STRATEGI KEAMANAN *CYBER* AMERIKA SERIKAT

Dewi Triwahyuni[1)],
Tine Agustin Wulandari [2)]

[1] Program Studi Ilmu Hubungan Internasional Universitas Komputer Indonesia
[2] Program Studi Ilmu Komunikasi Universitas Komputer Indonesia

email: dewi.triwahyuni@email.unikom.ac.id
email: Tine.wulandari@email.unikom.ac.id

Abstract

The development of information technology has provided a significant shift from the concept of security. At present, countries are not limited to interact physically in real space but also extends to cyberspace. Consequently, the state must adapt to this development. nowadays the concept of cyber security should be established as one of the "territory" of the state which should be safeguarded as the state's obligation to secure its borders. Now the interaction between the actors of international relations is not only in the land, sea and air alone. The interaction between the actors also performed in the virtual space into other options to achieve the interests. This study aimed to test the importance of cyber security strategies in the foreign policy of the United States. Where the United States in the last 10 years is very intense spawned a cyber security strategy. This study uses qualitative research methods to get in-depth answers to the problems studied. The results showed that the United States has put cyber security as a top priority in its foreign policy. It is clearly mentioned in official documents and US security strategy. The United States realizes that it needs a comprehensive strategy to safeguard its national interests in the global world.

Keywords: Strategy, Cyber Security, United States

Abstrak

Perkembangan teknologi informasi telah memberikan perubahan yang signifikan dari konsep keamanan. Saat ini, negara-negara tidak terbatas untuk berinteraksi secara fisik dalam ruang nyata tetapi juga meluas ke dunia maya. Akibatnya, negara harus beradaptasi dengan perkembangan ini. saat ini konsep keamanan cyber harus ditetapkan sebagai salah satu dari "wilayah" negara yang harus dijaga sebagai kewajiban negara untuk mengamankan perbatasannya. Sekarang interaksi antara aktor-aktor hubungan internasional tidak hanya di darat, laut dan udara saja. Interaksi antara aktor juga dilakukan di ruang virtual ke pilihan lain untuk mencapai kepentingan. Penelitian ini bertujuan untuk menguji pentingnya strategi keamanan cyber dalam kebijakan luar negeri Amerika Serikat. Di mana Amerika Serikat dalam 10 tahun terakhir sangat intens menelurkan strategi keamanan cyber. Penelitian ini menggunakan metode penelitian kualitatif untuk mendapatkan jawaban yang mendalam terhadap permasalahan yang diteliti. Hasil penelitian menunjukkan bahwa Amerika Serikat telah menempatkan keamanan cyber sebagai prioritas utama dalam kebijakan luar negerinya. Hal ini jelas disebutkan dalam dokumen resmi dan strategi keamanan AS. Amerika Serikat menyadari bahwa itu memerlukan strategi yang komprehensif untuk melindungi kepentingan nasional dalam dunia global.

Kata kunci: Strategi, Cyber Security, Amerika Serikat

1. Pendahuluan

1.1. Latar Belakang

Perkembangan teknologi informasi dewasa ini mendorong pola-pola baru dalam interaksi hubungan internasional. Prilaku-perilaku internasional kini dilakukan tidak hanya secara aktual namun juga secara virtual. Dalam era teknologi informasi, khususnya perkembangan jaringan internet menambah luas sarana negara dalam mencapai kepentingan nasionalnya.

Kini interaksi yang dilakukan antar aktor hubungan internasional tidak hanya pada

ruang darat, laut dan udara saja. Interaksi antar aktor juga memadati ruang maya (*cyberspace*) yang menjadi pilihan lain untuk mencapai kepentingan. Bertambahnya ruang interaksi ini sekaligus memperluas makna *power* dalam hubungan antar negara. Ukuran *power* dalam ruang darat, laut, udara lebih mudah untuk dicari standarisasinya, sebaliknya *cyberspace* mengaburkan stadarisasi *power* tersebut. *Cyberspace* menjadi ruang sekaligus sarana baru dalam mencapai kepentingan yang kemudian dikenal dengan *cyberpower*.

Pada abad informasi, negara (atau bukan negara) negara yang berkuasa bukan lagi negara yang memiliki angkatan militer kuat saja, tetapi juga negara yang menjalin narasi terbaik. Kini, sulit untuk mengukur perimbangan kekuatan, terlebih bagaimana strategi bertahan yang berhasil. Negara akan tetap menjadi pelaku utama di panggung dunia. Namun, negara akan mendapatkan panggung yang lebih sesak dan sulit dikendalikan.

Fenomena ini dirasakan benar oleh Amerika Serikat (AS). Seluruh manusia, termasuk 315,256,801 juta jiwa (dalam http://www.census.gov/population/www/popclockus.html). Rakyat AS kini hidup di dunia yang berjejaring baik, seluler, komputer dan laman-laman sosial di internet. Namun jaringan-jaringan yang berbeda menghasilkan bentuk-bentuk kekuatan baru sehingga membutuhkan gaya kepemimpinan yang berbeda. Tantangan kepemimpinan ini direspon dengan baik oleh Barack Obama. AS sangat sadar bahwa untuk mempertahankan kekuasaannya di panggung internsional menuntut adaptasi yang baik dalam politik luar negerinya atas perkembangan konsep power tadi.

