,006	0.79%	86.75%	4.45%	9.58%
3	India	243,198,922	14%	29,859,598	1,267,401,849	1.22%	19.19%	17.50%	8.33%
4	Japan	109,252,912	8%	7,668,535	126,999,808	-0.11%	86.03%	1.75%	3.74%

Sumber: Internet Live Stats. 2014. *Internet Users by Country (2014)*. Diakses dari http://www.internetlivestats.com/internet-users-by-country/. Diakses pada tanggal 16 Desember 2014.

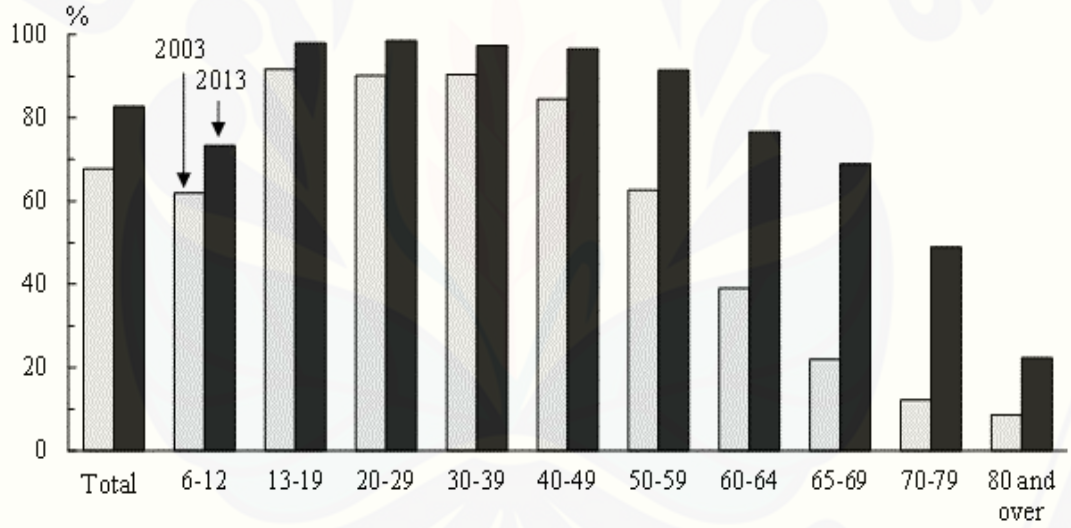
Sebagai negara dengan tingkat populasi pengguna internet yang cukup tinggi, Jepang menjadi salah satu negara yang memiliki infrastruktur teknologi informasi yang tinggi dan sangat mendukung penggunaan teknologi dalam berbagai aspek termasuk dalam bidang industri. Menurut laporan yang dikeluarkan oleh Pusat Evaluasi Teknologi Jepang atau yang disebut *Japanese Technology Evaluation Center* dalam jurnal yang berjudul *Electronic Manufacturing and Packaging in Japan*, asosiasi industri di Jepang sangat terlibat dalam pengembangan teknologi dan manajemen.[63] Banyak perusahaan besar yang

[61] Internet Live Stats adalah Lembaga statistik internet yang merupakan bagian dari proyek statistik dengan waktu yang riil (Worldometers dan 7 Billion World). Lembaga tersebut terdiri dari pengembang, peneliti, dan analis internasional dengan tujuan membuat suatu data statistik dengan menggunakan format waktu yang dinamis dan dapat dipakai oleh khalayak luas di seluruh dunia.
[62] Sreeja VN. 2013. *India Overtakes Japan As World's Third-Largest Internet User, Posts 31% Y-o-Y Growth.* Diakses dari http://www.ibtimes.com/india-overtakes-japan-worlds-third-largest-internet-user-posts-31-y-o-y-growth-1398037. Diakses pada tanggal 22 Januari 2015.
[63] Michael J. Kelly et al. 1995. *Electronic Manufacturing and Packaging in Japan*. Diakses dari www.wtec.org/loyola/pdf/ep.pdf. Diakses pada tanggal 16 Desember 2014. Hlm.36.

memainkan peran utama dalam teknologi industri di Jepang. Oleh karena itu, Pemerintah Jepang sangat mempunyai peran besar dalam medukung keamanan sistem informasi dan komunikasi.

Jumlah pengguna internet mengalami perkembangan yang cukup signifikan sejak awal penggunaan internet komersial tahun 1993.[64] Jumlah tersebut terus mengalami peningkatan terutama pada usia-usia produktif untuk memenuhi kegiatan sehari-hari mereka. Biro statistik Kementerian Urusan Dalam Negeri dan Komunikasi Jepang atau *The Statistics Bureau of the Ministry of Internal Affairs and Communications (MIC)*[65] melakukan survei terhadap jumlah pengguna internet sampai pada akhir tahun 2013.

Diagram 2.2 Kecenderungan Pemakaian Internet berdasarkan Kelompok Usia*



*Umur 6 tahun keatas

Sumber : Statistic Bureau MIC Japan. 2014. *Statistical Handbook of Japan 2014*. Diakses dari http://www.stat.go.jp/english/data/handbook/c0117.htm. Diakses pada tanggal 16 Desember 2014.

[64] Statistic Bureau MIC Japan. 2014. *Statistical Handbook of Japan 2014*. Diakses dari http://www.stat.go.jp/english/data/handbook/c0117.htm. Diakses pada tanggal 16 Desember 2014.
[65] Biro Statistik Kementerian Dalam Negeri dan Komunikasi (MIC) Jepang bertanggung jawab dalam hasil sensus fundamental dan survei statistik di wilayah Jepang.

Survei di halaman sebelumnya meliputi semua jenis perangkat koneksi internet yang digunakan, termasuk komputer pribadi, ponsel, tablet, dan terminal mesin-mesin permainan sebesar 100.440.000 orang atau sekitar 82,8% dari populasi penduduk yang berusia 6 tahun keatas.[66] Pemakaian internet tertinggi adalah kelompok yang berada pada usia produktif antara usia 13-59 tahun, yaitu lebih dari 90%. Sedangkan pada usia 60 sampai usia 80 keatas terjadi penurunan penggunaan internet yaitu dari sekitar 78% pada usia 60-64 tahun, 75% pada usia 65-69 tahum, 55% pada usia 70-79, dan sekitar 20% penduduk dengan usia 80 keatas.

Penggunaan internet oleh seluruh kelompok usia merupakan hal yang tidak dapat dihindari. Survei diatas menunjukkan tingginya tingkat penggunaan internet yang memungkinkan terjadinya kejahatan dunia maya. Oleh sebab itu, jaminan keamanan dunia maya di Jepang menjadi tugas yang sangat penting bagi pemerintah.

2.3 Kerugian dari Kejahatan Dunia Maya di Negara Jepang

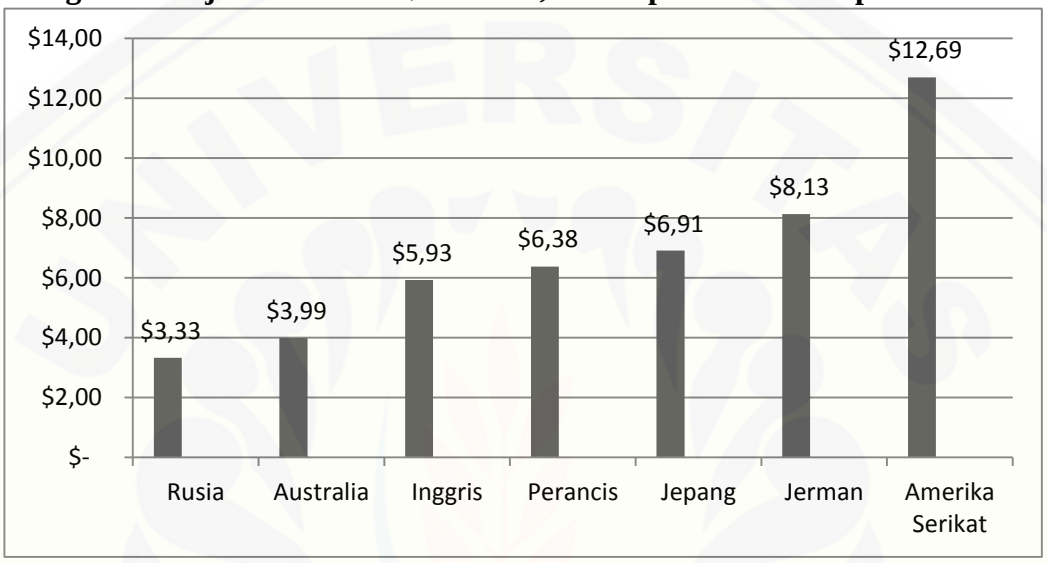
Kejahatan dunia maya membawa dampak negatif yang cukup besar bagi masyarakat Jepang, terutama terhadap perusahaan-perusahaan yang menjadi korban aksi tersebut. Dampak yang paling dirasakan oleh beberapa organisasi atau perusahaan tersebut adalah dampak ekonomi. Kejahatan dunia maya sangat merugikan bagi perusahaan dan organisasi.[67] Kerugian tersebut menyebabkan biaya setiap produktivitas hilang, ditambah dengan kemungkinan data hilang, dampak terhadap reputasi organisasi, dan biaya untuk membersihkan dan memulihkan dari serangan yang terjadi.[68] Subbab ini menjelaskan tentang dampak ekonomi yang terjadi akibat serangan dunia maya dan mengamati kecenderungan biaya (kerugian) pada tahun 2014. Dampak ekonomi yang dijelaskan dalam subbab ini akan dilengkapi oleh beberapa diagram yang diperoleh dari laporan penelitian oleh Lembaga Ponemon berjudul *2014 Cost of Cyber Crime*

[66] Statistic Bureau MIC Japan. *Op. cit*.
[67] Tony Bradley. 2014. *Your business can't afford the cost of cyber crime*. Diakses dari http://www.csoonline.com/article/2837805/malware-cybercrime/your-business-can-t-afford-the-cost-of-cyber-crime.html. Diakses pada tanggal 16 Desember 2014.
[68] Ibid.

Study:Japan. Studi yang dilakukan di negara Jepang pada tahun 2014 didasarkan pada sampel yang representatif dari 31 organisasi di berbagai sektor industri.[69] Subbab ini dimulai dengan penyajian diagram yang menunjukkan kerugian total dari serangan dunia maya yang terjadi di tujuh negara besar di dunia.

Diagram 2.3 Kerugian total dari kejahatan dunia maya di tujuh negara

Kerugian ditunjukkan dalam $1000.000, n=257 perusahaan terpisah



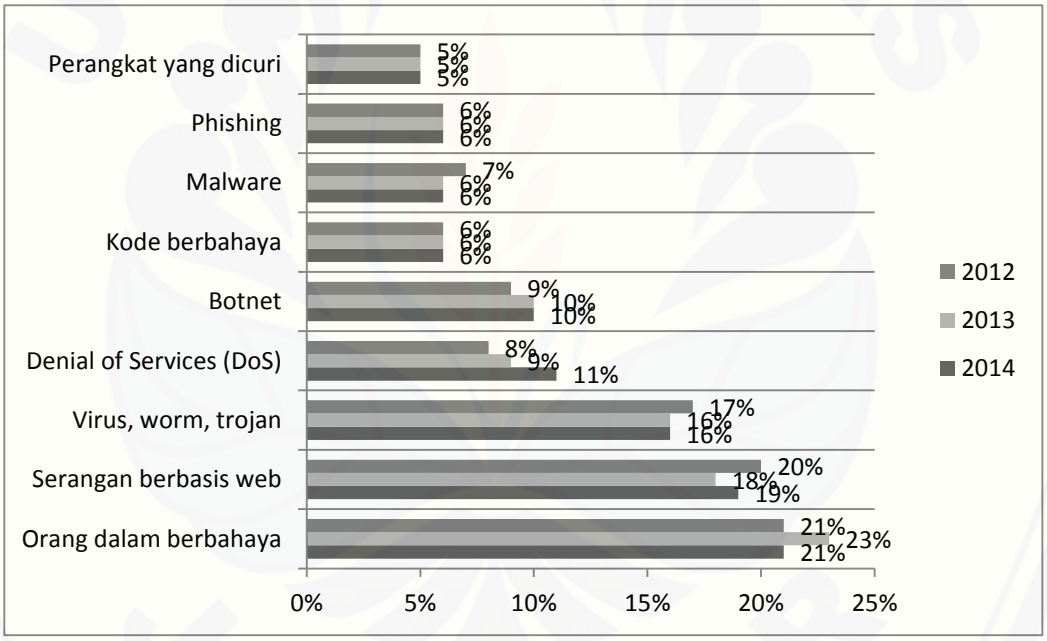
Sumber : Ponemon Institute. 2014. *2014 Cost of Cyber Crime Study: Japan*. Diakses dari http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA5-5213JPN. Diakses pada tanggal 15 Desember 2014. Hlm. 2.

Diagram di atas menunjukkan perkiraan rata-rata kerugian tahunan yang terjadi di tujuh negara akibat kejahatan dunia maya dari tahun 2012 sampai 2014. Tujuh negara tersebut merupakan contoh beberapa negara dengan jaringan teknologi informasi yang tinggi namun diiringi dengan tingginya tingkat kejahatan dunia maya pula. Dalam diagram tersebut, negara yang paling banyak mengalami kerugian adalah Amerika Serikat yaitu sekitar 12.690.000 dollar. Sedangkan negara Jepang merupakan negara ketiga terbesar yang mengalami kerugian akibat kejahatan dunia maya tersebut yaitu sekitar 6.900.000 dollar.

[69] Ponemon Institute, *Op. cit*. hlm. 1.

Kerugian yang dialami oleh negara Jepang disebabkan oleh beberapa tipe serangan yang digunakan oleh para pelaku. Tipe-tipe tersebut telah dijelaskan dalam diagram 2, namun diagram di bawah akan menjelaskan tentang kerugian per tahun yang disebabkan oleh 9 tipe serangan dunia maya dari tahun 2012 sampai 2014 dikutip dari laporan riset Lembaga Ponemon. Kerugian tahunan yang disebabkan tipe tersebut bervariasi tergantung dari kesembilan tipe serangan yang ada. Diagram tersebut menunjukkan presentase kerugian tahunan akibat dari serangan dunia maya selama 3 tahun terhadap organisasi-organisasi yang dijadikan sebagai tolak ukur lembaga tersebut.

Diagram 2.4 Presentase kerugian tahunan akibat serangan dunia maya di negara Jepang berdasarkan tipe serangan

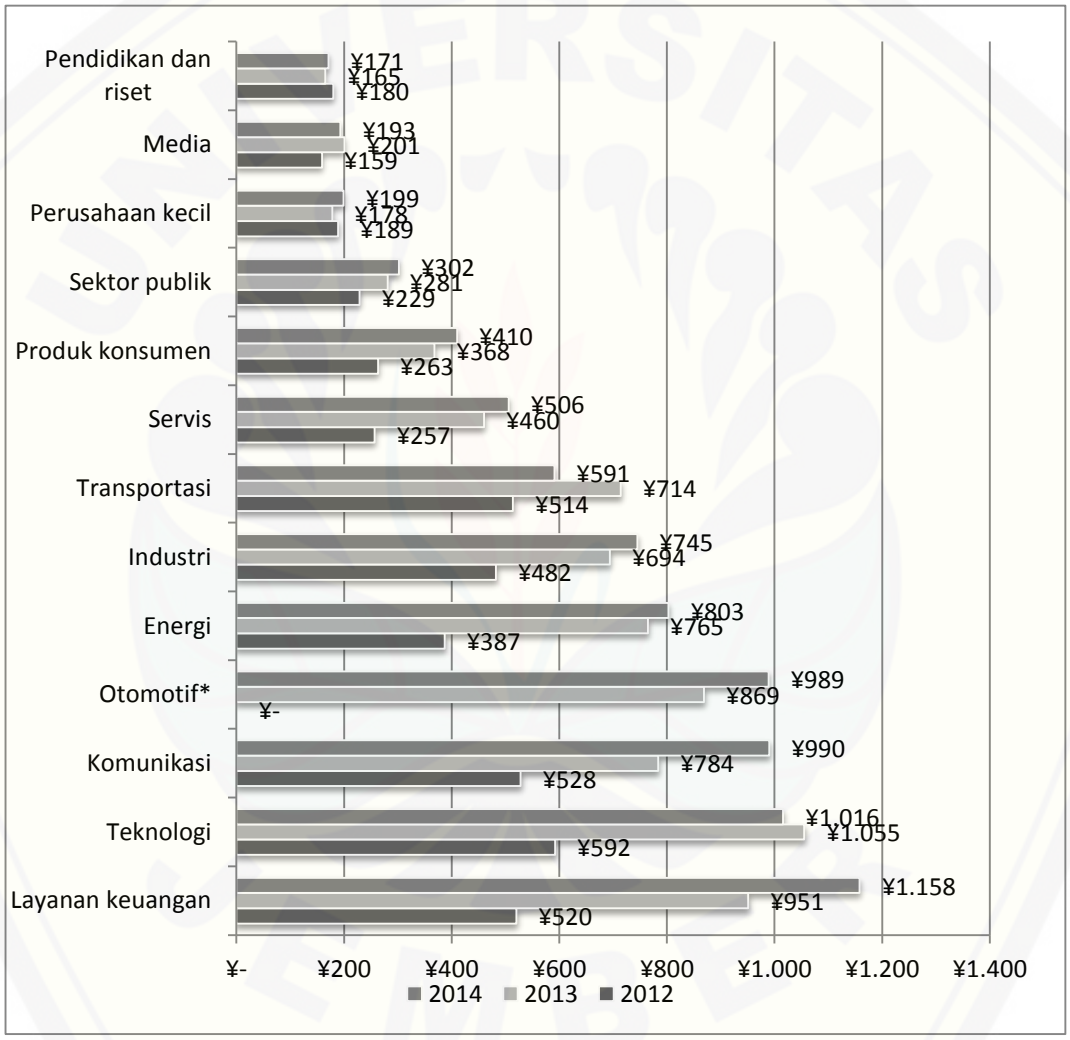


Sumber : Ponemon Institute. 2014. *2014 Cost of Cyber Crime Study: Japan*. Diakses dari http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA5-5213JPN. Diakses pada tanggal 15 Desember 2014. Hlm. 11.

Diagram di atas menunjukkan bahwa kerugian yang diakibatkan oleh berbagai tipe serangan tersebut sama tiap tahunnya. Hal itu dibuktikan dengan angka presentase yang hampir sama dari tahun 2012 sampai 2014. Tipe-tipe serangan yang menimbulkan kerugian paling besar pada perusahaan di Jepang

adalah orang dalam berbahaya *(malicious insiders)*, serangan berbasis web *(web-based attacks)*, dan penggunaan virus, worms, dan trojan. Ketiga tipe serangan tersebut menyebabkan kerugian terhadap perusahaan dan organisasi di Jepang lebih dari 55% tiap tahunnya dari keseluruhan total kerugian akibat dari kesembilan tipe serangan.

Diagram 2.5 Kerugian yang menimpa organisasi-organisasi di negara Jepang dalam satuan ¥1000.000



Sumber : Ponemon Institute. 2014. *2014 Cost of Cyber Crime Study: Japan*. Diakses dari http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA5-5213JPN. Diakses pada tanggal 15 Desember 2014. Hlm. 9.