Respon AS terhadap kekuatan dunia maya diperlihatkan dalam garis besar Politik luar negeri AS yang terangkup dalam QDDR 2010. Dalam Dokumen tersebut dikatakan bahwa sudah saatnya Amerika Serikat melakukan adaptasi diplomasi untuk menjawab tantangan perkembangan dunia saat ini. AS akan membangun sebuah koordinasi untuk persoalan dunia maya (*cyber issues*) dan keamanan dunia maya, termasuk melakukan upaya-upaya untuk melindungi bagian terpenting dalam diplomasi: yaitu kenyamanan dan kerahasian komunikasi antar pemerintahan.

Keseriusan Amerika serikat menghadapi dunia *cyber* ini semakin jelas dengan dikeluarkannya formulasi kebijakan Internasional AS untuk *cyberspace*. Pengaturan secara rinci dan komprehensif mengenai bagaimana strategi AS menghadapi berbagai persoalan menyangkut *cyberspace*. Sejumlah formulasi dalam menghadapi ancaman yang datang dari *cyberspace* ini diantaranya:

1. *The National Strategy to secure Cyberspace*, dikeluarkan pada bulan Febuari 2003.
2. *International Strategy for Cyberspace*, dikeluarkan pada bulan Mei 2011.
3. *Departement of Defense Strategy for Operating in Cyberspace*, dikeluarkan Juli 2011.

Sejumlah formulasi strategi untuk keamanan *cyber* tadi dibuat oleh AS bukan tanpa sebab. Sejumlah peristiwa baik yang langsung menimpa AS maupun yang tidak secara langsung menimpa AS mempengaruhi lahirnya strategi keamanan *cyber* tersebut. Estonia pada tahun 2007 pernah mendapat serangan *cyber* secara masif terhadap infrastruktur sistem keamanan mereka.

Peristiwa ini cukup membuka mata dunia, termasuk AS sendiri, bahwa ancaman *cyber* tidak saja sebuah wacana lagi, bahkan menuntut penanganan militer untuk penanggulangannya. Tidak hanya negara, sejumlah perusahan-perusahan swasta multinasional, termasuk milik AS juga tidak luput dari serangan *cyber.* Tercatat google dan Adobe system pernah menjadi korban operasi Aurora pada tahun 2009. Pada tahun 2010,

serangan virus Stuxnet juga menjadi perbincangan dunia karena mampu melumpuhkan pembangkit listrik Bushehr.

AS juga sering diberitakan mengalami serangan *cyber* yang cukup mengancam kepentingan serta keamanan nasionalnya. Tingkok dan Rusia adalah negara yang paling sering "dituduh" oleh AS melakukan spionase bahkan meretas (*hacking*) terhadap sistem informasi baik infrastruktur pemerintah sampai perusahaan swasta.

Latar belakang inilah yang mendorong peneliti untuk mengangkat tema ini menjadi penelitian. Fokus penelitian ini adalah untuk melihat urgensitas serta pelaksanaan strategi keamanan *cyber* tersebut dalam politik luar negeri Amerika Serikat.

1.2. Rumusan Masalah

a. Apa kepentingan utama Amerika Serikat membangun strategi keamanan *cyber*?
b. Bagaimana strategi keamanan *cyber* dilaksanakan dalam politik luar negeri Amerika Serikat ?

2. Kajian Pustaka dan Kerangka Pemikiran

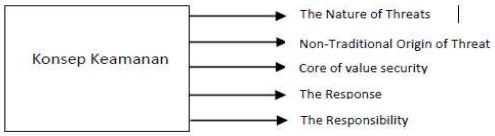
2.1. Konsep Strategi Keamanan

Pengkajian keamanan internasional telah mengalami perkembangan yang signifikan. Pemahaman konsep keamanan pasca perang dingin tidak lagi sempit sebagai hubungan konflik atau kerjasama antar negara, tetapi juga berpusat pada keamanan untuk masyarakat (lihat Perwita & Yani, 2005: 119).

Arnold Wolfers dalam Perwita & Yani mendefinisikan keamanan sebagai berikut, *"security, in any objective sense, measures the absence of threats to acquired values and in a subjective sense, the absence of fear that such values will be at tacked* (2005: 121)*"*.

Steven Spiegel dalam Winarno, mengatakan bahwa perluasan definisi keamanan nasonal mempunyai konsekuensi akan memperbesar ancaman: nuklir, ekonomi, sosial dan budaya. Konsep keamanan tersebut dapat digambarkan sebagai berikut (2014:10):

Gambar 2.1 Konsep Keamanan



Gambar 1 diatas menunjukan bahwa jika ditinjau dari dimensi the origin of threats (sumber ancaman) maka ancaman dapat berasal dari domestik/dalam negeri contoh: isu-isu primordial yang berkaitan dengan ras, suku, kelompok dan agama. Ancaman juga dapat berasal dari lingkungan global, yang dilakukan oleh aktor-aktor negara maupun non negara. Dimensi berikutnya adalah *Nature of threats*, jika ancaman terhadap keamanan tradisional bersifat militer. Namun seiring berkembangnya zaman ancaman menjadi jauh lebih rumit tidak sekedar bersifat militer, melainkan muncul ancaman yang bersifat non militer, atau berkaitan dengan aspek ekonomi, sosial budaya, lingkungan hidup, HAM dan persoalan keamanan lainnya yang lebih komprehensif (Spiegel dalam Winarno, 2014: 11).