Kerugian tahunan yang disebabkan oleh sembilan tipe serangan dari pelaku kejahatan dunia maya menimpa banyak organisasi dan perusahaan di

Jepang dari berbagai bidang. Tidak hanya layanan keuangan saja yang mendapat serangan dunia maya, namun lembaga seperti lembaga pendidikan dan riset pun juga mengalami kerugian akibat serangan di dunia maya. Kerugian tersebut dijabarkan melalui diagram yang masih tetap dikutip dari riset Lembaga Ponemon.

Kerugian yang dialami beberapa institusi dan perusahaan di Jepang mengalami kenaikan tiap tahun. Organisasi atau perusahaan yang paling bayak mengalami kerugian akibat serangan dunia maya adalah organisasi yang bergerak di bidang keuangan atau layanan keuangan online, bidang teknologi, dan bidang komunikasi. Selanjutnya diikuti oleh bidang otomotif, energi, industri, dan lain-lain. Diagram di halaman sebelumnya menunjukkan bahwa kerugian yang menimpa berbagai bidang di Jepang rata-rata mengalami kenaikan tiap tahunnya. Bidang yang mengalami kenaikan kerugian paling tajam adalah layanan keuangan, yaitu sebesar ¥520 juta pada tahun 2012 dan terus mengalami peningkatan menjadi ¥1.158 juta pada tahun 2014. Sedangkan bidang teknologi dan bidang komunikasi mengalami peningkatan kerugian lebih dari ¥400 juta dari tahun 2012 sampai tahun 2014. Bidang-bidang lain pun rata-rata mengalami peningkatan kerugian meskipun tak setajam bidang keuangan *online,* teknologi, dan komunikasi. Hal yang menarik adalah kerugian yang dialami oleh bidang otomotif. Pada tahun 2012, bidang tersebut masih belum menjadi korban atas serangan dunia maya, namun pada tahun 2013 bidang otomotif sudah mulai mengalami kerugian dan meningkat lebih dari ¥100 juta pada tahun 2014.

Bidang teknologi dan komunikasi serta keuangan online merupakan bidang yang bersangkutan langsung dengan internet dan dunia maya. Implikasinya, bidang-bidang tersebut sangat rentan dengan adanya serangan dunia maya. Namun, organisasi atau lembaga yang tidak bergerang di bidang ekonomi pun mengalami kerugian tahunan akibat serangan dunia maya, yaitu pendidikan dan riset meskipun nilai kerugian yang dialami tidak sebesar layanan keuangan.

2.4 Modus Operandi Kejahatan Dunia Maya *(Cyber Crime)* di Jepang

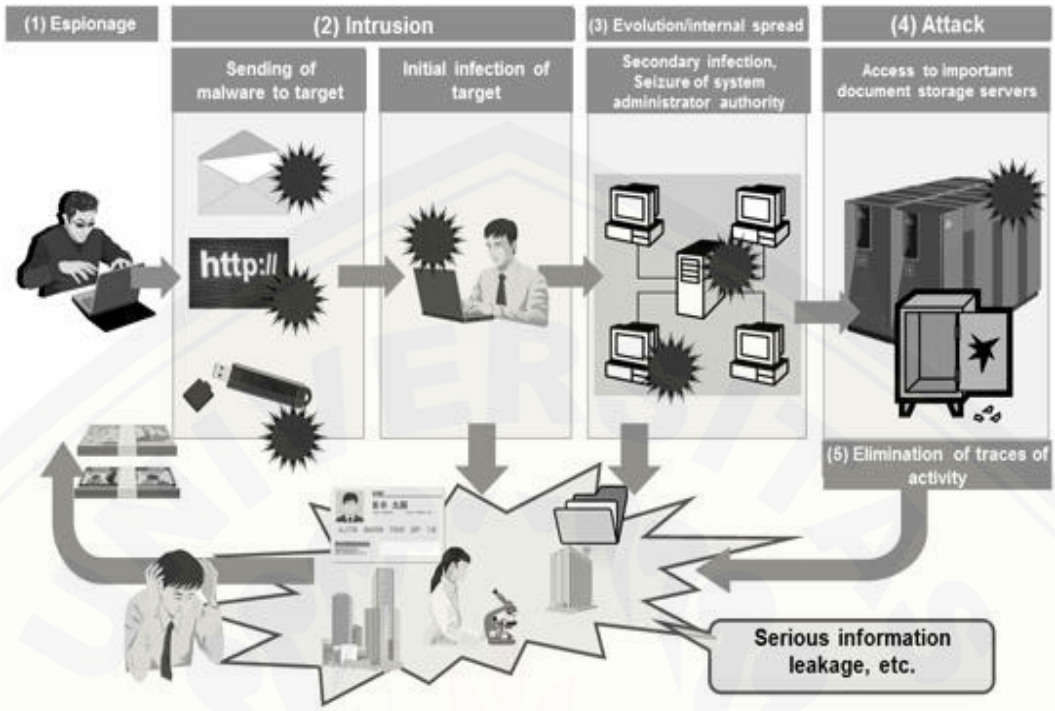
Pada umumnya kejahatan dunia maya dilakukan oleh individu atau kelompok-kelompok kecil. Namun, kelompok kejahatan terorganisir yang besar juga memanfaatkan internet. Penjahat profesional melakukan kejahatan lama mereka dengan cara baru yaitu melalui dunia maya dan membentuk komunitas kriminal global di dunia maya.[70] Komunitas kriminal tersebut berbagi strategi dan menggabungkan kekuatan untuk memulai serangan terkoordinasi. Mereka bahkan memiliki pasar bawah tanah di mana penjahat dunia maya dapat membeli dan menjual informasi dan identitas yang dicuri.[71] Serangan dunia maya yang ditujukan pada organisasi tertentu, layanan, dan individu untuk mendapatkan informasi pribadi, teknis, dan kelembagaan, dan aset intelektual lainnya untuk tujuan vandalisme atau keuntungan moneter.[72]

Metode yang paling sering dilakukan dalam serangan dunia maya adalah dengan cara mengirimkan virus atau program berbahaya kepada komputer target. Metode ini pada umunya dilakukan melalui 5 tahap, yaitu spionase *(espionage)*, penyusupan *(intrusion)*, penyebaran internal *(internal spread)*, penyerangan *(attack)*, dan yang terakhir penghapusan jejak aktivitas *(elimination of traces of activity)*. Tahap-tahap penyerangan dunia maya terhadap lembaga yang telah ditargetkan akan dijelaskan melalui gambar di halaman selanjutnya.

---

[70] Carnegie Cyber Academy. *How Cyber Criminals Operate*. Diakses dari http://www.carnegiecyberacademy.com/facultyPages/cyberCriminals/operate.html. Diakses pada tanggal 24 Februari 2015.
[71] Ibid.
[72] NEC. *Information Management*. Diakses dari http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html. Diakses pada tanggal 24 Februari 2015.

Gambar 2.1 Tahap-tahap Serangan Dunia Maya



Sumber : NEC. *Information Management.* Diakses dari http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html. Diakses pada tanggal 24 Februari 2015.

Gambar diatas menjelaskan bahwa serangan dunia maya yang telah ditargetkan terhadap lembaga tertentu adalah dengan cara memata-matai dan mengumpulkan informasi mengenai lembaga tersebut yang melibatkan penetrasi aktif ke lokasi dimana data penting tersebut disimpan. Selanjutnya pelaku melakukan aksi penyusupan dengan cara mengirimkan virus berbahaya *(malware)* ke komputer target. Virus tersebut menyebabkan adanya infeksi awal *(initial infection)* terhadap komputer target. Setelah virus berhasil masuk dan menyebar dari satu komputer ke komputer yang lain melalui jaringan internet, infeksi kedua *(secondary infection)* mulai terjadi. Dalam tahap ini, terjadi penyitaan otoritas sistem *(seizure of system administrator authority)* sehingga berhasil diretas *(hacked)* dan sistem dapat dikendalikan oleh pelaku serangan. Tahap selanjutnya adalah pelaku berhasil mengakses *server* yang menyimpan dokumen penting dari lembaga yang menjadi target. Pada akhirnya terjadi kebocoran informasi yang

serius. Namun, dalam kasus-kasus yang terjadi dengan hanya melalui 2 atau 3 tahap, para pelaku juga bisa menyebabkan kebocoran informasi. Tahap terakhir adalah pelaku melakukan penghapusan jejak aktivitas *(elimination of traces of activity)* sehingga jejak mereka tidak dapat dilacak.

Jepang menjadi salah satu target serangan kejahatan dunia maya adalah karena teknologi informasi dan jaringan internet telah menjadi dasar bagi semua kegiatan di luar bidang teknologi, seperti ekonomi, sosial, ataupun budaya. Dunia maya telah menjadi *platform* penting untuk mendukung pertumbuhan nasional negara Jepang. Semakin tinggi ketergantungan negara Jepang terhadap teknologi informasi, serangan dunia maya pun menjadi semakin tinggi dan semakin kompleks. Banyak perusahaan-perusahaan besar, organisasi dan lembaga Pemerintah Jepang yang menjadi korban akibat serangan dunia maya.

Dalam bidang ekonomi, kerugian yang timbul akibat dari serangan dunia maya cukup besar. Negara Jepang termasuk negara ketiga terbesar yang mengalami kerugian akibat serangan dunia maya setelah Amerika Serikat dan Jerman yaitu sekitar $6,91 juta. Serangan tersebut tersebut terbagi menjadi sembilan tipe serangan yaitu orang dalam berbahaya *(malicious insiders)*, serangan berbasis web *(web-based attacks)*, virus, Worm dan Trojan *(viruses, worms, trojan)*, serangan *Denial of Service* (DoS), botnets, kode berbahaya *(malicious code)*, *malware*, *phishing*, dan perangkat yang dicuri *(stolen devices)*. Dalam modus operandi yang dilakukan para pelaku kejahatan dunia maya, serangan dilakukan dengan cara mengirimkan virus atau program berbahaya kepada lembaga atau entitas yang menjadi target.

Sembilan tipe yang dijelaskan diatas menyebabkan kerugian yang bervariasi terhadap beberapa perusahaan dan organisasi di Jepang. Kerugian yang terus meningkat dari tahun ke tahun membuat Pemerintah Jepang harus mengambil langkah-langkah yang lebih proaktif dalam hal menjaga keamanan informasi dan memerangi kejahatan dunia maya khususnya pada masa Pemerintahan Shinzo Abe yang kedua

BAB III

ANCAMAN-ANCAMAN KEJAHATAN DUNIA MAYA TERHADAP KEAMANAN NASIONAL DI JEPANG

Perkembangan dunia teknologi informasi dan komunikasi yang sangat pesat saat ini merupakan tantangan bagi hampir semua negara di dunia termasuk Jepang. Hal tersebut tentunya juga memiliki implikasi besar terhadap penerapan pertahanan dan keamanan negara yang berbasis pada sistem teknologi informasi dan komunikasi. Selain itu, perkembangan dunia teknologi informasi dan komunikasi pun berhubungan dengan meningkatnya penggunaan internet pada hampir seluruh aspek kehidupan. Peningkatan penggunaan internet telah membawa dampak dan manfaat yang cukup besar, namun juga membawa resiko munculnya berbagai bentuk kejahatan yang memanfaatkan internet sebagai wadahnya. Masalah dunia maya sebagai sumber ketergantungan individu, masyarakat bahkan negara menjadi suatu ancaman bagi keamanan negara. Dengan demikian kejahatan dunia maya dapat menjadi *referent objects* terkait dengan ancaman yang ditimbulkannya terhadap individu dan negara secara langsung dan juga mempengaruhi keamanan negara. Target serangan dunia maya pun mengalami peningkatan. Korban yang muncul yang pada awalnya hanya pada lingkup individu dan rumah tangga telah meluas kepada lingkup infrastruktur sosial, perusahaan-perusahaan besar dan lembaga Pemerintahan Jepang. Pengaruh dari isu keamanan nasional terhadap ancaman dunia maya bagi situasi keamanan internasional adalah bisa menciptakan ketegangan antar negara-negara dan mengganggu stabilitas keamanan serta bisa mengganggu hubungan antar negara. Hal ini karena kejahatan dunia maya merupakan kejahatan yang melintasi batas negara. Bab 3 berisi tentang beberapa ancaman serangan dunia maya yang menimpa beberapa infrastruktur dari dimensi keamanan nasional di Jepang. Serangan tersebut berimplikasi pada terbentuknya beberapa kebijakan oleh Pemerintah Jepang.

3.1 Ancaman Dunia Maya terhadap Industri Pertahanan di Jepang

Ancaman Dunia Maya terhadap industri pertahanan yang pernah terjadi di Jepang berupa pencurian informasi rahasia yang dimiliki oleh perusahaan kontraktor Jepang yang bergerak di bidang pertahanan. Pencurian informasi dari kontraktor mungkin merupakan ancaman dengan peringkat paling serius terhadap keamanan nasional, dan hampir pasti membutuhkan tindakan pemerintah.[73] Selain itu ada berbagai motivasi yang digunakan oleh pelaku serangan dunia maya termasuk motif komersial. Tetapi hal tersebut juga mewakili efektifitas militer di masa depan terutama jika penyusup atau pelaku adalah musuh potensial atau bersedia untuk memberikan atau menjual informasi yang mereka curi.

Pada tahun 2011, dilaporkan telah terjadi serangan dunia maya terhadap Mitsubishi Heavy Industries Ltd. Perusahaan kontraktor pertahanan terbesar di Jepang ini mengatakan bahwa pada bulan Agustus tahun 2011 para peretas atau *hacker* telah memperoleh akses ke komputer dengan mengatakan pabrik kapal selam, rudal dan komponen pembangkit listrik tenaga nuklir yang telah menjadi targetnya.[74]

Mitsubishi Heavy Industries, Ltd. merupakan perusahaan industri raksasa di Jepang yang memproduksi pembuatan mesin untuk berbagai pasar, seperti pembangkit listrik tenaga nuklir, jembatan, dan mesin pesawat, kapal, dan pendingin udara untuk berbagai industri di seluruh dunia. Perusahaan industri raksasa tersebut beroperasi melalui enam segmen usaha, yaitu sistem daya, mesin dan struktur baja, ruang angkasa, mesin umum dan kendaraan khusus, pengembangan kapal dan samudera, dan lainnya. Perusahaan dan pasar utamanya terletak di Jepang, namun juga melakukan kerjasama dengan negara lain seperti di

---

[73] Ian Wallace. 2013. *The Military Role in National Cybersecurity Governance*. Diakses dari http://www.brookings.edu/research/opinions/2013/12/16-military-role-national-cybersecurity-governance-wallace. Diakses pada tanggal 25 April 2015.
[74] Rob Taylor. 2011. *Japan's Defense Industry Hit by its First Cyber Attack*. Diakses dari http://www.reuters.com/article/2011/09/19/us-mitsubishiheavy-computer-idUSTRE78I0EL20110919. Diakses pada tanggal 23 Agustus 2014.

Asia, India, Amerika Utara, Eropa, Amerika Tengah dan Selatan, Afrika, dan Timur Tengah.[75]

Pemerintah Jepang dan para investor utama perusahaan Mitsubishi Heavy Industries, Ltd. (MHI) pantas cemas dengan adanya kejadian peretasan sistem komputer perusahaan mereka. Sebuah artikel yang dimuat dalam website Reuters mengatakan bahwa perusahaan tersebut telah memenangkan 215 penawaran yang senilai dengan $ 3,4 Milyar dari Kementerian Pertahanan Jepang. Artikel tersebut juga menjelaskan bahwa:

> *"*Mitsubishi Heavy Industries adalah kontraktor pertahanan terbesar di negara Jepang yang telah memenangkan memenangkan 215 penawaran senilai ¥ 260 miliar dari Kementerian Pertahanan Jepang pada tahun hingga Maret lalu, atau hampir seperempat dari anggaran belanja kementerian tahun itu, yaitu 2011 *(it is the country's biggest defense contractor, winning 215 deals worth 260 billion yen ($3.4 billion) from Japan's Ministry of Defense in the year to last March, or nearly a quarter of the ministry's spending that year).*
> Senjata tersebut meliputi rudal *surface-to-air Patriot* dan rudal *AIM-7 Sparrow air-to-air (weapons included surface-to-air Patriot missiles and AIM-7 Sparrow air-to-air missiles).*
> Mitsubishi Heavy juga telah bekerja sama dengan Boeing, membuat sayap untuk 787 jet Dreamliner *(Mitsubishi Heavy has also been working closely with* Boeing*, making wings for its 787 Dreamliner jets).*"[76]

Seorang analis perang dunia maya *(cyber war)*, Andrew Davies, memberikan pernyataan kepada Reuters bahwa serangan peretasan dunia maya merupakan serangan pertama yang terdeteksi yang terjadi pada perusahaan besar di Jepang, dan pernah terjadi pada perusahaan-perusahaan pertahanan di Amerika Serikat. Pada sistem komputer perusahaan tersebut, ditemukan virus di 11 lokasi di seluruh Jepang. Sekitar 45 server dan 38 PC.[77] Ia mengatakan juga dalam artikel Reuters bahwa setidaknya ada delapan virus komputer termasuk *Trojan*

---

[75] Mitsubishi Heavy Industries, Ltd.
Global Network. Diakses dari http://www.mhi-global.com/network/. Diakses pada tanggal 23 Agustus 2014.
[76] Rob Taylor. *Loc. cit*.
[77] Paul Kallender Umezu. *Loc. cit*.

horse yang menginfeksi perangkat keras komputer perusahaan kontraktor pertahanan terbesar negara itu.

Serangan dunia maya yang menimpa perusahaan Mitsubishi Heavy Industries tersebut merupakan awal dari gelombang serangan peretasan berikutnya. Reuters juga melaporkan bahwa telah terjadi serangan peretasan di hari berikutnya pada perusahaan kontraktor militer Jepang, *(Ishikawajima-Harima Heavy Industries Co., Ltd.)* IHI Corp. dan Kawasaki Heavy Industries. Perusahaan kontraktor militer terbesar kedua di Jepang tersebut mengaku telah mendapat email yang berisi virus. IHI Corp merupakan perusahaan yang bergerak di bidang yang sama dengan MHI,Ltd., yaitu membagun bagian-bagian mesin untuk pesawat tempur, produsen pesawat, helikopter, dan sistem roket.

3.2 Ancaman Dunia Maya terhadap Lembaga Pemerintahan Jepang

Sistem komputer di Majelis Rendah Jepang telah menjadi korban serangan dunia maya dari server berbasis Cina.[78] Serangan dunia maya tersebut telah menyebabkan kebocoran data rahasia seperti identitas pengguna dan password. Password dan informasi lainnya mendapat serangan dunia maya telah dimulai ketika seorang staf Majelis Rendah membuka lampiran yang ada pada email pada bulan Juli 2011 namun pihak yang terkait tidak melaporkannya sampai akhir bulan Agustus.[79] Komputer di Majelis Rendah Jepang terinfeksi virus Trojan Horse berisi program yang memungkinkan server berbasis Cina tersebut untuk mencuri password dan informasi lainnya. Surat kabar Jepang bernama Yomiuri Shimbun menjelaskan bahwa virus tersebut telah menginfeksi komputer di sekitar 10 kedutaan dan konsulat.[80] Serangan dunia maya yang bertujuan mencuri kode identitas pengguna *(user ID)* dan password dari anggota majelis memungkinkan peretas dapat mengakses *e-mail* dan dokumen yang dimiliki mereka. Selain itu,

---

[78] *Japan parliament hit by China-based cyberattack*. 2011. Diakses dari http://www.spacewar.com/reports/Japan_parliament_hit_by_China-based_cyberattack_999.html. Diakses pada tanggal 23 Agustus 2014.
[79] Ibid.
[80] *China-based servers in Japan cyber attacks: report*. 2011. Diakses dari http://phys.org/news/2011-10-china-based-servers-japan-cyber.html. Diakses pada tanggal 15 Desember 2014.