Sementara itu, Strategi oleh John P. Lovell (dalam Mas'oed, 1989: 90) diartikan sebagai "serangkaian langkah-langkah atau keputusan-keputusan yang dirancang sebelumnya dalam situasi kompetititf dimana hasil akhirnya tidak semata-mata bersifat untung-untungan. Strategi adalah cara yang digunakan untuk mencapai suatu tujuan atau kepentingan dengan menggunakan power yang tersedia, termasuk juga kekuatan militer.

Dalam politik luar negeri, strategi merupakan pola perencanaan yang digunakan para pembuat keputusan untuk memajukan serta mencapai kepentingan-kepentingan

nasionalnya dengan disertai usaha mencegah engara lain melakukan tabrakan atau menghambat tercapainya kepentingan itu.

Ada tiga asumsi dari teori strategi (Mas'oed, 1989: 90-91):

1. Perilaku politik luar negeri suatu negara-bangsa pasti diarahkan sebagai langkah untuk mencapai satu atau beberapa tujuan kepentingan tersebut.
2. Par pembuat keputusan selalu berusaha memaksimalkan perolehan bagi negara-bangsanya dengan menelaah berbagai alternatif tindakan yang masing-masing dinilai berdasarkan analisis biaya dan hasil.
3. Dalam dunia ini saling bergantung sehingga keputusan harus memperhitungkan tujuan dan strategi negara-bangsa yang lainnya.

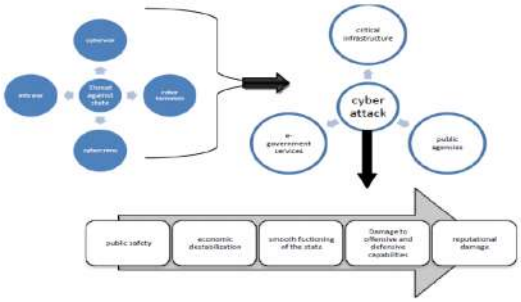
2.2. Memahami Cyber dalam Konteks Keamanan Nasional

Ada banyak terminologi dan interpretasi yang dihubungkan dengan konsep "*cyber security"* atau "keamanan *cyber"*. Karena c*yberspace* merupakan ruang virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi. Teknologi yang dimaksud ialah teknologi informasi dan komunikasi (Sitompul, 2012: 15). Maka konsep keamanan cyber tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadi ancaman terhadap keamanan nasional.

Sebelumnya, diskusi tentang keamanan nasional sangat jarang dihubungkan dengan teknologi. Namun, seiring dengan meningkatnya ancaman serangan *cyber* domestik dan intenasional pada infrastruktur publik dan swasta AS setelah berlalunya peristiwa 9/11, maka muncul kesadaran untuk mempopulerkan bahwa keamanan dunia maya bukanlah sekedar persoalan proteksi *password* yang sederhana (dalam http://www.ciso.co.id/2013/10/cyber-security-awareness-perguruan-tinggi-dan-ancaman-digital/ diakses pada 29 April 2015). Keamanan *cyber* lebih jauh membutuhkan serangkaian strategi karena menyangkut kepentingan nasional.

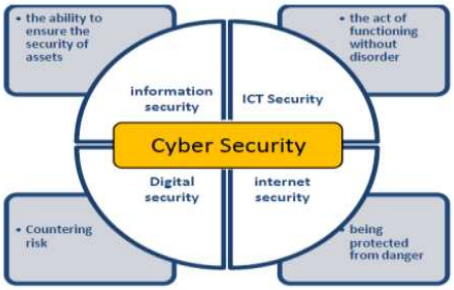
Perkembangan teknologi informasi juga telah memberikan perubahan signifikan mengenai konsep keamanan, kini ruang interaksi tidak bisa hanya dibatasi seara fisik (*physic*) tapi juga meluas ke dunia maya (*cyber*). Konsekuensinya, negara harus beradaptasi dengan perkembangan ini konsep keamanan dunia maya (*cyber security*) sudah saatnya ditetapkan sebagai salah satu "wilayah" negara yang jaga keamanannya sebagaimana kewajiban negara mengamankan teritorialnya. Apalagi, serangan cyber tidak hanya terjadi pada institusi publik saja, namun juga menyerang institusi pemerintah. Gambaran serangan cyber dapat diilustrasikan seperti dibawah ini (Ghernaouti, 2013:126):

Gambar 2.2 Kejahatan melawan institusi negara dan publik



Keamanan *cyber* ditujukan pada isu keamanan informasi bagi pemerintahan, organisasi dan urusan individual yang dihubungkan dengan teknologi ICT, dan secara khusus dengan teknologi internet (Ghernaouti, 2013:329). Keamanan *cyber* tidak dapat diabstraksikan terlalu jauh dari wilayah aplikasinya dan lingkungan sosial-kultural (Lihat gambar dibawah ini).

Gambar 2.3 Konsep *Cyber Security*



Terminologi "keamanan informasi (*information security*)" dan keamanan *cyber* adalah dua konsep berbeda. Dalam konteks tertentu ada kesamaan pemahaman jika dikaitkan dengan proteksi aset atau perlawanan terhadap spionase industri dan ekonomi, perlawanan terhadap terorisme atau kejahatan ekonomi, perlawanan tehadap konten-konten terlarang (Ghernaouti, 2013: 330).

Dalam konteks lain, dua konsep tadi memiliki perbedaan. Keamanan cyber mencakup segala sesuatu berhubungan dengan pengawasan komputer, monitoring sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental.

Sedangkan keamanan informasi berhubungan dengan isu-isu yang lebih luas, seperti kedaulatan negara, keamanan nasional, proteksi atas infrastruktur penting, keamanan aset-aset yang terlihat maupun yang tidak terlihat, dan proteksi data personal dan sebagainya (Ghernaouti, 2013: 330).

1.3. Politik Luar Negeri

Politik luar negeri pada dasarnya merupakan kebijakan suatu negara yang ditujukan kepada negara lain untuk mencapai suatu kepentingan tertentu. Secara umum, politik luar negeri merupakan suatu perangkat formula nilai, sikap dan arah serta sasaran untuk mempertahankan, mengamankan, dan memajukan kepentingan nasional di dalam percaturan dunia internasional (Perwita & Yani, 2005: 47).

Secara umum politik luar negeri dapat dikatakan sebagai kebijakan yang diambil oleh pemerintah suatu negara atau komunitas politik lainnya baik dalam hubungan dengan negara, maupun aktor bukan negara di kancah internasional. Politik Luar Negeri menjembatani batas wilayah dalam negeri dan lingkungan internasional. Politik Luar Negeri itu bisa berupa hubungan diplomatik, mengeluarkan doktrin, membuat aliansi, dan mencanangkan tujuan jangka panjang maupun jangka pendek (Holsti dalam Hara, 2011: 13).

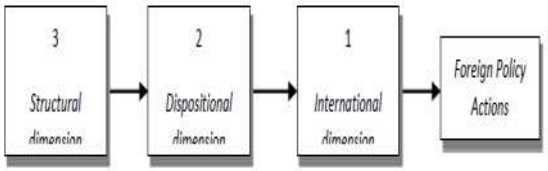
Politik luar negeri merupakan sistem tindakan-tindakan dari suatu pemerintah terhadap pemerintahan lainnya. Menurut Columbis & Wolf, Politik luar negeri adalah sekumpulan kebijakan yang berperan danberpengaruh, dalam hubungansuatu negara (pemerintah) dengan negara (pemerintahan) lainnya, dengan (pemerintahan) lainnya, dengan mempertimbangan juga tanggapan (respon terhadap kejadian dan masalah di lingkungan dunia internasional). Dengan kata lain politik luar ngeri merupakan sintesa dari pengerjawantahan tujuan dan kemampuan (kapabilitas) nasional (1990: 89-90).

Sedangkan menurut Walter Carlnaes dalam Hara mempertegas pengertian Politik Luar Negeri sebagai : "Tindakan –tindakan yang diarahkan ke tujuan kondisi dan aktor (baik pemerintah maupun non-pemerintah) yang berada diluar di wilayah teritorial mereka dan yang ingin mereka pengaruhi. Tindakan-tindakan itu diekspresikan dalam bentuk tujuan-tujuan, komitmen dan/atau arah yang dinyatakan secara eksplisit, dan yang dilakukan oleh wakil-wakil pemerintah yang bertindak atas nama negara/komunitas yang berdaulat" (2011: 13).

Definisi lain mengenai politik luar negeri menurut Valerie M. Hudson yaitu: "*the strategy or approach chosen by the national government to achieve its goal in its relations with external entities. This includes decisions to do nothing (2008: 11-12)".*

Berdasarkan definisi-definisi ini, fokus utama kajian politik luar negeri adalah untuk memperhatikan intensi (maksud), pernyataan dan tindakan aktor yang diarahkan pada dunia eksternal dan respon dari aktor-aktor lain terhadap instansi, pernyataan dan tindakan ini (Gerner dalam Hara, 2011: 14).

Gambar 2.4 ***Three dimensions for explaining foreign Policy actions***



Ada dimensi-dimensi yang mempengaruhi tindakan politik luar negeri. Dimensi struktural, dimensi disposisional, dan dimensi internasional atau yang datang dari lingkungan global (lihat gambar 2.4). Dimensi-dimensi tersebut saling memberikan pengaruh sehingga lahirlah sebuah tindakan sebagai implementasi dari sebuah politik luar negeri.

3. Objek dan Metode Penelitian

3.1. Metode Penelitian

Penelitian ini menggunakan metode penelitian kualitatif. Strauss & Corbin dalam Sujawerni mendefinisikan penelitian kualitatif sebagai jenis penelitian yang menghasilkan penemuan-penemuan yang tidak dapat dicapai (diperoleh) dengan menggunakan prosedur-prosedur statistik atau cara-cara lain dari kuantifikasi (pengukuran). Penelitian kualitatif secara umum dapat digunakan untuk penelitian tentang kehidupan masyarakat, sejarah, tingkah laku, fungionalisasi organisasi, aktivitas sosial dan lain-lain (2014: 19). Alasan pemilihan metode kualitatif adalah untuk menjawab rumusan masalah penelitian.. Melalui penelitian ini diharapkan diperolehnya informasi dan data yang relevan untuk menjawab Apa kepentingan utama AS membangun strategi keamanan *cyber* dan bagaimanan strategi tersebut dilaksanakan dalam politik luar negeri AS.