Majelis Tinggi Jepang juga menjadi korban serangan dunia maya seperti yang terjadi pada Majelis Rendah dan mengakibatkan banyak email yang terinfeksi *malware* beredar di mesin pemerintah. Beberapa komputer dari sejumlah misi diplomatik Jepang ke negara-negara lain juga diduga menjadi target, menunjukkan bahwa adanya upaya besar-besaran untuk mencuri informasi yang berkaitan dengan operasi diplomatik Jepang. Apabila hal tersebut terus terjadi tanpa diadakan langkah-langkah pencegahan, informasi-informasi rahasia penting yang ada di Majelis Rendah dan Majelis Tinggi Jepang dapat dengan mudah dicuri oleh peretas *(hacker)* yang selama ini menggunakan server berbasis Cina. Hal itu juga bisa berdampak besar pada rahasia keamanan nasional Jepang.

Selain itu, badan legislatif Jepang juga pernah menjadi korban dari serangan dunia maya. Kelompok aktivis peretas atau *hacker* bernama *Anonymous* menanggapi terbentuknya RUU untuk merevisi hukum hak cipta bangsa oleh Badan Legislatif Jepang, yaitu adanya hukuman pidana bagi seseorang yang mendownload materi yang berhak cipta atau *back up* isi dari DVD. Hukum tersebut akan berlaku pada bulan Oktober tahun 2012. Majelis Tinggi Jepang menyetujui Rancangan Undang-Undang (RUU) tersebut dengan suara 221-12. Bagi pelanggar akan dikenakan hukuman 2 tahun penjara atau denda hingga 2 juta yen atau sekitar $ 25.000. Kelompok peretas tersebut mengancam akan melakukan tindakan lebih lanjut sebagai aksi protes atas hukuman baru tersebut yang berlaku dalam amandemen undang-undang hak cipta.[81] Setelah peluncuran protes oleh kelompok peretas tersebut, serangkaian serangan DdoS terjadi terhadap beberapa lembaga Pemerintah Jepang dalam menanggapi hukum hak cipta baru tersebut.[82] Implikasinya, serangan-serangan tersebut berpotensi mengganggu website-website yang ada di lembaga Pemerintah Jepang. Selain itu,

[81] Mohit Kumar. 2012. Anonymous Hacks Japanese Government Websites against Anti-Piracy Laws in Japan. Diakses dari http://thehackernews.com/2012/06/anonymous-hacks-japanese-government.html. Diakses pada tanggal 23 Agustus 2014.
[82]Steven. 2012. *Anonymous Tweets to Japanese Public After 6.27 Attacks, Japanese Public Responds: "Kawaii"*. Diakses dari http://en.rocketnews24.com/tag/opjapan/. Diakses pada tanggal 19 Februari 2015.

aksi protes tersebut dapat berpotensi terprovokasinya pihak-pihak lain untuk menolak RUU baru mengenai hak cipta tersebut.

3.3 Ancaman Dunia Maya terhadap Infrastruktur Nasional Penting Jepang

Sebuah sistem komputer di Badan Antariksa Jepang, JAXA *(Japan Aerospace Exploration Agency)* yang setara dengan US NASA *(National Aeronautics and Space Administration)* telah terinfeksi virus sehingga terjadi potensi kebocoran data dari badan HTV *(H-11 transfer vehicle)*, pada tanggal 16 Januari 2012.[83] Selanjutnya terjadi serangan lainnya terhadap Badan Antariksa Jepang tersebut pada November tahun 2012, yaitu informasi pada salah satu roket terbarunya dicuri dari komputer oleh seseorang menggunakan virus komputer. *The Japan Aerospace Exploration Agency* (JAXA) mengatakan bahwa virus komputer di perusahaan Tsukuba Space Center yang berada di timur laut dari Tokyo ditemukan secara rahasia mengumpulkan data dan mengirimkannya ke luar agensi tersebut. Data yang dicuri dari badan antariksa tersebut termasuk informasi tentang epsilon, sebuah roket berbahan bakar padat yang masih dalam pengembangan. Epsilon dimaksudkan untuk meluncurkan satelit dan *space probes* (pesawat ruang angkasa tak berawak yang meninggalkan orbit Bumi dan mengeksplorasi ruang), roket berbahan bakar padat sebesar itu juga dapat memiliki kegunaan militer sebagai rudal balistik antarbenua.[84] Program Epsilon yang menghabiskan dana ¥15 miliar untuk pengembangannya, dapat memajukan Jepang dalam ruang-eksplorasi dan industri satelit.[85] Selain itu, JAXA mengalami

---

[83]SPAMfighter News. 2012. *Virus Strikes Computer at Japan's Space Agency.* Diakses dari www.spamfighter.com/News-17323-Virus-Strikes-Computer-at-Japans-Space-Agency.htm. Diakses pada tanggal 23 Agustus 2014.

[84]Martin Fackler. 2012. *Japan's Space Agency Says Rocket Information Was Stolen by Computer Virus*. Diakses dari http://www.nytimes.com/2012/12/01/world/asia/japans-space-agency-says-rocket-information-was-stolen-by-computer-virus.html?_r=1&. Diakses pada tanggal 23 Agustus 2014.

[85] Iain Thomson. 2012. *Malware slurps rocket data from Japanese space agency: Secrets of Epsilon go out the door*. Diakses dari http://www.theregister.co.uk/2012/11/30/jaxa_data_loss/. Diakses pada tanggal 19 Februari 2015.

serangan dunia maya kedua pada 18 April 2013.[86] Para pelaku berusaha mengakses informasi referensi yang digunakan untuk persiapan operasi *Japanese Experiment Module (JEM)*, yang dikenal sebagai "Kibo" (diucapkan key-bow) berarti harapan (dalam bahasa Jepang). Kibo merupakan fasilitas laboratorium antariksa pertama Jepang dan kontribusi JAXA yang pertama untuk program Stasiun Antariksa Internasional *(International Space Station)*. Kibo dirancang dan dikembangkan dengan maksud untuk melakukan kegiatan penelitian ilmiah di orbit. Selain itu, pelaku serangan berusaha mengakses beberapa nomor dari daftar personel yang terkait dengan program Kibo. Keberhasilan Jepang dalam membuat roket berbahan bakar padat dan menciptakan suatu fasilitas ruang angkasa baru terganggu oleh adanya aktivitas peretasan. Apabila serangan peretasan tersebut terus-menerus terjadi, hal itu akan berpotensi hilangnya data penting terkait dengan program epsilon yang sedang dijalankan oleh Pemerintah Jepang dan juga dapat menyebabkan penyalahgunaan roket berbahan bakar padat tersebut sebagai senjata berbahaya, karena roket tersebut juga dapat digunakan dalam bidang militer sebagai rudal balistik. Selain itu, serangan tersebut dapat mengakibatkan menurunnya daya saing yang dimiliki oleh Pemerintah Jepang di bidang teknologi dan ruang angkasa karena data rahasia mengenai program epsilon dan program Kibo dapat diakses dan dicuri oleh pelaku serangan dunia maya sehingga para pelaku dapat melakukan aksi plagiat terhadap kedua program tersebut.

Pembangkit Listrik Tenaga Nuklir Jepang yang berlokasi di Monju juga menjadi target serangan dunia maya. Pada 2 Januari 2014 salah satu dari delapan komputer di ruang kontrol di Pembangkit Listrik Tenaga Nuklir Monju menjadi target peretas. Administrator IT telah menemukan bahwa sistem di ruang kontrol reaktor telah diakses lebih dari 30 kali oleh seorang peretas dalam lima hari terakhir setelah seorang karyawan memperbarui aplikasi gratis di salah satu mesin di pabrik. Informasi pertama yang ada mengenai insiden tersebut menegaskan

[86] JAXA. 2013. *Unauthorized Access of JAXA Server*. Diakses dari http://global.jaxa.jp/press/2013/04/20130423_security_e.html. Diakses pada tanggal 24 Februari 2015.

bahwa ada lebih dari 42.000 e-mail dan laporan pelatihan staf yang tersedia pada sistem pembangkit listrik tenaga nuklir tersebut. Insiden yang terjadi di Badan Energi Atom Jepang bukan peristiwa yang pertama kali, pada bulan November 2012 komputer di markas Badan Energi Atom Jepang atau *The Japan Atomic Energy Agency (JAEA)* di Tokaimura juga terinfeksi oleh *malware*. Badan yang bergerak di bidang energi tersebut telah menginformasikan bahwa pihaknya masih menyelidiki aksi penyerangan tersebut. Pembangkit listrik tenaga nuklir merupakan infrastruktur yang penting dan keamanan mereka adalah salah satu perhatian utama bagi setiap pemerintah. Pembangkit listrik tenaga nuklir adalah infrastruktur penting dan jaminan keamanan bagi infrastruktur tersebut adalah salah satu perhatian utama bagi pemerintah. Apabila tindakan penyerangan terhadap infrastruktur penting tersebut terus terjadi dan tidak dibuat langkah-langkah keamanan, maka berpotensi munculnya penyalahgunaan infrastruktur yang bersumber energi nuklir tersebut. Sebuah insiden serangan dunia maya ke fasilitas nuklir seperti serangan yang terjadi pada Pembangkit Listrik Tenaga Nuklir Monju bisa memiliki dampak lingkungan yang signifikan dan mempengaruhi ekosistem secara keseluruhan planet ini,[87] salah satunya adalah dampak radiasi dari nuklir yang berbahaya bagi masyarakat.

3.4 Ancaman Spionase Dunia Maya di Jepang

Serangan dunia maya yang terjadi di Jepang bukan hanya bermotif *hacktivism* atau kejahatan dunia maya semata, namun sudah masuk dalam spionase dunia maya karena aksi peretasan yang dilakukan bertujuan untuk mencuri informasi penting dari komputer korban. Apalagi korban dari kejahatan tersebut bukan dari *website-website* personal atau perusahaan biasa, namun menimpa instansi pemerintahan dan perusahaan besar di Jepang. Penasehat Strategi Teknologi Informasi untuk Kabinet Jepang, William Saito, menyatakan dalam artikel website Bloomberg bahwa spionase dunia maya juga telah menjadi

[87] Pierluigi Paganini. *Loc. cit.*

ancaman bagi daya saing Jepang Inc.[88] Beberapa situs tidak terdaftar dan situs portal di Cina ditemukan mengandung ratusan desain dan spesifikasi produk dari produsen Jepang, kata pihak yang bertugas untuk memantau dan tidak ingin disebutkan namanya karena menyangkut masalah keamanan nasional.[89]

Server yang digunakan untuk melakukan beberapa serangan dunia maya di Jepang berlokasi di Cina. Para peretas Cina merupakan salah satu aktor utama di balik hampir setiap operasi serangan dunia maya.[90] Banyak virus-virus yang digunakan untuk melakukan serangan dunia maya sering ditulis menggunakan sistem operasi *(operating-system)* berbahasa Cina.[91] Cina sering dituduh menjadi pelaku dari serangan *online* pada instansi pemerintah dan perusahaan, namun Pemerintah Beijing selalu membantahnya.[92] Menurut Badan Keamanan Komputer Tokyo, sebuah aktivitas *hacking* telah ditemukan di Cina dengan target India, Jepang, dan Tibet pada tahun 2012. Seorang programmer Cina dengan julukan yang mengandung kata-kata "Dang0102" dan "scuhkr" terlibat dalam aktivitas peretasan tersebut dan memata-matai untuk mencuri rahasia militer.[93]

Pemerintah Jepang juga telah menyadari sejak lama bahwa negara Cina merupakan suatu ancaman bagi beberapa negara termasuk Jepang terkait dengan sikap agresif Cina. Situs *Foreign Policy* melakukan wawancara eksklusif dengan Menteri Pertahanan Jepang Satoshi Morimoto untuk membahas sikap agresif Cina

---

[88] Yuriy Humber dan Gearoid Reidy. 2014. *Yahoo Hacks Highlight Cyber Flaws Japan Rushing toThwart*. Diakses dari http://www.bloomberg.com/news/2014-07-08/yahoo-hacks-highlight-cyber-flaws-japan-rushing-to-thwart.html. Diakses pada tanggal 15 Desember 2014.
[89] Ibid.
[90]Pierluigi Paganini. 2012. *Japan under cyber attack. The cyber threat China*. Diakses dari http://securityaffairs.co/wordpress/1911/cyber-warfare-2/japan-under-cyber-attack-the-cyber-threat-china.html. Diakses pada tanggal 15 Desember 2014.
[91]Yuriy Humber dan Gearoid Reidy. 2014. *Yahoo Hacks Highlight Cyber Flaws Japan Rushing toThwart*. Diakses dari http://www.bloomberg.com/news/2014-07-08/yahoo-hacks-highlight-cyber-flaws-japan-rushing-to-thwart.html. Diakses pada tanggal 15 Desember 2014.
[92]*China-based servers in Japan cyber attacks: report*. 2011. Diakses dari http://phys.org/news/2011-10-china-based-servers-japan-cyber.html. Diakses pada tanggal 15 Desember 2014.
[93]SPAMfighter News. 2012. *Chinese Hackers Pose Cyber Threat for Japan, India, and Tibet*. Diakses dari http://www.spamfighter.com/News-17620-Chinese-Hackers-Pose-Cyber-Threat-for-Japan-India-and-Tibet.htm. Diakses pada tanggal 15 Desember 2014.

tersebut khususnya terkait masalah serangan dunia maya yang ditujukan ke negara Jepang.

Berikut ini kutipan wawancara antara reporter dari Situs *Foreign Policy* melakukan wawancara eksklusif dengan Menteri Pertahanan Jepang Satoshi Morimoto:

> *"***FP:** Seberapa rentan Jepang terhadap serangan dunia maya dari Cina? *(How vulnerable is Japan to cyberattacks from China?)*
>
> ***SM*:** Masyarakat kita, termasuk organisasi pemerintah, serta beberapa (bagian dari) pertahanan dan industri teknologi informasi telah menjadi target serangan dunia maya dari Cina, meskipun Cina membantah melakukan serangan dunia maya yang sangat disengaja tersebut. Permasalahannya adalah kita tidak memiliki beton atau hukum internasional yang komprehensif untuk melarang serangan dunia maya atau aksi teroris dunia maya terhadap negara lain. Terutama karena definisi dunia maya begitu sulit dan begitu kompleks. Bahkan jika kita bisa mendefinisikan apa itu dunia maya, kita tidak memiliki organisasi internasional atau mekanisme untuk mendeteksi serangan dunia maya. Bahkan jika kita dapat mendeteksi serangan dunia maya, kita tidak dapat melakukan intervensi pada kedaulatan bangsa lain *(already our society, including government organizations, as well as some [parts of] the defense and IT industries have already been the target of cyberattacks from China, although China denies conducting such very intentional cyberattacks. The problem is we have no concrete or comprehensive international law to prohibit cyberattacks or cyber-terrorism against another country. Mainly due to the definition of cyber -- it's so difficult, so complex. Even if we could define what cyber is, we have no international organization or mechanism to detect cyberattacks. And even if we can detect cyberattacks, we cannot intervene on the sovereignty of another nation).*"*[94]

Jurnalis dari situs *Foreign Policy* meminta penjelasan tentang kerentanan serangan dunia maya terhadap Jepang yang berasal dari Cina. Menteri Pertehaan

[94]Isaac Stone Fish. 2013. *Japan's former defense minister talks to FP about cyberattacks, the East China Sea face-off, and whether North Korea's Kim Jong Un is a puppet dictator*. Diakses dari http://www.foreignpolicy.com/articles/2013/06/10/we_face_a_very_serious_chinese_military_threat_japan_defense_minister_interview. Diakses pada tanggal 15 Desember 2014.

Jepang (Satoshi Morimoto) menjelaskan bahwa saat masyarakat Jepang termasuk organisasi pemerintah telah menjadi bagian dari teknologi informasi dan komunikasi, saat itu mereka menjadi target serangan dunia maya oleh Cina. Hal yang menjadi masalah adalah masih sedikit hukum internasional yang dapat melarang serangan dunia maya dan menindak dengan tegas pelaku kejahatan tersebut. Pemerintah Jepang pun masih belum memiliki organisasi yang berskala internasional atau mekanisme untuk mendeteksi serangan dunia maya. Sekalipun mereka dapat mendeteksi serangan dunia maya, mereka tidak dapat melakukan intervensi terhadap kedaulatan bangsa lain. Oleh karena itu, Pemerintah Jepang berusaha untuk mengajak kerjasama negara-negara lain secara internasional untuk memperkuat hukum terkait masalah dunia maya *(cyberspace)* lintas negara.

Ancaman-ancaman yang dilakukan melalui dunia maya di Jepang saat ini membuat isu kejahatan dunia maya bukan lagi dianggap sebagai kejahatan biasa namun dapat mengganggu keamanan nasional Jepang. Hal itu mendorong Pemerintah Jepang untuk segera mengambil langkah-langkah khusus untuk membuat kebijakan dan strategi yang bertujuan untuk memperkuat keamanan negara tersebut dari ancaman dunia maya.

BAB IV
UPAYA PEMERINTAH SHINZO ABE DALAM MENINGKATKAN KEAMANAN NASIONAL JEPANG DARI ANCAMAN DUNIA MAYA

Pemerintah Jepang membuat upaya-upaya keamanan dunia maya yang lebih intensif melalui pertahanan diri dari ancaman dunia maya *(cyber defense)* pada masa pemerintahan Perdana Menteri Shinzo Abe. Perdana Menteri Shinzo Abe menyadari bahwa kehadiran dunia maya sebagai pendukung infrastruktur telah meningkat setiap hari dan berpotensi menimbulkan ancaman dunia maya yang lebih serius. Shinzo Abe memberikan pernyataan sebagai berikut:

> *"*Aktivitas ekonomi global terjadi tanpa memikirkan batas-batas negara di dunia maya saat ini. Kehadiran dunia maya sebagai pendukung infrastruktur meningkat setiap hari. Pada sisi lain, dibandingkan dengan delapan tahun lalu, ketika, sebagai Sekretaris Kabinet, saya adalah menteri yang bertanggung jawab atas kebijakan keamanan dunia maya, ancaman di dunia maya global menjadi lebih kompleks dan serius *(in cyberspace right now, global economic activity is occurring with no thought to national borders. The presence of cyberspace as infrastructure supporting society is increasing on a daily basis. On the other hand, compared to eight years ago, when, as Chief Cabinet Secretary, I was the minister in charge of cyber security policy, the threats in globalized cyberspace are becoming more complex and serious).*"[95]

Pernyataan Shinzo Abe diatas menjelaskan bahwa dalam dunia maya, aktivitas ekonomi global terjadi tanpa menghiraukan batas-batas negara dan ancaman dunia maya global menjadi lebih kompleks dan serius pada saat ini. Selain itu, menurut Perdana Menteri Shinzo Abe, keamanan dunia maya merupakan masalah yang sangat penting dan harus segera dilakukan upaya untuk menjaga keamanan tersebut. Shinzo Abe memberikan pernyataan sebagai berikut:

> "Keamanan dunia maya merupakan masalah yang sangat penting sehingga kita tidak harus menunggu untuk bertindak. Jepang, sebagai negara terkemuka di bidang teknologi informasi dan

[95] Prime Minister of Japan and His Cabinet. 2013. *ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation*. Diakses dari http://japan.kantei.go.jp/96_abe/actions/201309/12asean_e.html. Diakses pada tanggal 6 Januari 2014.