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah triangulasi, dimana menggunakan kombinasi teknik pengumpulan data secara simultan seperti :

(i) Studi Pustaka

Studi Pustaka dilakukan karena banyaknya informasi dan data mengenai Strategi Keamanan *Cyber* Amerika Serikat. Hal ini dapat ditelusuri melalui berbagai informasi dalam buku, jurnal ilmiah, koran, majalah, serta sumber informasi dari laman situs/website melalui internet. Studi pustaka menjadi penting dalam menganalisa konsep Strategi, Keamanan *Cyber* dan Politik Luar Negeri Amerika Serikat.

(ii) **Dokumentasi Penelitian**.

Teknik ini digunakan untuk menganalisa sumber informasi yang tersedia dari dokumen-dokumen resmi seperti dokumen-dokumen kebijakan mengenai strategi keamanan *cyber* Amerika Serikat serta dokumen-dokumen mengenai formulasi politik luar negeri Amerika Serikat.

(iii) Rekam Jejak.

Teknik ini digunakan untuk memperoleh dan menganalisa rekam jejak dan informasi terumatama yang berkenaan dengan keamanan *cyber*, seperti data mengenai sejak kapan masalah keamanan *cyber* menjadi prioritas dan perhatian pemerintah Amerika Serikat dan bagaimanan strategi keamanan cyber tersebut dijalankan dalam politik luar negeri Amerika Serikat.

(iv) Wawancara.

Teknik ini digunakan untuk memperoleh data secara mendalam dari informan sebagai pihak yang berwenang dan memiliki kapasitas berkenaan dengan penelitian.

Setelah pengumpulan data dilakukan maka dilakukan analisa data. Dalam analisa kualitatif terdiri dari tiga alur yaitu reduksi data, data *display* dan kesimpulan. Dalam prosesnya, analisa data dilakukan dengan menganalisa semua data yang diperoleh dari berbagai sumber. Setelah itu diperoleh inti dari jawaban permasalahan dan hasil wawancara yang diperoleh dari informan akan memudahkan pengambilan kesimpulan penelitian.

4. Hasil Dan Pembahasan

4.1. Arti Penting Keamanan Cyber Bagi Amerika Serikat

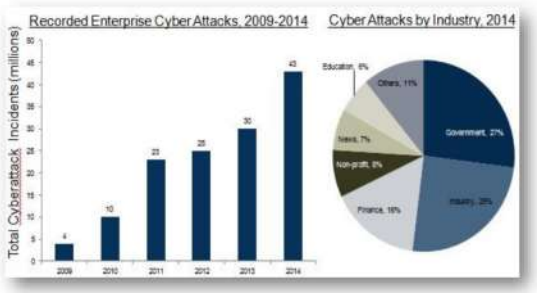
Pemerintah Amerika Serikat (AS) telah memperlihatkan keseriusannya dalam membangun system keamanan informasinya. Hal ini tentu saja berkaitan erat dengan ketergantungan pemerintah AS yang sangat besar terhadap jaringan keamanan sistem informasi. Keamanan dunia maya telah menjadi prioritas bagi kebijakan politik domestik AS mengingat eksistensinya yang sangat vital.

Pemerintah AS membangun jaringan sistem keamanan informasi dalam bidang militer, agraria, sistem pengaturan lalu lintas, air dan sanitasi, energi dan transportasi. Aspek vital tersebut sangat tergantung pada peranan komputer dan dunia maya. Oleh karena itulah, pemerintah AS melakukan pembaharuan untuk standardisasi *cyber security*. Bila sistem keamanan informasi tersebut diretas, secara otomatis negara AS akan lumpuh dan mengakibatkan dampak yang serius (Rahmadhan, http://www.Ciso.co.id).

Keseriusan AS membangun sistem keamanan cyber khususnya pada era kepemimpinan Barack Obama merupakan respon pemerintah atas masukan serta kritikan masyarakat AS tentang lemahnya jaringan keamanan sistem infomasi di Negara Adi daya tersebut. Kondisi ini dapat dilihat dari catatan sejumlah serangan cyber yang dialami AS dalam 10 tahun terakhir. Antara lain serangan retasan terhadap Sony Pictures Entertainment, Anthem Insurance, Target, Home Depot, eBay dan JPMorgan Chase. Pemerintah federal juga pernah mengalami serangan dunia maya, termasuk retasan komputer *unclassified* di Gedung Putih dan Departemen Luar Negeri dan peretasan akun Twitter dan YouTube milik komando militer AS (Http://www.voaindonesia.com).

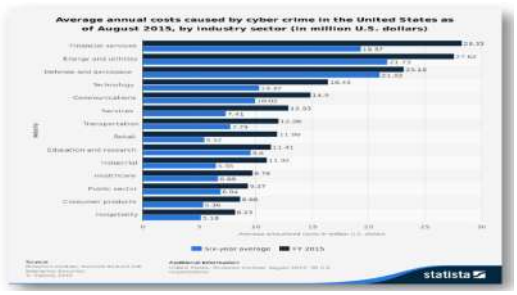
Amerika Serikat memiliki cukup alasan untuk menempatkan keamanan cyber sebagai salah satu prioritas utama keamanan negaranya. Dilihat dari data serangan cyber yang dialami AS sejak 2009 – 2014 (gambar 4.1) persentase serangan tertinggi justru terjadi pada wilayah pemerintahan (27%) dan dunia industry (25%) hal ini tentu saja merupakan wilayah vital negara.