> komunikasi, telah mendorong maju dunia untuk mengambil berbagai, masalah serius keamanan dunia maya *(cybersecurity is an issue of the utmost importance that we must not wait to act upon. Japan, as a leading country in the field of ICT, has been pushing ahead of the world to take on the various, serious issues of cybersecurity).”*[96]

Jepang sebagai negara yang maju dalam bidang teknologi informasi dan komunikasi mendorong negara-negara di dunia untuk mengambil beberapa upaya dalam menanggapi masalah serius dari keamanan dunia maya. Bab 4 berisi tentang upaya-upaya yang dilakukan Pemerintah melalui Perdana Menteri Shinzo Abe untuk meningkatkan keamanan nasional Jepang dari ancaman kejahatan dunia maya, seperti membuat strategi dan personel yang bertanggung jawab untuk menjaga keamanan dunia maya dan kerjasama bilateral maupun multilateral dengan negara-negara yang mempunyai fokus keamanan yang sama dengan Jepang.

4.1 Strategi Keamanan Dunia Maya *(Cyber Security Strategy)*

Pemerintah Jepang mengambil langkah-langkah untuk memperkuat keamanan nasionalnya dari ancaman kejahatan dunia maya dengan membuat suatu strategi yang bertujuan untuk menilai ancaman serangan *online* dan menerapkan langkah-langkah untuk melawan mereka. Pusat Keamanan Informasi Nasional Jepang atau *National Information Security Center (NISC)* merilis Strategi Keamanan Dunia Maya Jepang *(Cyber Security Strategy)* pada tanggal 10 Juni 2013. Pemerintah Jepang membuat strategi tersebut untuk mempromosikan langkah-langkah yang berkaitan dengan dunia maya kepada seluruh pemangku kepentingan baik secara nasional maupun internasional.[97]

---

[96] Ibid.

[97] Information Security Policy Council. 2013. *Cyber Security Strategy: Towards a world-leading, resilient, and vigorous cyberspace.* Diakses dari www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf. Diakses pada tanggal 6 Januari 2015. Hlm. 4.

Strategi Keamanan Dunia Maya *(Cyber Security Strategy)* mempunyai slogan yaitu *a "world-leading," "resilient" and"vigorous" cyberspace*.[98] Slogan tersebut mempunyai arti bahwa Pemerintah Jepang bertekad untuk menjadikan ruang dunia maya Jepang sebagai ruang yang "kuat", "tangguh", dan "terdepan di dunia" sehingga dunia maya dapat menjadi sistem sosial untuk mewujudkan suatu masyarakat yang kuat terhadap serangan dunia maya dan masyarakat yang penuh inovasi.[99] Strategi tersebut menggambarkan peran pemerintah *(government)*, penyedia infrastruktur penting *(critical infrastructure providers)*, perusahaan *(companies)*, individu *(individuals)*, dan operator yang terkait dengan dunia maya *(cyberspace-related operators)* dalam mewujudkan tiga elemen yang telah dijelaskan sebelumnya, yaitu dunia maya yang "kuat", "tangguh", dan "terdepan di dunia".[100] Oleh karena itu, demi mewujudkan ketiga elemen tersebut, Pemerintah Jepang meningkatkan keamanan informasi dan memperkuat kemampuan untuk melawan serangan dunia maya di antara para pemangku kepentingan *(stakeholders)* untuk mewujudkan dunia maya yang "tangguh", memperkuat kreativitas dan pengetahuan melalui teknologi berkembang, pengembangan kapasitas dan meningkatkan keaksaraan masyarakat untuk mewujudkan dunia maya yang "kuat", dan memperkuat kontribusi dan sosialisasi melalui diplomasi, sosialisasi global dan kerjasama internasional untuk mewujudkan dunia maya yang "terdepan di dunia".[101]

Strategi Keamanan Dunia Maya diharapkan dapat menjadi solusi bagi Pemerintah Jepang dalam mewujudkan dunia maya yang aman bagi semua pihak, baik individu, organisasi, perusahaan, maupun instansi pemerintahan. Oleh karena itu, strategi ini berfokus pada kerjasama antara pihak-pihak yang terkait dengan dunia maya untuk mewujudkan keamanan dunia maya seperti yang diharapkan oleh pemerintah. Selanjutnya penjelasan mengenai prinsip dasar strategi

---

[98] Ibid. Hlm. 19.
[99] Ibid.
[100] Kelly Ng. 2013. *Japan releases national cyber security strategy*. Diakses dari http://www.futuregov.asia/articles/japan-releases-national-cyber-security-strategy. Diakses pada tanggal 7 januari 2015.
[101] Ibid.

keamanan dunia maya untuk mewujudkan keamanan dunia maya yang ada di Jepang dan peran dari para pemangku kepentingan.

4.1.1 Prinsip Dasar Strategi Keamanan Dunia Maya *(Cyber Security Strategy)*

Dokumen Strategi Keamanan Dunia Maya mempunyai empat prinsip dasar untuk mewujudkan keamanan dunia maya yang ada di Jepang, yaitu :[102]

1. Menjamin Arus Informasi yang Bebas

   Dunia maya telah memberikan berbagai manfaat positif bagi masyarakat Jepang, termasuk berbagai inovasi, pertumbuhan ekonomi dan solusi untuk isu-isu sosial namun tetap menjamin kebebasan berekspresi dan melindungi kepentingan privasi. Oleh karena itu, Pemerintah Jepang sedang menuju arah pengembangan suatu ruang dunia maya yang aman dan dapat diandalkan, dimana arus pertukaran informasi dapat mengalir bebas tanpa adanya resiko kejahatan dunia maya *(cyber crime)*.[103]

2. Menanggapi Resiko yang Semakin Serius

   Resiko yang ada di sekitar dunia maya menjadi semakin serius. Respon langsung terhadap resiko tersebut menjadi penting untuk dilakukan. Jika dunia maya rentan terhadap serangan dunia maya dan berbagai ancaman lain, maka semakin sulit untuk memastikan arus informasi yang bebas dan bisa terjadi penurunan kepercayaan masyarakat terhadap dunia maya. Oleh karena itu, selain langkah-langkah penanganan sebelum dan setelah kejadian, pun dibutuhkan mekanisme baru melalui upaya multi-lapis *(multi-layered)* sebagai suatu sistem sosial yang cepat dan tepat untuk mengatasi perubahan resiko terkait dengan revolusi yang ada dalam teknologi informasi dan komunikasi.[104]
3. Meningkatkan Pendekatan Berbasis Resiko

   Pemerintah Jepang telah menerapkan kebijakan bagi masing-masing aktor termasuk instansi pemerintah, penyedia infrastruktur penting, bisnis dan

[102] Information Security Policy Council. *Op. cit*. Hlm. 20.
[103] Ibid.
[104] Ibid.

individu untuk mengerahkan upaya maksimal dalam menangani keamanan informasi mereka sendiri. Namun pemerintah perlu melanjutkan langkah-langkah yang dilakukan oleh masing-masing aktor, seperti memajukan kemampuan analisis ancaman dengan mempromosikan pertukaran informasi, dan memperkuat pendekatan berbasis resiko berdasarkan karakteristik resiko melalui kemampuan secara dinamis dalam menanggapi insiden yang terjadi.[105]

4. Bertindak dalam Kemitraan Berdasarkan Tanggung Jawab Bersama

   Lembaga yang berbeda seperti pemerintah, masyarakat, akademisi, industri dan sektor swasta di Jepang telah ikut merasakan manfaat dari dunia maya. Dengan demikian, penting bagi setiap entitas untuk melaksanakan langkah-langkah keamana informasi mereka sendiri dengan cara yang independen dan proaktif sebagai bagian dari tanggung jawab sosial mereka untuk mewujudkan dunia maya yang kuat, tangguh, dan terkemuka di dunia. Dalam hal ini, para pemangku kepentingan *(multi-stakeholder)* dan masyarakat perlu untuk bekerja sama dan membantu satu sama lain termasuk kerjasama internasional dan kerjasama antara sektor publik dan swasta demi memenuhi tanggung jawab sesuai dengan peran masing-masing.[106]

4.1.2 Peran Para Pemangku Kepentingan *(multi-stakeholders)*

Beberapa lembaga dan perusahaan yang ada di Jepang telah ikut berperan secara proaktif sebagai aktor keamanan dunia maya. Pemerintah Jepang berencana untuk memberikan lebih banyak wewenang kepada Pusat Keamanan Informasi Nasional atau *National Information Security Center (NISC)* untuk memungkinkan mereka berfungsi sebagai komando keamana dunia maya dan mereorganisasi

[105] Ibid. Hlm. 21.
[106] Ibid. Hlm. 22.

NISC menuju/menjadi Pusat Keamanan Dunia Maya *(Cyber Security Center)* pada akhir Maret 2016.[107]

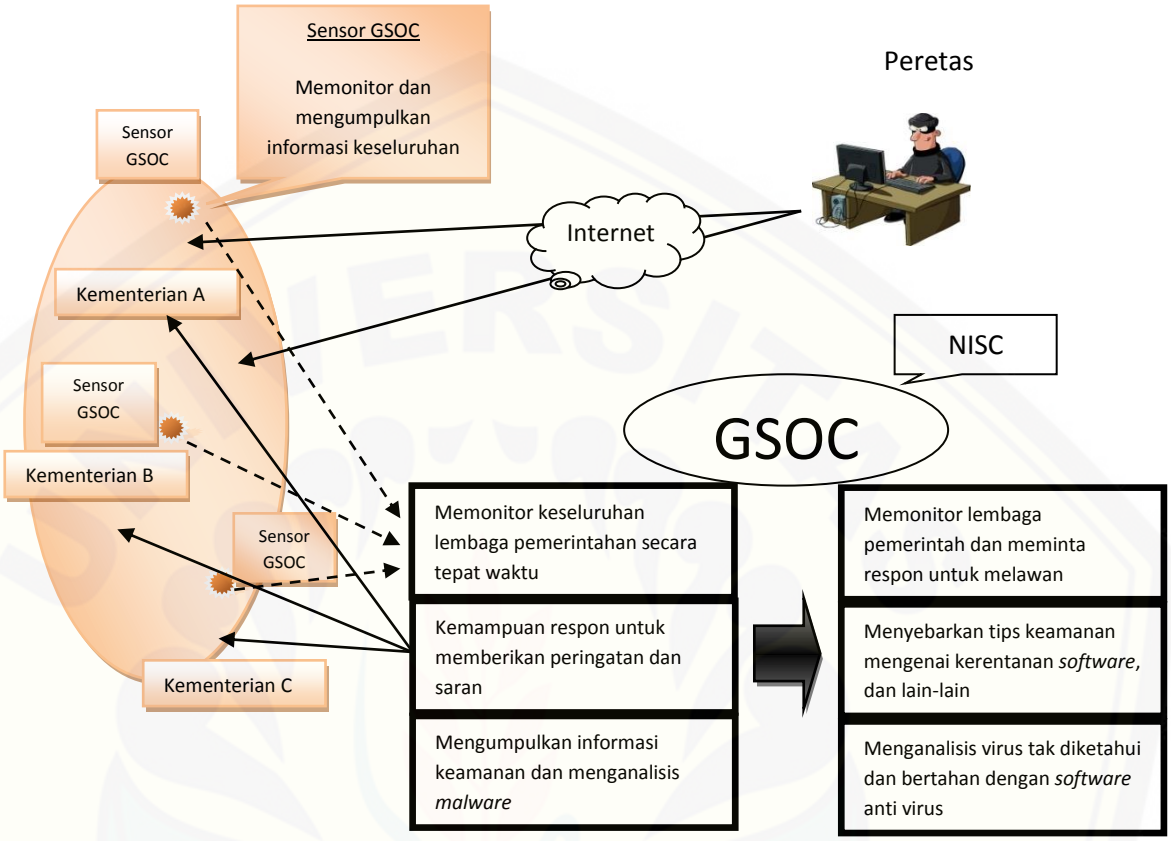
Peran Pemerintah Jepang sangat berpengaruh dalam memperkuat dunia maya di Jepang. Pemerintah harus memperkuat fungsi dasar negara yang terkait dengan dunia maya. Selain itu, pemerintah harus melaksanakan penanggulangan kejahatan dunia maya dan pertahanan dunia maya *(defense of cyberspace)* dengan melibatkan partisipasi lembaga lain terkait dan pemerintah asing. Pada saat yang sama, Pemerintah Jepang pun harus bekerja untuk memperkuat fungsi NISC sebagai pusat keamanan dunia maya dan juga secara proaktif mempersiapkan sistem baru.[108] Salah satunya adalah penguatan fungsi Tim Koordinasi Operasi Keamanan Pemerintah atau *Government Security Operation Coordination team* (GSOC).[109] GSOC berfungsi untuk memperkuat kemampuan institusi pemerintah dalam menghadapi keadaan darurat yang berkaitan dengan isu-isu keamanan informasi seperti serangan dunia maya eksternal.

NISC dan GSOC bekerjasama untuk menghadapi kerentanan yang ada pada sistem di lembaga-lembaga Pemerintah Jepang. Sebelumnya tugas GSOC adalah memonitor keseluruhan lembaga secara tepat waktu, memberikan peringatan dan saran saat terjadi serangan, dan mengumpulkan informasi keamanan dan menganalisis *malware*. Namun, penguatan yang dilakukan Pemerintah Jepang membuat tugas GSOC sedikit berubah. Tugas GSOC adalah memonitor lembaga pemerintah dan meminta respon untuk melawan serangan. Selain itu, GSOC bersama NISC bertugas untuk menyebarkan tips keamanan mengenai kerentanan *software*, dan menganalisis virus tidak diketahui sekaligus bertahan darinya.

---

[107] SSRC. 2013. *The gist of Japan's Cybersecurity Strategy adopted in June 2013*. Diakses dari http://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-027-en.html. Diakses pada tanggal 7 Januari 2015.
[108] Information Security Policy Council. *Op. cit.* Hlm. 24.
[109] Information Security Policy Council. *Op. cit.* Hlm. 32.

Gambar 4.1 Fungsi dan Tugas GSOC



Sumber: NISC. 2014. *CYBERSECURITY ANNUAL REPORT*. Diakses dari http://www.nisc.go.jp/eng/pdf/CYBERSECURITY_ANNUAL%20REPORT_2013_eng.pdf. Diakses pada tanggal 20 Maret 2015.

Gambar 4.1 merupakan fungsi GSOC saat terjadi serangan peretas terhadap lembaga-lembaga Pemerintah Jepang. Peretas melakukan serangan dunia maya melalui internet dengan mengirimkan suatu *e-mail* dengan melampirkan virus berbahaya *(malware)* didalamnya. Saat *e-mail* masuk ke dalam sistem lembaga pemerintahan, hal itu terdeteksi oleh sensor GSOC dan GSOC melakukan tugasnya seperti yang telah disebutkan sebelumnya dengan dibantu oleh NISC.

Peran yang tidak kalah penting adalah peran dari infrastruktur penting yang ada di Jepang. Infrastruktur penting merupakan dasar dari kehidupan sosial

masyarakat dan kegiatan ekonomi yang tidak bisa digantikan. Oleh karena itu, Pemerintah Jepang membutuhkan inisiatif untuk penyedia infrastruktur penting dalam 10 bidang informasi dan komunikasi seperti bidang keuangan, penerbangan, kereta api, listrik, gas, pemerintah dan pelayanan administrasi (termasuk pemerintah daerah), pelayanan kesehatan, air dan logistik.[110] Selanjutnya, Pemerintah Jepang harus mempertimbangkan langkah-langkah untuk bidang-bidang ini yang didasarkan pada karakteristik atau masing-masing bidang. Salah satu contohnya adalah Pemerintah Jepang pada sistem CEPTOAR. CEPTOAR adalah Kemampuan untuk Teknik Perlindungan, Operasi teknis, Analisis dan Respon atau *Capability for Engineering of Protection, Technical Operation, Analysis and Response.* Sistem ini berfungsi untuk menyaring dan menganalisis informasi di 10 bidang infrastruktur penting.

Perusahaan swasta, lembaga pendidikan dan lembaga penelitian pun memiliki peran untuk menguatkan keamanan dunia maya Jepang. Badan-badan tersebut memiliki properti intelektual terkait informasi seperti informasi teknologi, informasi keuangan, informasi teknologi manufaktur seperti informasi pribadi seperti daftar klien, informasi kepegawaian dan informasi pendidikan, dan informasi penting lainnya.[111] Oleh karena itu, selain langkah-langkah keamanan informasi secara pribadi, langkah-langkah kolektif di perusahaan swasta, lembaga pendidikan dan lembaga penelitian seperti berbagi informasi yang berhubungan dengan serangan dunia maya sangat diperlukan. Perusahaan swasta, pendidikan lembaga dan lembaga penelitian diharapkan dapat bekerja sama dalam kolaborasi industri-pemerintah-akademisi untuk menciptakan teknologi yang canggih dan sumber daya manusia tingkat tinggi yang dapat membentuk suatu dunia maya yang kuat, tangguh dan terkemuka di dunia.

Kolaborasi antara industri-pemerintah-akademisi terlihat dengan diadakannya program kesadaran menjangkau keamanan informasi baru atau *New Information Security Outreach Awareness Program*. Pengetahuan mengenai dunia maya diperluas ke semua generasi, semua tempat, dan semua kegiatan. Pada bulan

[110] Ibid.
[111] Ibid.

Juli 2014, lembaga-lembaga tersebut mengadakan program kesadaran menjangkau keamanan informasi baru atau *New Information Security Outreach Awareness Program*.[112] Program baru tersebut dilaksanakan melalui pembuatan suatu logo dan simbol di media mengenai program itu setiap tahun, kegiatan yang dapat diikuti oleh semua kalangan, dan berjuang memperkuat masyarakat Jepang dari serangan dunia maya.

Gambar 4.2 Aktivitas Mencapai Kesadaran dan Penjangkauan Keamanan Informasi

Poster bulanan Keamanan Informasi

Logo Program dan Animasi program *New Information Security Outreach Awareness Program*

Sumber: Sumber: NISC. 2014. *CYBERSECURITY ANNUAL REPORT*. Diakses dari http://www.nisc.go.jp/eng/pdf/CYBERSECURITY_ANNUAL%20REPORT_2013_eng.pdf. Diakses pada tanggal 20 Maret 2015.

[112] NISC. 2014. *CYBERSECURITY ANNUAL REPORT*. Diakses dari http://www.nisc.go.jp/eng/pdf/CYBERSECURITY_ANNUAL%20REPORT_2013_eng.pdf. Diakses pada tanggal 20 Maret 2015. Hlm. 23.

4.2 Unit Pertahanan Dunia Maya *(Cyber Defense Unit)* dibawah Pasukan Pertahanan Jepang *(Self Defense Forces)*

Departemen Pertahanan Jepang atau *Japanese Ministry of Defense (JMoD)* dan Pasukan Pertahanan Jepang atau *Self Defense Forces (SDF)*[113] mengambil langkah-langkah penting untuk meningkatkan keamanan dunia maya Jepang seiring dengan banyaknya serangan-serangan dunia maya khususnya pada kontraktor pertahanan Jepang. SDF menangani serangan dunia maya dengan mengoperasikan fungsi yang diperlukan secara terpadu untuk melindungi sistem informasi mereka sendiri, sementara juga memberikan kontribusi terhadap pemerintah dengan mengumpulkan pengetahuan dan keterampilan tentang serangan dunia maya.[114] Dunia maya yang aman dan stabil sangat penting bagi Pasukan Pertahanan Jepang dalam melaksanakan tugas dan misinya.[115] Oleh karena itu, Departemen Pertahanan dan Pasukan Pertahanan Jepang mengambil langkah-langkah untuk melindungi sistem dan jaringan mereka sendiri.

Sejak tahun 2010, Departemen Pertahanan Jepang tidak hanya mengeluarkan doktrin-doktrin pertahanan dunia maya namun juga mulai menyiapkan komando terpadu, dalam bentuk Unit Pertahanan Dunia Maya atau yang disebut dengan *Cyber Defense Unit (CDU).*[116] Unit Pertahanan Dunia Maya mulai terbentuk pada bulan Maret 2014 untuk mendeteksi dan menanggapi serangan dunia maya yang terjadi pada jaringan *(network)* di dalam Departemen Pertahanan Jepang dan Pasukan Pertanan Jepang *(Self Defense Forces)*. Namun, Pemerintah Jepang akan memperluas tugas dan tanggung jawab dari unit tersebut agar mencakup lembaga-lembaga pemerintahan lainnya.[117] CDU bertujuan untuk menyatukan kemampuan dunia maya militer Jepang *(Japan's military cyber*

---

[113]Pasukan Pertahanan Jepang atau *Self Defense Forces (SDF)* adalah pasukan militer terpadu Jepang yang didirikan setelah berakhirnya Perang Dunia II.

[114] Ministry of Defense. 2013. *Regarding Response to Cyber Attacks.* Diakses dari http://www.mod.go.jp/e/jdf/no42/specialfeature.html. Diakses pada tanggal 8 Januari 2015.

[115] Ibid.

[116] Paul Kallender. 2014. J*apan, the Ministry of Defense and Cyber-Security.* Diakses dari *The RUSI Journal.* Diakses pada tanggal 8 Januari 2015. Hlm. 95.

[117] *Japan to form cyberspace defense unit Wednesday*. 2014. Diakses dari http://www.japantimes.co.jp/news/2014/03/25/national/japan-to-form-cyberspace-defense-unit-wednesday/#.VOgMiHysUSg. Diakses pada tanggal 8 Januari 2015.

capabilities) dari darat, laut, dan udara menjadi satu unit pada 2014[118] dengan personel sebanyak 100 orang.[119] Unit dengan anggaran sekitar ¥14.100.000.000[120] tersebut memonitor jaringan Departemen Pertahanan dan Pasukan Pertahanan Jepang selama 24 jam dan segera merespon apabila terjadi serangan dunia maya. Selanjutnya Unit tersebut bertugas mengumpulkan, menganalisis, mempelajari, dan meneliti informasi dari serangan dunia maya[121] serta berkolaborasi dengan kementerian dan lembaga lain dalam memperkuat kemampuan Jepang untuk menanggapi ancaman dunia maya dan berlokasi di dalam fasilitas Departemen Pertahanan.[122]

Selain itu, jurnal *Japan Defense Focus No. 42* juga menjelaskan tentang enam pilar tindakan penanggulangan serangan dunia maya yang diambil Pasukan Pertahanan Jepang *(Self Defense Forces)* dan Departemen Pertahanan Jepang *(Japanese Ministry of Defense)*.[123] Enam pilar penanggulangan serangan dunia maya oleh Pasukan Pertahanan Jepang dan Departemen Pertahanan Jepang adalah sebagai berikut:

1. Peningkatan keamanan sistem komunikasi informasi.

   Departemen Pertahanan Jepang bersama Pasukan Pertahanan Jepang menciptakan suatu program perangkat lunak atau perangkat keras bernama *firewall* yang berfungsi untuk menyaring kegiatan peretasan *(hacktivism)*, virus, dan Worm yang mencoba mencapai sistem komputer Infrastruktur Informasi Pertahanan atau *Defense Information Infrastructure (DII)* dari SDF dan Sistem Komando Pusat *(Central Command System)* melalui internet.

---

[118] Tobias Feakin. 2013. *Cyber Wrap*. Diakses dari http://www.aspistrategist.org.au/cyber-wrap/. Diakses pada tanggal 8 Januari 2015.
[119] Nir Kshetri. 2014. *Japan's Changing Cybersecurity Landscape*. Diakses dari *libres.uncg.edu/ir/uncg/f/N_Kshetri_Japans_2014.pdf. Diakses pada tanggal 8 Januari 2015.*
[120] Paul Kallender-Umezu. 2014. *Experts: Japan's New Cyber Unit Understaffed, Lacks Skills*. Diakses dari http://archive.defensenews.com/article/20130709/DEFREG03/307090007/Experts-Japan-s-New-Cyber-Unit-Understaffed-Lacks-Skills. Diakses pada tanggal 9 Januari 2015.
[121] Japan Defense Focus. 2014. *Japan-US Defense Ministrial Meeting*. Diakses dari http://www.mod.go.jp/e/jdf/pdf/jdf_no52.pdf. Diakses pada tanggal 8 Januari 2015. Hlm. 4.
[122] Tobias Feakin. *Loc. cit.*
[123] Ibid.

2. Pengembangan sistem perlindungan

   Pengembangan sistem perlindungan dilakukan dengan cara membentuk sistem pemantauan jaringan. Departemen Pertahanan Jepang bersama Pasukan Pertahanan Jepang menciptakan suatu sistem yang berfungsi untuk memantau jaringan infrastruktur pertahanan Jepang. Jaringan tersebut harus tetap berjalan, dan jika terjadi masalah seperti terjadi peretasan dapat segera diketahui oleh sistem pemantauan jaringan dan segera diperbaiki.

3. Pengembangan aturan-aturan.

   Departemen Pertahanan Jepang bersama Pasukan Pertahanan Jepang melakukan pengembangan aturan-aturan mengenai keamanan informasi di dalam Departemen Pertahanan Jepang. Kegiatan pengembangan tersebut dilakukan melalui pengajaran tentang perlindungan pelayanan informasi pertahanan. Selain itu, kedua instansi tersebut memperkuat sistem aturan, contohnya melakukan kegiatan mempromosikan pendidikan tentang pertahanan dunia maya dan melatih agar setiap karyawan dapat melakukan pengawasaan dan pemeriksaan secara mandiri mengenai serangan dunia maya.

4. Pengembangan sumber daya manusia

   Departemen Pertahanan Jepang bersama Pasukan Pertahanan Jepang mengadakan kegiatan untuk mengembangkan sumber daya manusia untuk menciptakan sumber daya manusia berkualitas dalam meningkatkan pertahanan keamanan dunia maya. Contohnya adalah dengan cara mengadakan studi ke luar negeri di Universitas Carnegie Mellon *(Carnegie Mellon University)* dan memberikan pendidikan khusus di Akademi Pertahanan Nasional Jepang.

5. Promosi pertukaran informasi,

   Departemen Pertahanan Jepang bersama Pasukan Pertahanan Jepang melakukan promosi untuk bertukar informasi masalah keamanan dunia maya dengan mengadakan kerjasama dan kolaborasi bersama departemen lain yang terkait dan Pusat Keamanan Information Nasional Jepang

(National Information Security Center), serta negara-negara lain yang terkait seperti Amerika Serikat.

6. Penelitian pada teknologi terkini.

   Departemen Pertahanan Jepang bersama Pasukan Pertahanan Jepang mengadakan penelitian pada teknologi yang bertujuan untuk menciptakan lingkungan praktis terhadap serangan dunia maya dan menciptakan lingkungan untuk melakukan pelatihan serangan dunia maya untuk para operator sistem komando.

Pasukan Pertahanan Jepang atau *Self Defense Force* menaungi suatu pasukan subordinat yang bertugas mengoperasi dan memelihara Infrastruktur Informasi Pertahanan *(Defense Information Infrastructure)* dari SDF dan Sistem Komando Pusat *(Central Command System)* yaitu Komando Sistem, Komputer, Komunikasi, Kontrol, Komando atau *the Command, Control, Communication, Computers, Systems Command (C4SC)*. Unit Pertahanan Dunia Maya Jepang berada dalam kontrol langsung Departemen Pertahanan dan tunduk pada bimbingan dan Pengawasan SDF C4SC.[124]

C4SC tidak hanya mendirikan sebuah sistem pencegahan intrusi untuk meningkatkan keamanan sistem informasi komunikasi dan sistem perlindungan termasuk peralatan analisis pertahanan dunia maya, tetapi juga memuat aturan yang menentukan pedoman dan pendekatan untuk melawan respon serangan dunia maya dan melakukan penelitian tentang teknologi terbaru. Hal tersebut bertujuan untuk memenuhi langkah-langkah komprehensif yang diperlukan termasuk peningkatan personel dan infrastruktur teknologi.[125]

---

[124] Kosuke Takahashi. 2014. *Japan establishes cyber defence unit*. Diakses dari www.neuro.sfc.keio.ac.jp/publications/pdf/jane.pdf. Diakses pada tanggal 9 Januari 2015.
[125] Ministry of Defense. 2013. *Regarding Response to Cyber Attacks*. Diakses dari http://www.mod.go.jp/e/jdf/no42/specialfeature.html. Diakses pada tanggal 8 Januari 2015.

Gambar 4.3 Posisi Unit Pertahanan Dunia Maya *(Cyber Defense Unit)* dalam Departemen Pertahanan Jepang

Sumber : Ministry of Defense. 2013. *Regarding Response to Cyber Attacks* http://www.mod.go.jp/e/jdf/no42/specialfeature.html, diakses pada tanggal 9 Januari 2015.

Gambar 4.1 penulis peroleh dari jurnal *Japan Defense Focus No. 42*. Gambar 4.1 menjelaskan bahwa Unit Pertahanan Dunia Maya Jepang berada di bawah C4SC. C4SC tersebut mengoperasi dan memelihara Infrastruktur Informasi Pertahanan atau *Defense Information Infrastructure (DII)* dan Sistem Komando Pusat *(Central Command System)* yang ada di SDF. Selain itu, gambar di atas menjelaskan bahwa Unit Pertahanan Dunia Maya sebagai suatu unit pengumpulan dan pertukaran informasi *(information gathering/sharing)*, perlindungan *(protection)*, latihan *(exercises)*, studi dan penelitian *(study and research)*, dan dukungan teknis *(technical support)* terhadap serangan dunia maya yang terjadi di Departemen Pertahanan.

Serangan dunia maya yang kompleks dan meluas membuat Departemen Pertahanan Jepang dan Pasukan Pertahanan Jepang perlu mengambil langkah-langkah untuk mengamankan sistem informasi mereka. Aksi peretasan *(hacktivism)* dan spionase dunia maya *(cyber espionage)* dapat berpotensi

menyebabkan kebocoran informasi rahasia di Kementerian Pertahanan terkait strategi-strategi pertahanan nasional Jepang kepada pihak-pihak luar dan secara tidak langsung akan berdampak pada Jepang secara keseluruhan. Oleh karena itu, Unit Pertahanan Dunia Maya didirikan sebagai langkah keamanan informasi dari Departemen Pertahanan Jepang *(Ministry of Defense)* dan Pasukan Pertahanan Jepang *(Self Defense Forces).*

4.3 Kerjasama Internasional Jepang terkait Keamanan Dunia Maya

Jepang merupakan negara dengan kekuatan ekonomi ketiga di dunia.[126] Semua kegiatan ekonomi bergantung pada teknologi dan internet, seperti munculnya *e-commerce.* Jika serangan dunia maya menyerang bidang ekonomi Jepang, hal itu akan berdampak pada negara-negara lain dan pasar internasional. Oleh karena itu, keamanan dunia maya Jepang sangat penting bagi Jepang dan juga masyarakat internasional. Tindakan secara internasional sangat diperlukan karena para pelaku kejahatan dapat menyerang jaringan melintasi batas-batas nasional.[127] Dampak potensial tersebut membuat Jepang berperan secara proaktif dalam meningkatkan keamanan dunia maya nasional dan internasonal, salah satunya dengan meningkatkan kerjasama internasional.

Selain itu, dunia maya internasional dapat terwujud dengan terbentuknya pertahanan diri secara kolektif *(collective self-defense).* Pertahanan diri secara kolektif membutuhkan sekutu atau mitra pertahanan untuk melakukan latihan bersama untuk meningkatkan keamanan informasi mereka.[128] Sejak operasi militer dan infrastruktur seperti pasokan energi, keuangan dan jasa medis semakin

---

[126] Mihoko Matsubara. 2013. *Japan's New Cybersecurity Mission: The government should act to bolster protections, for both national and international security.* Diakses dari http://thediplomat.com/2013/08/japans-new-cybersecurity-mission/. Diakses pada tanggal 11 Januari 2015.

[127] Ibid.

[128] Mihoko Matsubara. 2014. *Collective self-defence: What Japan's new defence policy means for international cooperation on cyber security*. Diakses dari http://www.eastasiaforum.org/2014/08/21/collective-self-defence-what-japans-new-defence-policy-means-for-international-cooperation-on-cyber-security/. Diakses pada tanggal 11 Januari 2015.

bergantung pada komputer dan internet, aliansi atau kemitraan pertahanan perlu menjaga keamanan dunia maya untuk membuat hubungan mereka tangguh.[129]

Pemerintah Jepang melalui Perdana Menteri Shinzo Abe mulai menyadari terjadinya signifikansi serangan dunia maya seperti spionase dan ancaman yang mengganggu infrastruktur penting di Jepang.[130] Oleh karena itu, Pemerintah Jepang mulai menyiapkan langkah-langkah seperti membangun sistem jaminan informasi yang kuat dan tidak terbatas, tidak hanya dengan menentukan aturan untuk melindungi informasi rahasia tetapi juga untuk menjamin sekutu dan negara-negara sahabat.[131]

4.3.1 Membangun Kerangka Kerjasama Keamanan Internasional di Dunia maya

Berbagai negara dengan nilai-nilai dan sistem yang berbeda hidup berdampingan di dunia maya. Selain itu, dunia maya digunakan dalam berbagai cara oleh entitas yang beragam. Sebagai upaya untuk memaksimalkan manfaat dunia maya, penting untuk memastikan bahwa hal itu dapat digunakan secara stabil. Oleh karena itu, aturan internasional perlu dibuat untuk berbagai kegiatan yang menggunakan media internet dan dunia maya, sekaligus memperkuat ikatan antar lembaga yang terkait dengan dunia maya dalam jangka menengah dan panjang.

Ada upaya global yang sedang berlangsung untuk pembuatan peraturan internasional tentang penggunaan dunia maya dalam rangka untuk memastikan penggunaan yang stabil dari dunia maya misalnya, Kelompok Ahli Pemerintah atau *Group of Government Experts* (GGE) dibentuk di bawah komite umum majelis PBB yang mengacu pada norma-norma untuk digunakan oleh negara

---

[129] Ibid.
[130] Mihoko Matsubara. 2013. *Japan's New Cybersecurity Mission: The government should act to bolster protections, for both national and international security.* Diakses dari http://thediplomat.com/2013/08/japans-new-cybersecurity-mission/. Diakses pada tanggal 11 Januari 2015.
[131] Ibid.

anggota dalam bidang informasi dan teknologi komunikasi.[132] Jepang terus memberikan kontribusi aktif seperti upaya global dan berbagi prinsip-prinsip dasar dan kebijakan di setiap kesempatan. Jepang memandang bahwa hukum internasional, termasuk Piagam PBB dan hukum kemanusiaan internasional, secara alami dapat berlaku untuk tindakan di dunia maya. Jepang secara aktif mengambil bagian dalam diskusi GGE di bidang informasi dan telekomunikasi dalam konteks keamanan internasional pada tahun 2013.[133] Negara tersebut memimpin diskusi internasional lebih lanjut tentang bagaimana hukum internasional yang ada harus diterapkan untuk tindakan di dunia maya.

Jepang secara terbuka terus mengumumkan berbagai strategi dan memperkuat kerjasama antar tim tanggap insiden keamanan komputer atau *computer security insident response team* serta membangun sistem berbagi informasi. Upaya juga dilakukan dalam membangun kerangka kerja kebijakan untuk keamanan nasional dari ancaman kejahatan dunia maya dengan penekanan pada aspek sosial dan ekonomi dari dunia maya, seperti peninjauan Pedoman *Organisation for Economic Co-operation and Development* OECD[134] untuk Keamanan Sistem dan Jaringan Informasi. Upaya tersebut juga merupakan bagian dari pembuatan peraturan internasional. Jepang telah berpartisipasi secara proaktif dalam diskusi di OECD, dan terus mempromosikan inisiatif dan langkah tersebut dalam kerjasama dengan berbagai negara.

Jepang secara aktif mengambil bagian dalam pembuatan peraturan internasional tentang kejahatan dunia maya dan mengembangkan langkah-langkah

---

[132] ISPC. 2013. *International Strategy on Cybersecurity Cooperation (j-initiative for Cybersecurity.* Diakses dari http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf. Diakses pada tanggal 22 Mei 2015.

[133] UNITED NATIONS. 2013. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Diakses dari http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf. Diakses pada tanggal 22 Mei 2015.

[134] OECD atau *Organisation for Economic Cooperation and Development* adalah adalah sebuah organisasi ekonomi internasional dari 34 negara yang didirikan pada tahun 1961 untuk mendorong kemajuan ekonomi dan perdagangan dunia. Jepang bergabung dalam organisasi tersebut pada tahun 1964. Untuk penjelasan lebih lengkap mengenai OECD dapat dilihat di http://www.oecd.org/.

membangun kepercayaan melalui dialog dan pertukaran informasi bilateral maupun multilateral termasuk melalui kerangka kerja regional seperti ASEAN Forum Regional. Selain itu, Jepang telah mengadakan dialog di berbagai tingkat, seperti *Japan-AS Cyber Dialogue* yang diadakan antara kementerian Jepang dan Amerika Serikat terkait dan lembaga. Kerjasama Jepang dengan Amerika Serikat sebagai sekutu negara tersebut menjadi sangat penting bagi keamanan nasional Jepang. Jepang akan terus memperkuat kemitraan dengan Amerika Serikat melalui berbagai cara termasuk berbagi dekat informasi dan praktik terbaik tentang ancaman kejahatan dunia maya, latihan praktis bersama, dan kerjasama untuk menjamin keamanan sistem bersama antara lembaga pertahanan Jepang dan Amerika Serikat, sebagai upaya untuk memperkuat pencegahan dan untuk meningkatkan efektivitas Pengaturan Keamanan Jepang-Amerika Serikat.