Gambar 4.1. Data Serangan cyber terhadap Amerika Serikat



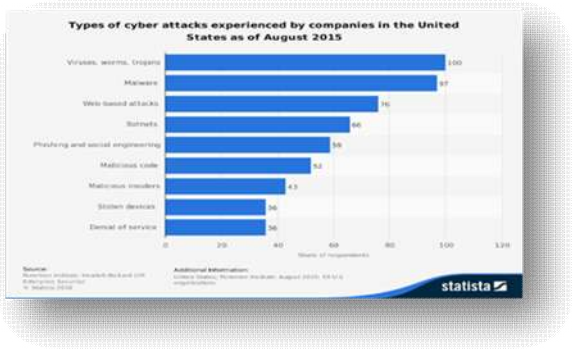
Sementara itu, dunia industry yang paling sering menjadi sasaran serangan kejahatan cyber adalah pada sektor jasa keuangan (gambar 4.2), hal ini tentu saja menjadi perhatian yang sangat besar mengingat jasa keuangan memegang wilayah yang sangat strategis dalam industry Amerika Serikat.

Gambar 4.2. Rata-rata Kerugian akibat Kejahatan Cyber dalam Sektor Industri



Hal yang lain yang membuat keamanan cyber menjadi perhatian sangat penting adalah tingkat kesulitan dalam menanggulanginya. Bentuk serangan yang beragam mulai dari bentuk virus, penyerangan terhadap situs, hacker dan lain sebagainya merupakan sebuah tantangan bagi departemen pertahanan dalam menciptakan keamanan karena berhadapan dengan musuh yang sulit diidentifikasi kehadirannya, sumber serangannya dan bentuk serangannya. Berbagai bentuk serangan cyber yang pernah dialami Amerika Serikat dapat dilihar dari gambar berikut ini:

Gambar 4.3 Tipe-tipe Serangan Cyber yang dihadapi perusahan di Amerika Serikat



4.2. Strategi Keamanan Cyber Amerika Serikat

Prioritas *cyber* dalam politik luar negeri AS ini semakin diperkuat dengan dirilisnya dokumen "*International Strategy for Cyberspace*" pada tahun yang sama (2011). Strategi ini merupakan strategi pertama yang dikeluarkan AS yang menghubungkan dan mengikat AS dengan seluruh dunia dalam isu *cyber* yang sangat luas. Strategi ini juga merupakan panduan AS dalam menghadapi semua tantangan keamanan teknologi informasi dalam dunia *cyber*. Oleh karena itu pada April 2015, Departemen Pertahanan AS mengeluarkan "*The Departement Of Defense (DoD) Cyber Strategy*" untuk menjawab pada wilayah apa dan bagaimana lembaga pertahanan AS tersebut harus mensukseskan tujuan-tujuan serta prioritas yang tertuang dalam *International Strategy for Cyberspace 2011*.

Prioritas keamanan *cyber* pada pemerintahan Barack Obama saat ini antara lain:

1. Menjaga Infrastruktur penting Negara dan sistem informasi penting Negara dari ancaman *cyber*.
2. Meningkatkan kemampuan untuk mengindentifikasi dan melaporkan peristiwa-peristiwa *cyber* agar dapat merespon diwaktu yang tepat
3. Mengajak dunia untuk mempromosikan *internet freedom* dan membangun dukungan bagi ruang *cyber* yang terbuka, mudah dioperasikan, aman dan terpercaya.
4. Mengamankan jaringan pemerintah pusat dengan menyusun target keamanan yang jelas dan menempatkan agen pemerintah yang akuntabel untuk dapat memenuhi target tersebut.
5. Membentuk kekuatan yang sangat memahami cyber dan bergerang melebihi kata sandi dalam kemitraan dengan sector privat. (https://www.whitehouse.gov/issues/foreign-policy/cybersecurity)

Kesadaran untuk mengembangkan keamanan *cyber* dan mempersiapkan strategi dalam menghadapi ancaman dan tantangan dunia digital sudah sejak lama disadari oleh AS. Namun intensitas pengembangan *cyberpower* sangat terlihat dalam kebijakan-kebijakan pemerintah AS kurang lebih dalam 10 tahun terakhir. Berikut beberapa kebijakan keamanan c*yber* yang dirilis oleh pemerintah AS dalam 10 tahun terakhir:

Tabel 5.1. Daftar Kebijakan *Cyber* Amerika Serikat

Tahun	Nama Dokumen	Lembaga Penerbit
2003	*The National Strategyto Secure Cyberspace*	Gedung Putih
2009	*Cyberspace policy Review*	Gedung Putih
2011	*International Strategy for Cyberspace*	Gedung Putih
2011	*Department of Defense Strategy for Operating Cyberspace*	Departemen Pertahanan Amerika Serikat
2015	*The Department of Defense Cyber Strategy*	Departemen Pertahanan Amerika Serikat
2016	*Department of State International Cyberspace Policy Strategy*	Departemen Luar Negeri Amerika Serikat