4.3.2 Kerjasama Bilateral

4.3.2.1 Kerjasama Keamanan Dunia Maya Jepang-Amerika Serikat

Amerika Serikat merupakan salah satu negara yang fokus terhadap keamanan negaranya terhadap ancaman kejahatan dunia maya. Presiden Obama memberikan pernyataan mengenai pentingnya keamanan dunia maya terhadap keamanan nasional Amerika Serikat. Selain itu, Presiden Obama juga memberikan pernyataan bahwa infrastruktur penting dan kekayaan intelektual Amerika Serikat sangat beresiko terhadap serangan dunia maya. Presiden Obama memberikan pernyataan sebagai berikut:

> “Kemakmuran ekonomi Amerika, keamanan nasional, dan kebebasan pribadi kita bergantung pada komitmen kita untuk mengamankan dunia maya dan mempertahankan Internet yang terbuka, dapat dioperasikan, aman, dan handal. Infrastruktur penting kita terus berada pada resiko ancaman di dunia maya, dan ekonomi kami dirugikan oleh pencurian kekayaan intelektual kita. Meskipun ancaman tersebut serius dan terus berkembang, saya percaya bahwa jika kita mengatasinya secara efektif, kita dapat memastikan bahwa

Internet tetap menjadi mesin pertumbuhan ekonomi dan *platform* untuk pertukaran ide yang bebas *(America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas)*"[135]

Pemerintah Jepang dan Amerika Serikat membuat beberapa kerjasama bilateral dalam menjaga keamanan nasional dari ancaman kejahatan dunia maya. Kedua negara tersebut membuat kesepakatan untuk membangun suatu kerangka bilateral untuk membahas cara-cara dalam melawan serangan dunia maya pada lembaga-lembaga pemerintahan, organisasi, maupun perusahaan. Selain itu, Jepang dan Amerika Serikat meningkatkan keamanan jaringan melalui beberapa kegiatan, salah satunya yaitu dengan cara berbagi informasi dan pertukaran keahlian teknis. Subbab ini menjelaskan tentang beberapa kerjasama bilateral antara Pemerintahan Amerika Serikat dan Pemerintahan Jepang dibawah Perdana Menteri Shinzo Abe termasuk upaya kedua negara tersebut untuk ikut berperan secara proaktif dalam menjaga keamanan dunia maya di Asia Pasifik.

[135] The White House. 2013. *Cybersecurity.* Diakses dari https://www.whitehouse.gov/issues/foreign-policy/cybersecurity. Diakses pada tanggal 22 Maret 2015.

A. Dialog Pertama terkait Isu Dunia Maya Jepang-Amerika Serikat *(the First Japan-US Cyber Dialogue)*

Kerjasama bilateral terkait dunia maya dan jaringan internet antara Pemerintah Jepang dan Amerika Serikat sudah dimulai sejak tahun 2009.[136] Kerjasama tersebut dimulai saat Amerika Serikat menerbitkan Buku Putih Ekonomi Internet yang berjudul Mencapai Potensi Penuh dari Ekonomi Internet di Jepang *(Internet Economy White Paper: Achieving the Full Potential of the Internet Economy in Japan)* dan merekomendasikan Jepang dan Amerika Serikat untuk memulai dialog ekonomi internet dengan akademisi, pemerintah, dan industri.[137] Dialog kerjasama itu terus dilakukan oleh Pemerintah Jepang dan Amerika Serikat dari tahun ke tahun.

Namun perjanjian kerjasama bilateral antara Pemerintah Jepang dan Amerika Serikat mulai direvisi pada tahun 2013.[138] Para pejabat Departemen Pertahanan dan Luar Negeri Jepang dan Amerika Serikat mengadakan pertemuan tingkat kerja *(working-level)* di Tokyo untuk memulai pembahasan tentang revisi Pedoman Kerjasama Pertahanan Jepang-Amerika Serikat *(Guidelines for Japan-U.S. Defense Cooperation)*, dan meliputi keamanan dunia maya.[139] Selanjutnya pada Mei 2013, Pemerintah Jepang dan Amerika Serikat mengadakan dialog pertama terkait isu dunia maya di Tokyo pada tanggal 9-10 Mei 2013.[140] Dialog antara Pemerintah Jepang dan Amerika Serikat terkait isu dunia maya dimulai pada tingkat Perdana Menteri Presiden.[141] Dialog tersebut dipandu oleh Duta Besar Jepang yang bertanggung jawab atas kebijakan dunia maya yaitu Osami

---

[136]SSRC. 2013. *History of Japan-US cybersecurity cooperation*. Diakses dari http://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-051-en.html. Diakses pada tanggal 13 Januari 2015.
[137] Ibid.
[138] Kyodo. 2013. *Talks start with U.S. on new defense plan: Greater SDF role sought as China grows more assertive*. Diakses dari http://www.japantimes.co.jp/news/2013/01/18/national/talks-start-with-u-s-on-new-defense-plan/. Diakses pada tanggal 13 Januari 2015
[139] SSRC. 2013. *History of Japan-US cybersecurity cooperation*. Diakses dari http://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-051-en.html. Diakses pada tanggal 13 Januari 2015.
[140] Ministry of Foreign Affairs of Japan. 2013. *Joint Statement Japan-U.S. Cyber Dialogue*. Diakses dari http://www.mofa.go.jp/region/page22e_000001.html. Diakses pada tanggal 13 Januari 2015.
[141] Ibid.

Imai dan sejumlah pejabat senior Pemerintah Jepang. Beberapa pejabat tersebut termasuk Departemen Luar Negeri; Sekretariat Kabinet (Urusan Keamanan Nasional dan Manajemen Krisis); Pusat Keamanan Informasi Nasional; Kabinet Intelejen dan Kantor Penelitian; Badan Kepolisian Nasional; Kementerian Dalam Negeri dan Komunikasi; Kementerian Ekonomi, Perdagangan dan Industri; Departemen Pertahanan; dan dari METI yang berafiliasi dengan Lembaga Promosi Teknologi Informasi.[142] Sedangkan dari pihak Pemerintah Amerika Serikat, Sekretaris Koordinator Negara untuk Isu Dunia Maya yaitu Christopher Painter memimpin delegasi antar lembaga Pemerintah Amerika Serikat. Delegasi tersebut termasuk perwakilan dari Departemen Luar Negeri; Departemen Keamanan Dalam Negeri; Departemen Kehakiman; dan Departemen Pertahanan.[143]

Dialog terkait dunia maya *(cyber dialogue)* merupakan wadah untuk bertukar informasi mengenai ancaman serangan dunia maya. Selain itu, dialog tersebut bertujuan untuk menyelaraskan kebijakan dunia maya internasional, saling membandingkan strategi dunia maya masing-masing negara, bekerja sama pada perencanaan dan upaya untuk melindungi infrastruktur penting, dan membahas kerjasama pada bidang pertahanan dunia maya nasional serta kebijakan keamanan dunia maya.[144] Pemerintah Jepang dan Amerika Serikat berupaya memperdalam kerjasama bilateral dan memperkuat aliansi Jepang-Amerika Serikat khususnya pada isu dunia maya melalui beberapa cara:[145]

1. Bertukar informasi tentang isu-isu dunia maya yang menjadi perhatian bersama dan membahas kemungkinan langkah-langkah kooperatif
2. Menegaskan tujuan bersama dalam forum dunia maya internasional, khususnya penerapan norma-norma terkait dunia maya
3. Mendukung pengembangan langkah-langkah pembangunan kepercayaan praktis dan pelaksanaan strategi dunia maya seluruh

[142] Ibid.
[143] Ibid.
[144] Ibid.
[145] Ibid.

pemerintah nasional dalam upaya untuk mengurangi resiko di dunia maya

4. Mengkonfirmasi dukungan terhadap pelestarian keterbukaan dan interoperabilitas yang ditingkatkan oleh sistem multi pihak *(multi-stakeholders)* dari tata kelola internet
5. Mengkoordinasi kerjasama pada upaya pengembangan kapasitas dunia maya di negara-negara ketiga
6. Mengidentifikasi tindakan pemerintah dan sektor swasta untuk mengamankan infrastruktur penting
7. Membahas peningkatan peran pertahanan dunia maya dalam strategi keamanan dan pertahanan nasional dan membahas tentang bidang baru dari kerjasama pertahanan dunia maya bilateral.

Dialog pertama antara Pemerintah Jepang dan Amerika Serikat menunjukkan bahwa para pembuat kebijakan mulai memberikan perhatian terhadap isu keamanan dunia maya. pembahasan itu termasuk masalah pertahanan dunia maya, pembentukan norma-norma perilaku di dunia maya, dan perlindungan infrastruktur penting. Dialog tersebut menjadi sebuah babak baru dalam hubungan bilateral kedua negara dengan membuat kerangka untuk kerjasama keamanan dunia maya yang komprehensif. Upaya tersebut tentu membantu pemerintah kedua negara dalam menggunakan sumber daya yang lebih efisen untuk melindungi dunia maya dan membuat aliansi yang lebih kuat.

B. Pelatihan Yama Sakura terkait Pertahanan Dunia Maya

Selain dialog mengenai isu dunia maya, Pemerintah Jepang dan Amerika Serikat melakukan upaya-upaya lain untuk meningkatkan pertahanan dunia maya. Salah satunya adalah Yama Sakura. Yama Sakura merupakan latihan bilateral tahunan antara Pasukan Pertahanan Darat Jepang atau *the Japan Ground Self-Defense Force (JGSDF)* dan militer Amerika Serikat.[146] Yama Sakura adalah latihan pos komando terbesar yang berfokus pada bilateral dan perencanaan

[146] USARPAC Public Affairs. 2013. *Yama Sakura 65*. Diakses dari http://www.army.mil/article/116507/Yama_Sakura_65/. Diakses pada tanggal 12 Januari 2015.

bersama, koordinasi, dan interoperabilitas elemen berbasis darat dari aliansi keamanan Jepang dan Amerika Serikat.[147]

Pertahanan dunia maya mulai tercakup dalam latihan Yama Sakura pada latihan Yama Sakura 65.[148] Yama Sakura 65 (YS65) dilakukan di Camp Higashi-Chitose Hokkaido, Jepang pada tanggal 8 sampai 14 Desember 2013.[149] Angkatan laut dan udara juga akan terlibat dalam latihan tersebut untuk melaksanakan perencanaan bersama.[150] YS65 menegaskan komitmen lanjutan oleh Amerika Serikat dan Jepang untuk bekerja sebagai mitra berdedikasi dalam mendukung aliansi keamanan Amerika Serikat dengan Jepang dan untuk perdamaian dan stabilitas di kawasan Asia Pasifik.[151] Yama Sakura 65 merupakan latihan Yama Sakura yang pertama kali menggabungkan pasukan JGSDF dan I CORPS[152] dalam skenario pertahanan dunia maya menjadi latihan bilateral mereka.[153] Kebutuhan untuk menguji dan mengembangkan sistem pertahanan maya menjadi prioritas utama. Sejak I CORPS menyeimbangkan korps militer Amerika Serikat di Asia Pasifik secara permanen, pasukan tersebut merencanakan masa depan terkait pertahanan diri melawan serangan dunia maya dengan mitra mereka yaitu Jepang.

Semua pasukan militer perlu memahami pentingnya peran pertahanan dunia maya untuk stabilitas suatu negara. Hal itu yang mulai disadari oleh Pemerintah Jepang da Amerika Serikat. Kesadaran ancaman dunia maya membuat Jepang dan Amerika Serikat mengadakan pelatihan bersama terkait dunia maya melalui latihan Yama Sakura. Yama Sakura menjadi dasar untuk implementasi lebih lanjut di masa depan. Pelatihan ini dapat memberikan pasukan militer

---

[147] Ibid.
[148] U.S. Pasific Command. 2013. *Yama Sakura trains US and Japanese troops on Cyber Defense*. diakses dari https://www.youtube.com/watch?v=7qND0roT5h8. diakses pada tanggal 12 Januari 2015.
[149] USARPAC Public Affairs. *Loc. cit*.
[150] Ibid.
[151] Ibid.
[152] I CORPS adalah korps Angkatan Darat Amerika Serikat yang berkantor pusat di Pangkalan Bersama Lewis-McChord, Whasington. Korps ini merupakan formasi utama dari Komando Ankatan Darat Amerika Serikat. Misi I CORPS saat ini adalah menjadi bagian dari pergeseran Asia Pasifik.
[153] U.S. Pasific Command. *Loc. cit.*

Jepang dan Amerika Serikan suatu pemahaman yang sama dalam beradaptasi terhadap organisai militer mereka untuk mengatasi ancaman dunia maya.

C. Kerjasama Dunia Maya Jepang-Amerika Serikat di ASEAN

Kerjasama antara Pemerintah Jepang dan Amerika Serikat untuk memerangi kejahatan dunia maya meluas ke wilayah regional ASEAN. Hal tersebut sebagai tindak lanjut pernyataan Jepang dan Amerika Serikat untuk membantu ASEAN dalam memerangi kejahatan dunia maya.[154] Selanjutnya pada bulan Mei 2014, kedua pemerintah tersebut membuat kesepakatan untuk melatih para penyelidik di ASEAN untuk menyelidiki serangan dunia maya yang terjadi. Langkah ini dinilai penting karena para peretas yang berasal dari Cina sering menggunakan server yang ada di Asia Tenggara untuk melakukan serangan dunia maya terhadap Jepang, Amerika Serikat, dan negara-negara lain. [155]

Pemerintah Jepang dan Amerika Serikat berencana untuk membantu 10 anggota Perhimpunan Negara-Negara Asia Tenggara *(the Association of Southeast Asian Nations)* dalam meningkatkan kemampuan teknis mereka untuk menyelidiki kejahatan dunia maya.[156] Oleh karena itu, Pemerintah Jepang akan memberikan dana sebesar $150.000 dan Pemerintah Amerika Serikat sebesar $250.000 kepada PBB untuk memfasilitasi pengiriman tenaga ahli anti kejahatan dunia maya oleh Kantor PBB untuk Narkoba dan Kejahatan *(the U.N. Office on Drugs and Crime).*[157] Program pelatihan tersebut berlangsung sampai 2015 dan diperpanjang berdasarkan keberhasilan awal. Jangka waktu pelatihan dan perpanjangan pelatihan tersebut tergantung dari hasil pembahasan oleh Jepang-

---

[154]Kyodo News International. 2014. *Japan, U.S. to help ASEAN boost cybercrime investigation skills*. Diakses dari http://www.globalpost.com/dispatch/news/kyodo-news-international/140607/japan-us-help-asean-boost-cybercrime-investigation-ski. Diakses pada tanggal 13 Januari 2015.

[155] Clint Richards. 2014. *New ASEAN Anti-Cyber Skills Aimed at China: Japan and the U.S. are using ASEAN to further crack down on Chinese cybercrimes.* Diakses dari http://thediplomat.com/2014/06/new-asean-anti-cyber-skills-aimed-at-china/. Diakses pada tanggal 13 Januari 2015.

[156] Kyodo News International. *Loc. cit*.

[157] Ibid.

Amerika Serikat bersama Kantor PBB untuk Narkoba dan Kejahatan (UNODC).[158]

Beberapa bentuk kerjasama yang dilakukan oleh Pemerintah Jepang dan Amerika Serikat terjadi karena kedua negara tersebut menyadari bahwa kejahatan dunia maya yang terjadi di beberapa negara khususnya Jepang dan Amerika tidak bisa dihentikan secara pribadi, namun memerlukan kerjasama dengan negara lain. Kejahatan dunia maya lintas batas yang semakin meningkat membuat kedua negara tersebut meningkatkan pertahanan di bidang dunia maya, dan diharapkan mampu untuk mewujudkan keamanan dunia maya intenasional secara bersama-sama.

4.3.2.2 Kerjasama Keamanan Dunia Maya Jepang-India *(Japan-India Cyber Security Cooperation)*

Negara India merupakan salah satu negara yang mengalami serangan *malware* dengan angka yang cukup tinggi.[159] India menjadi negara kedua dengan serangan dunia maya terbesar setelah Amerika Serikat.[160] Serangan dunia maya yang canggih seperti *ransomware*[161] dan *phishing* telah merugikan individu dan perusahaan di India sebesar $4 miliar.[162] Gulshan Rai, Direktur Jenderal Tim Respon Darurat Komputer India atau *Computer Emergency Response Team India (CERT-In)* mengatakan dalam artikel Nikkei bahwa serangan dunia maya di India berjumlah sekitar 250 pada tahun 2005 dan meningkat menjadi lebih dari 70.000

---

[158] Ibid.
[159] Nikkei. 2014. *India and Japan beef up cyber security*. Diakses dari http://asia.nikkei.com/Business/Trends/India-and-Japan-beef-up-cyber-security. Diakses pada tanggal 14 Januari 2015.
[160] Atlantic Council. 2013. *Addressing India's Cyber Threats.* Diakses dari http://www.atlanticcouncil.org/events/past-events/addressing-india-s-cyber-threats. Diakses pada tanggal 14 Januari 2015.
[161] *Ransomware* merupakan suatu perangkat lunak berbahaya yang didesain untuk meblokir akses ke suatu komputer sampai dilakukan pembayaran sebelum pemilik komputer dapat mengakses file dan program lagi. Untuk penjelasan lebih lengkap mengenai *ransomware* dapat dilihat di http://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
[162] Amit R Saksena. 2014. *India Scrambles on Cyber Security:*
One of the most targeted countries in the world, India is beginning to act on the cyber threat. Diakses dari http://thediplomat.com/2014/06/india-scrambles-on-cyber-security/. Diakses pada tanggal 14 Januari 2015.

pada Desember 2013.[163] Hal itu membuat keamanan dunia maya menjadi prioritas bagi Pemerintah India.

Oleh karena itu, Pemerintah Jepang dan India memutuskan untuk bekerjasama dalam bidang teknologi, seperti keamanan dunia maya, teknologi hijau dan pengembangan teknologi informasi dan komunikasi.[164] Kedua negara tersebut mempunyai kekuatan yang saling melengkapi dalam bidang telekomunikasi. Jepang mempunyai teknologi yang sangat baik dalam sisi perangkat keras *(hardware)* sedangkan negara India mempunyai perangkat lunak *(software)* yang sangat baik. Dua kekuatan yang saling melengkapi antara Jepang dan India membuat kedua negara tersebut mempererat kerjasama di bidang teknologi dan dunia maya.

Jepang dan India memiliki proyek bersama dalam bidang teknologi dan keamanan dunia maya. Proyek tersebut ditegaskan dalam pertemuan Kelompok Kerja Bersama Jepang-India *(Japan-India Joint Working Group)* selama dua hari di New Delhi pada tanggal 3 Desember 2014.[165] Pertemuan tersebut diresmikan oleh H.E. Ravi Shankar Prasad, Menteri Komunikasi dan Informatika India, dan diketuai oleh H.E. Mr Yasuo Sakamoto, Wakil Menteri untuk Koordinasi Kebijakan MIC dari Jepang dan Shri Rakesh Garg, Sekretaris Telekomunikasi dari India.[166]

Selama pertemuan berlangsung, Jepang dan India membuat rencana proyek-proyek bersama, dan sebagai hasil dari diskusi tersebut telah diputuskan lima bidang proyek yang akan dijadikan prioritas dari proyek tersebut, yaitu:[167]

- Dalam bidang Teknologi Informasi dan Komunikasi Hijau *(Green ICT)*

---

[163] Nikkei. *Loc. cit.*
[164] Press Information Bureau. 2014. *India and Japan to Cooperate in the Fields of Cyber Security and Green ICT (Information and Communication Technology)*. Diakses dari http://pib.nic.in/newsite/PrintRelease.aspx?relid=112548. Diakses pada tanggal 14 Januari 2015.
[165] Press Information Bureau. 2014. *Two Day India Japan Joint Working Group for Strengthening Cooperation in the Field Information and Communication Technologies begins in New Delhi.* Diakses dari http://pib.nic.in/newsite/PrintRelease.aspx?relid=112474. Diakses pada tanggal 14 Januari 2015.
[166] *Joint Press Statement for The Second India - Japan Joint Working Group under India-Japan ICT Comprehensive Cooperation Framework*. 2014. Diakses dari http://www.soumu.go.jp/main_content/000325863.pdf. Diakses pada tanggal 14 Januari 2015.
[167] Ibid.

- Proyek stasiun induk berbasis seluler hijau

- Dalam bidang kerjasama keamanan dunia maya
  - Jepang dan India bersama-sama akan memerangi proyek spam
  - Proyek kerjasama untuk mendeteksi gejala dan respon cepat untuk serangan dunia maya
- Dalam bidang teknologi informasi dan komunikasi untuk penanggulan bencana
  - Proyek penggunaan teknologi komunikasi dan informasi dalam daerah yang terkena dampak bencana
- Dalam bidang aplikasi teknologi informasi dan komunikasi untuk tantangan ekonomi dan sosial
  - Proyek aplikasi identitas nasional *(National ID)* dan landasan pemanfaatan *(utilization platform)*

Selanjutnya Kementerian Komunikasi dan Informasi India atau *Ministry for Communication and Information Technology (MCIT)* dan Kemernterian Dalam Negeri dan Komunikasi Jepang atau *Ministry of Internal Affairs and Communication (MIC)* akan mengkoordinasikan kegiatan untuk melajutkan proyek-proyek tersebut dengan melibatkan mitra industri kedua negara.[168] Selain itu, sebagai upaya untuk lebih mempererat jalinan kerjasama di bidang teknologi informasi dan komunikasi, Pemerintah India telah menawarkan kepada Pemerintah Jepang untuk untuk memproduksi peralatan teknologi informasi dan komunikasi di India.[169]

Jepang dan India merupakan negara dimana tingkat penggunaan internet relatif tinggi. Selain itu, kedua negara tersebut mempunyai infrastruktur teknologi yang tinggi pula. Kondisi itu membuat Jepang dan India memperluas kerjasama mereka yang telah lama terjalin dengan memasukkan bidang pertahanan dunia maya karena serangan dunia maya dapat mengancam infrastruktur teknologi

[168] Press Information Bureau. 2014. *India and Japan to Cooperate in the Fields of Cyber Security and Green ICT (Information and Communication Technology)*. Diakses dari http://pib.nic.in/newsite/PrintRelease.aspx?relid=112548. Diakses pada tanggal 14 Januari 2015.
[169] Ibid.

informasi di kedua negara. Namun, sedikit berbeda dengan kerjasama keamanan dunia maya yang telah ada, Pemerintah Jepang dan India memasukkan bidang teknologi informasi dan komunikasi hijau *(green ICT)* sebagai salah satu proyek yang menjadi prioritas. Selain langkah-langkah keamanan dunia maya, Jepang dan India membangun suatu stasiun induk yang bergerak di bidang *green ICT* untuk mengurangi dampak teknologi terhadap lingkungan, baik secara langsung maupun tidak langsung.

4.3.3 Kerjasama Multilateral

4.3.3.1 Kerjasama Keamanan Dunia Maya Jepang dan ASEAN

Negara-negara anggota ASEAN telah mulai meningkatkan kewaspadaan mereka dalam hal serangan dunia maya. Negara-negara anggota ASEAN menyadari bahwa serangan dunia maya mempunyai pengaruh yang cukup besar terhadap pertumbuhan ekonomi di negara-negara ASEAN. Saat ini, negara-negara anggota ASEAN sangat mendorong pertumbuhan ekonomi melalui penelitian dan pengembangan *(research and development)*.[170] Oleh karena itu, negara-negara tersebut mulai memiliki peraturan kejahatan dunia maya dan membentuk kelompok kerja kejahatan dunia maya yang baru *(new cybercrime working group)*.[171] Negara harus meningkatkan kemampuan mereka untuk menindak kejahatan dunia maya sebagai upaya untuk melindungi rahasia dagang dari industri penelitian mereka. Selain itu, keamanan dunia maya yang tangguh bisa memicu investasi berbasis teknologi dan penelitian yang tinggi di kawasan tersebut.

Hubungan Jepang dan ASEAN yang sudah cukup lama terjalin dan kesamaan fokus terhadap ancaman kejahatan dunia maya di masing-masing negara membuat Pemerintah Jepang dan ASEAN bekerjasama dalam meningkatkan keamanan dunia maya di kawasan ASEAN dan meningkatkan

---

[170] Jake Lerner. 2013. *Cybercrime Enforcement: ASEAN's New Industrial Policy?.* Diakses dari http://basc.berkeley.edu/?p=1184. Diakses pada tanggal 16 Januari 2015.
[171] Ibid.

kemampuan negara-negara ASEAN untuk melawan ancaman dunia maya. Pemerintah Jepang berencana untuk mempromosikan komunikasi yang efisien antara Pemerintah Jepang dan lembaga-lembaga pemerintahan yang bertanggung jawab atas kejahatan dunia maya di negara anggota ASEAN.[172] Pemerintah Jepang melalui Perdana Menteri Shinzo Abe intensif melakukan beberapa kerjasama internasional yang lain terkait masalah keamanan dunia maya dengan ASEAN karena banyak perusahaan Jepang yang berada di kawasan tersebut, diantaranya adalah Pertemuan Kebijakan Kementerian ASEAN-Jepang dalam Kerjasama Keamanan Dunia Maya *(ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation)* pada September 2013 dan Dialog Dunia Maya Perdana antara ASEAN dan Jepang *(The Inaugural ASEAN-Japan Cybercrime Dialogue)* pada Mei 2014.

Pemerintah Jepang telah membuat dan mendistribusikan sebuah film animasi pendidikan tentang cara untuk melawan kejahatan dunia maya.[173] Film ini berupa film pendek yang berisi tentang cara seseorang melindungi informasi pribadinya di *handphone* dari para peretas dan para mitra ASEAN akan menunjukkan film di lembaga pendidikan dan di TV.[174] Pada bulan April 2014, film tersebut telah tersebar di *youtube* dalam bahasa Inggris.[175] Namun, film tersebut diterjemahkan dalam bahasa Indonesia, Tagalog, Brunei Malay, Khmer, Laos, Malaysia, Myanmar, Cina, Thailand, dan Vietnam untuk memudahkan penonton yang berasal dari negara anggota ASEAN. Jepang dan ASEAN juga membuat suatu kampanye berupa tulisan dan poster di Jepang dan negara-negara ASEAN tentang pentingnya keamanan informasi dan bahayanya kejahatan dunia maya. Langkah-langkah tersebut merupakan inisiatif dalam meningkatkan kewaspadaan terhadap keamanan informasi.

---

[172]Nikkei. 2014. *Japan to help Asean fight cybercrime*. Diakses dari http://asia.nikkei.com/Politics-Economy/International-Relations/Japan-to-help-Asean-fight-cybercrime. Diakses pada tanggal 16 Januari 2015.
[173] Ibid.
[174] Ibid.
[175] NISC. 2014. *Use Your Smartphone with Confidence(English)[NISC]*. Diakses dari https://www.youtube.com/watch?v=ZHc2s6Gq-BU. Diakses pada tanggal 15 Maret 2015.

A. Pertemuan Kebijakan Kementerian ASEAN-Jepang dalam Kerjasama Keamanan Dunia Maya *(ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation)*

Pertemuan Kebijakan Kementerian ASEAN-Jepang dalam Kerjasama Keamanan Dunia Maya *(ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation)* diadakan di Tokyo, Jepang selama dua hari, yaitu pada tanggal 12 dan 13 September 2013. Pertemuan tentang dunia maya tersebut bertepatan dengan 40 tahun terjalinnya persahabatan antara negara Jepang dengan negara-negara anggota ASEAN.[176] Peserta yang hadir dalam pertemuan tersebut diantaranya adalah menteri-menteri dari negara anggota ASEAN (Brunei Darussalam, Kerajaan Kamboja, Republik Indonesia, Republik Demokratik Rakyat Laos, Malaysia, Republik Uni Myanmar, Republik Filipina, Republik Singapura, Kerajaan Thailand dan Republik Sosialis Vietnam) yang bertanggungjawab dalam informasi dan komunikasi, Mr. Yoshitaka Shindo (Menteri Urusan Dalam Negeri dan Komunikasi), dan Mr. Masaaki Taira (Sekretaris Parlemen Ekonomi, Perdagangan, dan Industri).[177] Para peserta mengeluarkan sebuah pernyataan bersama tingkat menteri sebagai hasil dari diskusi mengenai percepatan kerjasama antara Jepang dan masing-masing negara ASEAN di bidang keamanan dunia maya.[178]

Sebuah laporan final hasil dari diskusi "Pertemuan Kebijakan Kementerian ASEAN-Jepang" menyatakan bahwa dunia maya yang aman merupakan salah satu faktor utama dalam inovasi serta menjadi penting dalam mempromosikan kegiatan sosial dan ekonomi, dan memperkuat konektivitas ASEAN.

---

[176] *Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation*. 2013. Diakses dari http://www.meti.go.jp/press/2013/09/20130913005/20130913005-5.pdf. Diakses pada tanggal 17 Januari 2015.

[177] Ministry of Internal Affairs and Communications. 2013. *Results of Japan-ASEAN Ministerial Policy Meeting on Cyber Security Cooperation*. Diakses dari http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130913_01.html. Diakses pada tanggal 17 Januari 2015.

[178] Ibid.

> "Kami percaya bahwa dunia maya yang aman merupakan salah satu faktor utama dalam inovasi serta menjadi penting dalam mempromosikan kegiatan sosial dan ekonomi dan memperkuat konektivitas ASEAN *(we believe that a secure cyberspace is one of the major drivers in innovation as well as being essential in promoting social and economic activities and strengthening ASEAN connectivity).*"[179]

Jadi, tujuan dari penguatan kerjasama di bidang keamanan dunia maya adalah untuk menciptakan lingkungan bisnis yang aman dalam ekonomi pengetahuan, membangun lingkungan untuk mengamankan penggunaan teknologi informasi dan komunikasi, dan mendukung strategi keamanan dunia maya oleh pemerintah melalui kerjasama kementerian yag terkait dan lembaga-lembaga dalam pemerintah masing-masing negara anggota ASEAN dan Jepang.[180]

Negara-negara ASEAN dan Pemerintah Jepang melakukan upaya-upaya keamanan dunia maya dengan melihat tingkat perkembangan yang berbeda dari masing-masing negara anggota. Oleh karena itu, dalam melakukan upaya tersebut mereka harus mempertimbangkan beberapa prinsip untuk mempromosikan keamanan dunia maya, yaitu:[181]

- Langkah-langkah apapun yang menumbuhkan dunia maya yang handal harus terus mendorong arus informasi, interoperabilitas dan kemakmuran ekonomi, dan tidak seharusnya mengganggu kelancaran fungsi teknis internet;
- Pertimbangan untuk menjaga arus informasi dan mendorong kegiatan ekonomi harus dipikirkan dan diambil saat mulai memperkenalkan regulasi;
- Pengguna internet harus didorong untuk mengembangkan literasi mereka mengenai keamanan dunia maya, termasuk pengaturan diri;

---

[179] *Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation*. 2013. Diakses dari http://www.meti.go.jp/press/2013/09/20130913005/20130913005-5.pdf. Diakses pada tanggal 17 Januari 2015.
[180] Ibid.
[181] Ibid.

- Para pembuat kebijakan dan regulator harus berkolaborasi dengan sektor swasta agar secara efektif dapat dan segera mengatasi ancaman dan resiko dunia maya.

Selanjutnya, para delegasi dari Pertemuan Kebijakan Kementrian ASEAN-Jepang dalam Kerjasama Keamanan Dunia Maya mempromosikan upaya bersama mereka lebih lanjut dengan mempertimbangkan undang-undang domestik, peraturan dan sumber daya yang tersedia. Mereka mendorong keamanan dunia maya dalam bidang berikut:[182]

I. Menciptakan lingkungan bisnis yang aman, yaitu dengan cara:
   - Mendorong entitas publik dan swasta untuk meningkatkan tingkat keamanan dunia maya melalui Sistem Manajemen Keamanan Informasi atau *Information Security Management System (ISMS)*;
   - Mempromosikan kerjasama dan kolaborasi antara kementerian yang terkait dan lembaga seperti Tim Respon Insiden Keamanan Komputer atau *Computer Security Incident Response Teams (CSIRTs)* dari negara-negara anggota ASEAN dan Jepang melalui inisiatif seperti Proyek Berbagi Data Pengawasan Lalu Lintas Internet atau *Internet Traffic Monitoring Data Sharing Project (TSUBAME Project);*

II. Membangun suatu jaringan komunikasi dan informasi yang aman
   - Meningkatkan keamanan jaringan melalui kegiatan seperti pertukaran informasi tentang langkah-langkah anti botnet dan anti spam;
   - Meningkatkan kerjasama teknis untuk keamanan melalui kegiatan seperti Kemitraan Keamanan Jepang-ASEAN atau *Japan-ASEAN Security Partnership (JASPER)* yang terdiri dari proyek Respon Proaktif Melawan Serangan Dunia Maya Melalui Pertukaran Kolaboratif Internasional atau *Proactive Response Against Cyber-attacks Through International Collaborative Exchange (PRACTICE)* dan peringatan infeksi;

[182] Ibid.

- Mempromosikan pertukaran keahlian teknis seperti kerjasama antar Penyedia Layanan Internet atau *Internet Service Providers (ISPs)* yang difasilitasi oleh otoritas terkait dari negara-negara anggota ASEAN dan Jepang, dan pertukaran peneliti;

III. Meningkatkan kapasitas untuk keamanan dunia maya

- Mempromosikan kerjasama di bidang strategi keamanan dunia maya termasuk perlindungan infastruktur penting, kemitraan publik-swasta, rencana kesinambungan bisnis untuk teknologi informasi dan komunikasi, perlindungan kelompok yang rentan secara *online* khususnya anak-anak, keamanan komputasi awan, dan keamanan telepon seluler canggih *(smartphone)*;
- Membina perkembangan sumber daya manusia melalui kegiatan seperti Inisiatif Pembangunan Kapasitas Kemananan Dunia Maya ASEAN-Jepang *(ASEAN-Japan Cybersecurity Capacity-Building Initiatives)*;
- Membangun suatu mekanisme untuk negara-negara anggota ASEAN dan Jepang untuk memungkinkan berbagi informasi, dan respon cepat pada insiden dunia maya melalui aktivitas seperti latihan dunia maya;
- Mempromosikan kewaspadaan bersama dengan meningkatkan kegiatan di antara negara-negara anggota ASEAN dan Jepang.

Beberapa upaya yang telah disebutkan di atas diterapkan dalam kerjasama antara Jepang dan ASEAN, sehingga dunia maya yang ada di kawasan tersebut dapat menjadi dunia maya yang tangguh dan aman.

> "Kami percaya bahwa dengan menerapkan prinsip-prinsip di atas dan memfokuskan upaya bersama kami secara terus-menerus di daerah yang disebutkan di atas dalam semangat konsensus, dengan mempertimbangkan berbagai tahap perkembangan negara anggota ASEAN, kita akan mampu mengembangkan langkah-langkah yang akan menghasilkan dunia maya lebih aman bagi warga negara, masyarakat bisnis dan pemerintah *(we believe that by applying the above principles and focusing our continued joint efforts in the areas mentioned above in the spirit of consensus, taking into consideration the*

different stages of development of ASEAN Member States, we will be able to develop measures which will result in a more secure cyberspace for our citizens, business communities and government)."[183]

Berdasarkan hasil diskusi dari Pertemuan Kebijakan Kementerian ASEAN-Jepang dalam Kerjasama Keamanan Dunia Maya, para menteri yang hadir dalam pertemuan tersebut percaya bahwa dengan memfokuskan upaya bersama dalam bidang yang telah disebutkan diatas dan dengan mempertimbangkan tahap perkembangan negara-negara anggota ASEAN, Pemerintah Jepang dan ASEAN akan mampu mengembangkan langkah-langkah yang akan menghasilkan dunia maya yang lebih aman bagi warga negara, komunitas bisnis dan pemerintah.

B. Dialog Perdana Kejahatan Dunia Maya ASEAN-Jepang *(The Inaugural ASEAN-Japan Cybercrime Dialogue)*

Pembahasan mengenai dunia maya yang terjadi antara Pemerintah Jepang dan ASEAN berlanjut dengan diadakannya "Dialog Perdana Kejahatan Dunia Maya ASEAN-Jepang" *(The Inaugural ASEAN-Japan Cybercrime Dialogue)* diselenggarakan pada hari Rabu, tanggal 28 Mei 2014 di Singapura. Dialog tersebut diketuai oleh H.E. Mr. Jun Shimmi, Duta Besar yang bertugas pada kebijakan dunia maya, Menteri Luar Negeri Jepang; dan Mr. Benny Oon, Direktur Senior, Divisi Kemitraan dan Kerjasaman Internasional, Menteri Dalam Negeri Republik Singapura.[184] Dialog tersebut dihadiri oleh para pejabat dari Jepang, semua negara-negara anggota ASEAN dan sekretariat ASEAN.

Dialog perdana tekait kejahatan dunia maya antara ASEAN dan Jepang membahas kerjasama antara negara-negara anggota ASEAN dan Jepang dalam meningkatkan keamanan dunia maya dan mengatasi kejahatan dunia maya yang terjadi, seperti promosi berbagi informasi mengenai kecenderungan dan pelajaran

[183] Ibid.
[184]Ministry of Foreign Affairs of Japan. 2014. *The Inaugural ASEAN-Japan Cybercrime Dialogue*. Diakses dari http://www.mofa.go.jp/press/release/press23e_000019.html. Diakses pada tanggal 19 Januari 2015.

untuk memerangi kejahatan dunia maya, promosi kerjasama internasional dalam mengatasi kejahatan dunia maya, pembangunan kapasitas untuk melawan kejahatan dunia maya, dan arah kegiatan nyata dengan menggunakan Dana Integrasi Jepang-ASEAN atau *Japan-ASEAN Integration Fund (JAIF).*[185]

Dialog perdana mengenai kejahatan dunia maya merupakan lanjutan dari Pertemuan Pejabat Senior ASEAN yang membahas Kejahatan Transnasional atau *ASEAN Senior Officials Meeting on Transnational Crime (SOMTC).* SOMTC membentuk suatu kelompok kerja pada kejahatan dunia maya. Kelompok kerja SOMTC yang membahas kejahatan dunia maya yang pertama diadakan sehari sebelum penyelenggaraan dialog mengenai kejahatan dunia maya, yaitu pada tanggal 27 Mei 2014.[186] Kelompok kerja tersebut mengasilkan suatu langkah *(roadmap)* untuk memerangi kejahatan dunia maya.

Puncak dari rangkaian pertemuan Pejabat Senior ASEAN yang membahas Kejahatan Transnasional atau *ASEAN Senior Officials Meeting on Transnational Crime (SOMTC)* adalah Dialog Penanggulangan Terorisme ASEAN-Jepang atau *ASEAN-Japan Counter-Terrorism (AJCT) Dialogue* yang diselenggarakan pada 29 dan 30 Mei 2014 di Singapura.[187] Dialog tersebut membahas tentang kemajuan negara-negara anggota ASEAN dan Jepang dalam bekerjasama menanggulangi terorisme, yang didalamnya juga mencakup tentang terorisme dunia maya *(cyber-terrorism).*

Hasil dari dialog dan diskusi antara Pemerintah Jepang dan ASEAN terkait keamanan dunia maya telah diaplikasikan melalui kegiatan pelatihan oleh Kementerian Ekonomi, Perdagangan, dan Industri atau *Ministry of Economy, Trade, and Industry* (METI) untuk mendukung peningkatan keamanan informasi di negara-negara anggota ASEAN. Kegiatan tersebut terselenggara pada 16

---

[185] Ibid.
[186] ASEAN Secretariat News. 2014. *ASEAN Steps Up Fight against Cybercrime and Terrorism*. Diakses dari http://www.asean.org/news/asean-secretariat-news/item/asean-steps-up-fight-against-cybercrime-and-terrorism. Diakses pada tanggal 19 Januari 2015.
[187] Ibid.

sampai 25 Februari 2015.[188] METI mengadakan sejumlah program pelatihan yang berjudul "Program Pelatihan pada Peningkatan Keamanan Informasi untuk ASEAN: fokus pada Keamanan ISMS dan ICS" atau *"the Training Program on Enhancing Information Security for ASEAN: Focusing on ISMS and ICS Security"*. Kegiatan tersebut mempunyai tujuan untuk meningkatkan sistem lingkungan bisnis pada negara-negara ASEAN.