Dari tabel diatas sangat jelas terlihat keseriusan pemerintah AS dalam mengembangkan keamanan *cyber*. Presiden Barack Obama pada tahun 2009 menyatakan bahwa infrastruktur digital Amerika adalah aset nasional. Pada bulan Mei 2010 Pentagon meluncurkan *US Cyber Command (USCYBERCOM)* untuk melindungi jaringan militer Amerika dan melakukan penyerangan. Sementara untuk jaringan pemerintahan dan korporasi dilindungi oleh *Department of Homeland Securit*y. Untuk mengantisipasi perang *cyber* di amerika dibentuk *DC3 (Defense Cyber Crime Center)* pada tahun 2008, *US Cyber Command* (2009), *Homeland Security* (utk non militer), serta penelitian untuk menciptakan senjata perang *cyber* oleh DARPA.

Dari serangkaian kebijakan AS mengamankan ruang *cyber,* yang *sangat* bersentuhan dengan Politik Luar Negeri adalah "*U.S International Strategy For Cyberspace"*. Strategi ini merupakan sebuah formulasi khusus yang dikeluarkan oleh Gedung Putih sebagai *international code of conduct* AS dalam persoalan *cyber* di hubungan internasional. AS sangat memahami bahwasanya dunia masih belum memiliki pengaturan yang jelas mengenai ruang cyber. Situasi ini tidak sedikit dimanfaatkan oleh beberapa Negara untuk bertindak sewenang-wenang di ruang cyber. Beberapa Negara yang dideteksi AS mengancam kepentingan nasional AS melalui tindakan ruang cyber antara lain: Tiongok dan Rusia.

Gambar 5.1. Penggunaan Kata "Cyber" dalam Strategi Internasional AS untuk ruang cyber (2011)

U.S International Strategy For Cyberspace mengatur strategi AS baik jangka pendek maupun jangka panjang dalam menghadapi era perang digital di dunia. Melalui strategi ini, AS akan mengejar kebijakan internasional untuk ruang cyber dan memberdayakan berbagai inovasi yang telah terbukti mendorong majunya ekonomi dan peningkatan hidup masyarakat AS dan masyarakat dunia umumnya. Untuk itulah AS menyatakan akan teguh terhadap prinsip-prinsip dasar yang berlaku tidak saja untuk lebijakan luar negeri AS tetapi untuk masa depan internet itu sendiri. Beberapa strategi pendekatan yang dibangun AS melalui strategi keamanan internasional ruang *cyber* AS antara lain:

Tabel 5.2. Strategi Pendekatan dalam *U.S International Strategy for Cyberspace*

Strategic Approach	*1. Building on Successes*	AS berkomitmen untuk memilihara dan meningkatkan keuntungan dari jaringan digital bagi masyarakat dan ekonomi.
	2. Recognizing the challenges	AS menyadari bahwa pertumbuhan jaringan-jaringan ini datang bersama dengan tantanganya terhadap keamanan ekonomi Negara dan masyarakat global.
	3. Grounded in Principle	AS akan melawan semua tantangan ini dalam waktu bersamaan juga mempertahankan prinsip-prinsip utama Negara.

Dalam rangka memperkuat Strategi Nasional tersebut, maka secara teknis langkah-langkah strategi telah disusun oleh *Departement Of Defense (DoD)* yang disebut sebagai Strategi inisiatif. Strategi ini disusun untuk keamanan dunia maya yang menjadi tugas dari Departemen Pertahanan Amerika Serikat. Strategi tersebut antara lain;

1) *Strategi inisiatif 1*: Memperlakukan ruang *cyber* sebagai sebuah wilayah operasional yang harus dikelola, dilatih dan dilengkapi sehingga Departemen Pertahanan AS dapat memanfaatkan potensi dari ruang *cyber* itu sendiri.
2) *Strategi inisiatif 2:* Mengembangkan system operasi pertahanan baru untuk melindungi system dan jaringan Departemen Pertahanan AS.
3) *Strategi inisiatif 3:* Bermitra dengan departemen / agen-agen pemerintah maunpun dengan sektor swasta untuk melaksanakan seluruh strategi ruang *cyber*.
4) *Strategi inisiatif 4:* membangun hubungan yang kuat dengan para sekutu AS dan patner internasional lainnya untuk memperkuat keamanan kolektif *cyber*.
5) Strategi inisiatif 5: Departemen pertahanan akan mempengaruhi kecerdasan bangsa dengan kemampuan istimewa dalam dunia *cyber* dan inovasi teknologi yang sangat cepat (*DOD Strategy for Operating in Cyberspace, Juli 2011*).

Untuk mendukung misi pengamanan dunia cyber tersebut, maka departemen pertahanan AS (DoD) melakukan berbagai aktifitas diluar duni cyber untuk mrngembangkan keamanan kolektif cyber dan dalam upaya menjaga kepentingan nasional AS. Sebagai contoh, DoD bekerjasama dengan agensi pemerintah, sektor privat, dan juga dengan patner internasional dalam pertukaran informasi, membangun aliansi dan partnership serta mengembangkan norma prilaku bertanggung jawab untuk meningkatkan stabilitas global.

Dalam rangka mendukung aktifitas-aktifitas diatas, maka dirumuskanlah 3 (tiga) Misi utama Departemen Pertahanan AS untuk dunia cyber:

1) DoD harus menjaga jaringan, sistem dan informasinya sendiri. Departemen pertahanan harus dapat mengamankan jaringannya dari serangan dan memulihkan sistem secara cepat jika pengamanan gagal.
2) DoD harus mempersiapkan diri untuk menjaga AS dan semua kepentingannya melawan serangan *cyber* yang memberikan dapak signifikan.
3) Dengan dipimpin oleh Presiden dan Menteri Pertahanan, DoD harus mampu untuk menciptakan kapabilitas *cyber*

yang terintegrasi untuk mendukung operasi militer dan rencana-rencana yang akan dicapai kedepannya (The DoD Cyber Strategy 2015: 4-6)

Ketiga misi utama ini dapat dicapai melalui 5 (lima) tujuan strategis, antara lain:

1) *Strategic Goal I : Build and maintain ready forces and capabilities to conduct cyberspace operations;*
   Untuk dapat beroperasi secara efektif di dunia cyber, DoD membutuhkan dukungan tenaga individual dan tentara yang terlatih dengan standar tinggi. Untuk itu DoD harus melakukan investasi besar dengan memberikan pelatihan kepada tentara, membangun organisasi yang efektif.
2) *Strategic Goal II : Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;*
   DoD harus memulai dengan melakukan identifikasi, membuat prioritas dan mempertahankan jaringan dan data terpenting sehingga dapat melaksanakan tujuan misi dengan efektif. DoD harus terus mengembangkan teknologi untuk tetap lebih terdepan dalam menghadapi ancaman dengan memperbesar kemampuan pertahanan cyber.
3) *Strategic Goal III : Be prepare to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;*
   DoD harus bekerja antar patner, mulai dari sektor swasta, dan aliansi termasuk dengan patner Negara lain untuk menangkal dan jika dibutuhkan melumpuhkan serangan cyber yang memberikan dampak signifikan atas kepentingan AS.
4) *Strategic Goal IV : Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environtment at all stages;*
   DoD harus membangun sistem cyber yang berkelanjutan dan terintegrasi dengan rencana-rencana lembaga yang berkaitan. DoD akan mengembangkan kemampuan cyber untuk mencapai tujuan dari keamanan kunci.
5) *Strategic Goal V : Build and maintain robust international alliances and patnerships to deter shared threats and increase international security and stability.*
   Ketiga misi Keamanan cyber DoD membutuhkan kolaborasi dengan sekutu asing dan patner lainnya. Dalam keterikatan dengan dunia cyber internasional, DoD harus membangun kapasitas kerjasama dalam keamanan cyber, pertahanan cyber, dan memperdalam hubungan kerjasama tersebut.

5. Kesimpulan dan Rekomendasi

Amerika Serikat merupakan Negara yang sangat serius membangun kekuatan *cyber* nya. AS menempatkan ruang *cyber* sebagai ruang baru dalam politik luar negerinya dan mendapatkan perhatian yang sama pentingnya dengan ruang darat, laut dan udara dalam kebijakan keamanan negaranya.

Karena itulah sejumlah formulasi kebijakan dan strategi untuk keamanan ruang *cyber* telah dirilis pemerintah Amerika Serikat. Hal ini dilakukan selain untuk membangun pertahanan *cyber* yang mumpuni dalam menjawab tantangan era digital, sekaligus dalam rangka mengantisapi kekosongan aturan ruang *cyber* di dalam hukum internasional.

Daftar Pustaka

Acuan dari buku:

Columbis, Theodore A. & Wolf, James. 1990. *Pengantar Hubungan Internasional: Keadialan dan Power*, Bandung: CV. Abardin.

Cyber Security Awareness: Perguruan Tinggi dan Ancaman Digital. http://www.ciso.co.id/2013/10/cyber-

security-awareness-perguruan-tinggi-dan-ancaman-digital/

Ghernaouti, Solange. 2013. *Cyber Power : Crime, Conflict and Security in Cyberspace*. Lausanne: EPFL Press.

Hara, Abubakar Eby. 2011. *Pengantar Analisis Politik Luar Negeri: dari Realisme sampai Konstruktivisme*. Bandung: Nuasana Cendikia.

Hudson, Valerie M. 2008. "The History and Evolution of Foreign Policy," dalam *Steve Smith, Amelia Hadfield dan Tim Dunne (eds), Foreign Policy: Theories, Actors, Cases*. New York: Oxford University Press.

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

Perwita, Anak Agung Banyu & Yani, Yanyan A. 2005. *Pengantar Ilmu Hubungan Internasional*. Bandung: Rosdakarya.

Sitompul, Josua. 2012. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: PT. Tatanusa.

Sujarweni, V. Wiratna. 2014. *Metode Penelitian: Lengkap, Praktis, dan Mudah Dipahami*. Yogyakarta: Pustaka Baru Press.

Winarno, Budi. 2014. *Dinamika Isu-isu Global Kontemporer*.Yogyakarta: CAPS (Center of Academic Publishing Service).

Acuan dari dokumen:

Departement of Defense Strategy for Operating in Cyber Space.

U.S. International Strategy for Cyberspace

The Department of Defense (DoD) Cyber Strategy

Cyberspace Policy Revie.