Dari beberapa langkah yang telah dilakukan oleh Pemerintah Jepang dan Pemerintah negara-negara ASEAN dapat ditarik kesimpulan bahwa negara-negara ASEAN juga telah mulai meningkatkan kesadaran mereka terhadap pentingnya meningkatkan keamanan dunia maya. Tidak bisa dipungkiri jika negara anggota ASEAN pun juga banyak yang menjadi korban serangan dunia maya. Sebagai mitra, Jepang dan ASEAN berharap dapat meningkatkan keamanan dunia maya nasional bersama melalui pertukaran informasi mengenai dunia maya, pelatihan bersama, dan perwujudan lingkungan dunia maya yang aman bagi semua pihak. Oleh karena itu, sebagai salah satu negara yang mempunyai teknologi canggih di dunia, Jepang mengajak ASEAN untuk mulai memperluas kerjasama mereka dengan memasukkan isu dunia maya sebagai salah satu isu penting yang harus didiskusikan bersama.

Uraian di atas menjelaskan bahwa Negara Jepang dibawah Pemerintahan Shinzo Abe sangat gencar melakukan beberapa langkah-langkah untuk mengamankan keamanan dunia maya dan informasi di Jepang. Langkah-langkah yang dilakukan berskala nasional dan internasioanal. Hal itu menunjukkan bahwa keamanan dunia maya sangat penting untuk ditingkatkan bagi setiap pihak yang merasakan langsung manfaat dunia maya di sekitar kehidupan mereka. Beberapa langkah tersebut banyak menunjukkan adanya saling kerjasama antar para pemangku kepentingan *(stakeholders)* baik secara nasional maupun internasional.

---

[188] METI. 2015. *METI to Hold Training Programs to Support Enhancement of Informastion Security in the ASEAN Region.* Diakses dari www.meti.go.jp/english/press/2015/0216_02.html. Diakses pada tanggal 20 Maret 2015.

Upaya yang dilakukan untuk menjaga dan meningkatkan keamanan dunia maya pada Pemerintahan Shinzo Abe adalah pembuatan strategi keamanan dunia maya pada tahun 2013 yang mempunyai tujuan untuk menjadikan ruang dunia maya Jepang sebagai ruang yang kuat, tangguh, dan terdepan di dunia; pembentukan unit khusus yang bertanggung jawab untuk menjaga keamanan dunia maya khususnya keamanan Departemen Pertahanan Jepang atau *Japanese Ministry of Defense (JmoD)* dan Pasukan Pertahanan Jepang atau *Self Defense Forces (SDF)* yaitu Unit Pertahanan Dunia Maya *(Cyber Defense Unit)*, dan kolaborasi antara negara Jepang dan negara-negara yang mempunyai fokus yang sama dalam masalah keamanan dunia maya. Upaya tersebut menunjukkan bahwa Pemerintah Jepang sangat serius menanggapi kejahatan dunia maya melalui peningkatan pertahanan diri negara terhadap serangan dunia maya nasional dan internasional.

BAB V

KESIMPULAN

Alasan Perdana Menteri Shinzo Abe melakukan upaya-upaya peningkatan keamanan dunia maya di Jepang karena bidang teknologi dan internet telah menjadi infrastruktur penting dalam pertumbuhan ekonomi Jepang. Masyarakat Jepang baik itu individu, organisasi, perusahaan, maupun lembaga pemerintahan sangat bergantung pada teknologi. Selain bidang ekonomi, teknologi informasi sangat dibutuhkan di bidang lainnya, seperti politik, sosial, militer, dan budaya. Namun, ketergantungan tersebut disalahgunakan oleh pelaku kejahatan di dunia maya. Pelaku kejahatan dunia maya memanfaatkan kecepatan, kemudahan dan sifat anonimitas pada ruang dunia maya yang tidak mengenal batas untuk meretas jaringan para calon korban.

Serangan-serangan dunia maya yang terjadi di Jepang semakin kompleks, rumit, dan mengkhawatirkan. Serangan dunia maya di Jepang telah meluas menjadi serangan spionase dunia maya *(cyber espionage)* karena menimpa beberapa infrastruktur penting yang ada di Jepang, seperti perusahaan kontraktor terbesar di Jepang yang memproduksi alat-alat militer Jepang dan lembaga-lembaga pemerintah Jepang. Ancaman-ancaman peretasan dalam dunia maya tersebut juga banyak merugikan perusahaan dan organisasi di Jepang dalam hal ekonomi. Hal itu secara tidak langsung dapat mempengaruhi keamanan nasional Jepang secara keseluruhan. Oleh karena itu, kejahatan di bidang dunia maya di Jepang menjadi suatu isu keamanan *non* tradisional baru. Jaminan keamanan di bidang dunia maya menjadi salah satu elemen untuk mewujudkan keamanan nasional Jepang.

Tindak kejahatan di bidang dunia maya yang semakin meningkat membuat dunia maya masuk dalam strategi keamanan nasional pada tahun 2013 yang dibuat oleh Kabinet Perdana Menteri Shinzo Abe dan strategi pertahanan oleh Departemen Pertahanan Jepang. Perdana Menteri Shinzo Abe melakukan beberapa upaya yang berskala nasional dan internasional. Langkah-langkah yang

dilakukan untuk meningkatkan keamanan dunia maya diharapkan agar Jepang menjadi negara yang kuat, tangguh, dan terkemuka di dunia terkait teknologi dan dunia maya. Beberapa langkah tersebut banyak menunjukkan kolaborasi antara para pemangku kepentingan *(stakeholders)* baik secara nasional maupun internasional. Hal itu menunjukkan bahwa keamanan dunia maya sangat penting untuk ditingkatkan bagi setiap pihak yang merasakan langsung manfaat dunia maya di sekitar kehidupan mereka, baik itu individu, para pemangku kepentingan dan masyarakat yang ada di negara lain. Selain itu, Pemerintah Jepang banyak melakukan kerjasama bilateral dan multilateral untuk mewujudkan keamanan dunia maya internasional.

DAFTAR PUSTAKA

Buku

Anthony, Mely Caballero and Cook, Alistair D.B. 2013. *Non-Traditional Security in Asia: Issues, Challenges and Framework for Action*. Singapore: ISEAS Publishing.

Arikunto, Suharmini. 1989. *Prosedur Penelitian, Suatu Pendekatan Praktek.* Jakarta: PT. Bina Aksara

Broadhurst, Roderic and Grabosky, Peter. 2005. *Cyber-Crime: The Challenge in Asia*. Hongkong: Hong Kong University Press.

Caballero-Anthony, M., Emmers, R and Acharya, A. 2006. *Non Traditional Security in Asia: Dilemmas in Securitization.* USA: Ashgate Publishing Company

Coplin, William D. 2003. *Pengantar Politik Internasional: Suatu Telaah Teoritis Edisi Kedua* (Terjemahan: Marsedes Marbun). Bandung: Sinar Baru.

Hadi, Sutrisno. 1986. *Methode Research Jilid 1*. Yogyakarta: Gajahmada University Press.

Mas'oed, Mochtar. 1990. *Ilmu Hubungan Internasional, Disiplin, dan Metodologi.* Jakarta: LP3ES

Rudy, T. May. 2002. *Studi Strategis dalam Transformasi Sistem Internasional Pasca Perang Dingin*. Bandung: Refika Aditama.

Snyder, Craig A. 2008. *Contemporary Security and Strategy.* New York: Palgrave Macmillan.

The, Liang Gie. 1984. *Ilmu Politik: Suatu Pembahasan tentang Pengertian, Kedudukan dan Metodologi.* Yogyakarta: Gajahmada University Press.

Internet

ASEAN-Japan Ministerial. 2013. *Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation*. Diakses dari http://www.meti.go.jp/press/2013/09/20130913005/20130913005-5.pdf. Diakses pada tanggal 17 Januari 2015.

ASEAN Secretariat News. 2014. *ASEAN Steps Up Fight against Cybercrime and Terrorism*. Diakses dari http://www.asean.org/news/asean-secretariat-

news/item/asean-steps-up-fight-against-cybercrime-and-terrorism. Diakses pada tanggal 19 Januari 2015.

Bradley, Tony. 2014. *Your business can't afford the cost of cyber crime*. Diakses dari http://www.csoonline.com/article/2837805/malware-cybercrime/your-business-can-t-afford-the-cost-of-cyber-crime.html. Diakses pada tanggal 16 Desember 2014.

Defense Of Japan. 2014. *Security Environment Surrounding Japan*. Diakses dari www.mod.go.jp/e/publ/w_paper/pdf/2014/DOJ2014_1-1-0_web_1031.pdf. Diakses pada tanggal 7 Februari 2015.

Fish, Isaac S. 2013. *Japan's former defense minister talks to FP about cyberattacks, the East China Sea face-off, and whether North Korea's Kim Jong Un is a puppet dictator*. Diakses dari http://www.foreignpolicy.com/articles/2013/06/10/we_face_a_very_serious_chinese_military_threat_japan_defense_minister_interview. Diakses pada tanggal 15 Desember 2014.

Feakin, Tobias dan Wodall, Jessica. 2013. *Cyber Wrap*. Diakses dari http://www.aspistrategist.org.au/cyber-wrap/. Diakses pada tanggal 8 Januari 2015.

Hansen, L and Nissenbaum, H. 2009. *Digital Disaster, Cyber Security, and the Copenhagen School*. Diakses dari www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf. Diakses pada tanggal 9 Agustus 2014.

Information Security Policy Council. 2006. *The First National Strategy on Information Security*. Diakses dari www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf. Diakses pada tanggal 7 Februari 2015.

Information Security Policy Council. Juni 2013. *Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace.* Diakses dari www.nisc.go.jp/eng/pdf/CyberSecurityStrategy.pdf. Diakses pada tanggal 21 Juli 2014.

Internet Live Stats. 2014. *Internet Users by Country (2014)*. Diakses dari http://www.internetlivestats.com/internet-users-by-country/. Diakses pada tanggal 16 Desember 2014.

Internet World Stats. 2014. *World Internet Users and Population Stats*. Diakses dari http://www.internetworldstats.com/stats.htm. Diakses pada tanggal 6 Juli 2014.

IT Strategy Headquarters. 2001. *e-Japan Strategy*. Diakses dari http://japan.kantei.go.jp/it/network/0122full_e.html. Diakses pada tanggal 27 Januari 2015.

Japan Defense Focus. 2014. *Japan-US Defense Ministrial Meeting*. Diakses dari http://www.mod.go.jp/e/jdf/pdf/jdf_no52.pdf. Diakses pada tanggal 8 Januari 2015.

JAXA. 2014. *Japanese Experiment Module (KIBO)*. Diakses dari http://iss.jaxa.jp/en/kibo/. Diakses pada tanggal 24 Februari 2015.

Joint Press Statement for The Second India - Japan Joint Working Group under India-Japan ICT Comprehensive Cooperation Framework. Diakses dari http://www.soumu.go.jp/main_content/000325863.pdf. Diakses pada tanggal 14 Januari 2015.

Halo Jepang. 2014. *Kabinet Abe Tingkatkan Peran Tangani Kejahatan Dunia Maya*. Diakses dari http://www.halojepang.com/kabarutama/7837-kabinet. Diakses pada tanggal 6 Juli 2014.

Kallender, Paul. 2014. *Japan, the Ministry of Defense and Cyber-Security*. Diakses dari *The RUSI Journal*. Diakses pada tanggal 8 Januari 2015.

Kelly, Michael J et al. 1995. *Electronic Manufacturing and Packaging in Japan*. Diakses dari www.wtec.org/loyola/pdf/ep.pdf. Diakses pada tanggal 16 Desember 2014.

Koizumi Junichiro. 2014. Diakses dari http://www.britannica.com/EBchecked/topic/761351/Koizumi-Junichiro. Diakses pada tanggal 6 Februari 2015.

Lerner, Jake. 2013. *Cybercrime Enforcement: ASEAN's New Industrial Policy?*. Diakses dari http://basc.berkeley.edu/?p=1184. Diakses pada tanggal 16 Januari 2015.

Library of Congress. 2009. *Cybercrime: An Bibliography of Select Foreign-Language Academic Literature*. Diakses dari https://www.ncjrs.gov/pdffiles1/nij/231832.pdf. Diakses pada tanggal 6 Juli 2014.

Matsubara, Mihoko. 2013. *Japan's New Cybersecurity Mission: The government should act to bolster protections, for both national and international security.* Diakses dari http://thediplomat.com/2013/08/japans-new-cybersecurity-mission/. Diakses pada tanggal 11 Januari 2015.

Ministry of Defense. 2013. *Regarding Response to Cyber Attacks*. Diakses dari http://www.mod.go.jp/e/jdf/no42/specialfeature.html. Diakses pada tanggal 8 Januari 2015.

Ministry of Foreign Affairs of Japan. 2013. *Joint Statement Japan-U.S. Cyber Dialogue*. Diakses dari http://www.mofa.go.jp/region/page22e_000001.html. Diakses pada tanggal 13 Januari 2015.

Ministry of Foreign Affairs of Japan. 2013. *Statement by Minister for Foreign Affairs of Japan on Adoption of the National Security Strategy (NSS)*. Diakses dari http://www.mofa.go.jp/press/release/press4e_000141.html. Diakses pada tanggal 7 Februari 2015.

Ministry of Internal Affairs and Communications. 2013. *Policy Meeting on Cyber Security Cooperation*. Diakses dari http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130913_01.html. Diakses pada 17 Januari 2015.

National Information Security Center. 2007. *Japanese Government's Efforts to Address Information Security Issues*. Diakses dari www.nisc.go.jp/eng/pdf/overview_eng.pdf. Diakses pada tanggal 7 Februari 2015.

Natsui, Takato. 2003. *Cybercrimes in Japan: Recent Cases, Legislations, Problem and Perspectives*. Diakses dari www.netsafe.org.nz/Doc_Library/netsafepapers_takatonatsui_japan.pdf. Diakses pada tanggal 21 Agustus 2014.

Nikkei. 2014. *Japan to help Asean fight cybercrime*. Diakses dari http://asia.nikkei.com/Politics-Economy/International-Relations/Japan-to-help-Asean-fight-cybercrime. Diakses pada 16 Januari 2015.

Nitta, Yoko. *Japan's Approach Towards Internasional Strategy on Cyber Security Cooperation*. Diakses dari http://lsgs.georgetown.edu/sites/lsgs/files/Japan_edited%20v2.pdf_for_printout.pdf. Diakses pada tanggal 6 Juli 2014.

Paganini, Pierluigi. 2014. *Malware based attack hit Japanese Monju Nuclear Power Plant*. Diakses dari http://securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html. Diakses pada tanggal 16 Desember 2014.

Parker, Donn B. 1989. *Computer Crime: Criminal Justice Resource Manual*. Diakses dari

https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf. Diakses pada tanggal 16 Juli 2014.

Ponemon Institute. 2014. *2014 Cost of Cyber Crime Study: Japan*. Diakses dari http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA5-5213JPN. Diakses pada tanggal 15 Desember 2014.

Press Information Bureau. 2014. *India and Japan to Cooperate in the Fields of Cyber Security and Green ICT (Information and Communication Technology)*. Diakses dari http://pib.nic.in/newsite/PrintRelease.aspx?relid=112548. Diakses pada tanggal 14 Januari 2015.

Press Information Bureau. 2014. *Two Day India Japan Joint Working Group for Strengthening Cooperation in the Field Information and Communication Technologies begins in New Delhi*. Diakses dari http://pib.nic.in/newsite/PrintRelease.aspx?relid=112474. Diakses pada tanggal 14 Januari 2015.

Prime Minister of Japan and His Cabinet. 2013. *ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation*. Diakses dari http://japan.kantei.go.jp/96_abe/actions/201309/12asean_e.html. Diakses pada tanggal 6 Januari 2014.

Prime Minister of Japan and His Cabinet. *Yoshiro Mori Administration (The 85th and 86th Prime Minister)*. Diakses dari http://japan.kantei.go.jp/rekidaisouri/mori_e.html. Diakses pada tanggal 25 Januari 2015.

Richards, Clint. 2014. *New ASEAN Anti-Cyber Skills Aimed at China: Japan and the U.S. are using ASEAN to further crack down on Chinese cybercrimes*. Diakses dari http://thediplomat.com/2014/06/new-asean-anti-cyber-skills-aimed-at-china/. Diakses pada tanggal 13 Januari 2015.

Saksena, Amit R. 2014. *India Scrambles on Cyber Security: One of the most targeted countries in the world, India is beginning to act on the cyber threat*. Diakses dari http://thediplomat.com/2014/06/india-scrambles-on-cyber-security/. Diakses pada tanggal 14 Januari 2015.

SSRC. 2013. *The gist of Japan's Cybersecurity Strategy adopted in June 2013*. Diakses dari http://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-027-en.html. Diakses pada tanggal 7 Januari 2015.

SSRC. 2013. *History of Japan-US cybersecurity cooperation*. Diakses dari http://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-051-en.html. Diakses pada tanggal 13 Januari 2015.

Statistic Bureau MIC Japan. 2014. *Statistical Handbook of Japan 2014*. Diakses dari http://www.stat.go.jp/english/data/handbook/c0117.htm. Diakses pada tanggal 16 Desember 2014.

Takahashi, Kosuke. 2014. *Japan establishes cyber defence unit*. Diakses dari www.neuro.sfc.keio.ac.jp/publications/pdf/jane.pdf. Diakses pada 9 Januari 2015.

Taylor, Rob. 2011. *Japan's Defense Industry Hit by its First Cyber Attack*. Diakses dari http://www.reuters.com/article/2011/09/19/us-mitsubishiheavy-computer-idUSTRE78I0EL20110919. Diakses pada tanggal 23 Agustus 2014.

Umezu, Paul K. 2012. *Japan Takes Action Against Complex Cyber Threats*. Diakses dari http://www.defensenews.com/article/20121009/C4ISR01/310090010/Japan-Takes-Action-Against-Complex-Cyber-Threats. Diakses pada tanggal 6 Juli 2014.

United States General Accounting Office. Juni 2010. *Cybersecurity: Key challenges need to be addressed to improve research and development.* Diakses dari http://www.gao.gov/new.items/d10466.pdf. Diakses pada tanggal 15 Desember 2014.

UNODC. 2013. *Comprehensive Study on Cybercrime*. Diakses dari http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Diakses pada tanggal 25 Februari 2015.

U.S. Pasific Command. 2013. *Yama Sakura trains US and Japanese troops on Cyber Defense*. Diakses dari https://www.youtube.com/watch?v=7qND0roT5h8. Diakses pada tanggal 12 Januari 2015

USARPAC Public Affairs. 2013. "Yama Sakura 65". Diakses dari http://www.army.mil/article/116507/Yama_Sakura_65/. Diakses pada 12 Januari 2015

Wilson, Dean. 2011. *Japanese parliament is under cyber attack.* Diakses dari http://www.theinquirer.net/inquirer/news/2121964/japanese-parliament-cyber-attack. Diakses pada tanggal 23 Agustus 2014.