PENGARUH *CYBER SECURITY STRATEGY* AMERIKA SERIKAT MENGHADAPI ANCAMAN *CYBER WARFARE*

Oleh: Moehammad Yuliansyah Saputera[1]
Pembimbing : Drs. Tri Joko Waluyo, M.si
Email and Phone : yuliansyah.saputera@yahoo.com/ +6281277870445
Bibliografi : 6 Jurnal, 11 Buku, 12 Situs Internet

Jurusan Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Riau

Kampus Bina Widya km. 12,5 Simpang Baru-Pekanbaru 28293 Telp. (0761) 63277, 23430

Abstract

This research describes United States of America's Cyber Security Strategy facing the cyber warfare threads from 2009 till 2014. The main goals are securing cyber vital infrastructures and digital informations of United States. Vital infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, postal and shipping, internet network, and many others.

The method that is used in this research is qualitative research. Some of the datas are obtained from books, journals, articles, internet and other media. This research focuses on the influence of United State's cyber security strategy facing cyber warfare threads. Using strategy theory and securitization theory, this research will find out if US government successes to secure their cyber environment or not.

Cyber warfare is a thread, it can be a trigger to the physical war. Cyber attackers can compromise other computers or networks to use as intermediaries, or channel through anonymizing proxies that hide their Internet protocol (IP) address. Also, using underground internet or deep web can penetrate enemy's database. Through the intelligence agencies, United States applied it. It has multy functions. Can be a tool for defense or securing cyberspace and also can be a tool to attack.

Keywords: *Cyber Security Strategy, Cyber Warfare, Deep Web.*

[1] Mahasiswa Jurusan Ilmu Hubungan Internasional Universitas Riau Angkatan 2011

PENDAHULUAN

Penelitian ini membahas pengaruh Cyber Security Strategy Amerika Serikat menghadapi ancaman Cyber Warfare tahun 2009-2014. Pada saat ini, kemajuan di bidang teknologi informasi dan komunikasi (TIK) telah merubah wajah dunia serta sekaligus menggeser pemahaman terhadap suatu kekuatan (*power*) atau kedaulatan dari *s*uatu negara. Kekuatan atau kedaulatan suatu negara saat ini tidak hanya semata-mata dinilai dari seberapa besar kekuatan militer atau ekonomi yang dimilikinya, tetapi juga tergantung dari penguasaan dan pemanfaatan TIK nya. Hal ini disebabkan karena pada abad ke-21 atau sering disebut abad informasi, hampir seluruh aktivitas mulai dari aktivitas personal hingga pemerintahan tidak terlepas dari pemanfaatan, pemberdayaan, dan pengimplementasian TIK.

Perkembangan TIK yang sangat pesat di berbagai belahan dunia juga berimbas kepada semakin canggih dan variatifnya bentuk-bentuk ancaman terhadap keamanan (*national security*) dan kedaulatan sebuah negara. Untuk menghadapi dan mengantisipasi situasi dan kondisi tersebut diperlukan pembekalan pengetahuan TIK yang tinggi dan komprehensif bagi para penegak dan penjaga kedaulatan negara di bidang TIK. Pesatnya perkembangan ilmu hubungan internasional tidak terlepas dari perkembangan teknologi informasi dan komunikasi (TIK), berdasarkan teknologi inilah globalisasi terealisasi. Sebagai sebuah proses, globalisasi berlangsung melalui dua dimensi dalam interaksi antar bangsa, yaitu dimensi ruang dan waktu.[2] Ruang makin dipersempit dan waktu makin dipersingkat dalam interaksi dan komunikasi pada skala dunia. Sesuai dengan pendapat Sofyan Djalil[3] yang mengatakan bahwa perkembangan TIK menyebabkan terciptanya lalu lintas informasi dan komunikasi bebas hambatan antar negara dan wilayah. Dengan kata lain, keberadaan TIK mampu menghilangkan berbagai hambatan geografis sehingga terjadi transformasi pola hidup manusia di berbagai bidang menuju masyarakat berbasis ilmu pengetahuan atau *knowledge-based society*.

Namun, tidak dapat dihindari laju perkembangan TIK juga banyak digunakan untuk berbagai tujuan yang kontra produktif, bahkan destruktif, baik oleh perorangan *(individuals)*, kelompok *(non-state actors)* atau bahkan oleh satu negara *(state actors).* Mereka mengeksploitasi informasi guna menyebarluaskan pengaruh dan dominasinya di dalam peperangan informasi *(Information Warfare / Cyber Warfare*). Di era *cyber* saat ini, penguasaan dan pemanfaatan TIK yang destruktif pada dasarnya juga merupakan ancaman bagi keamanan serta ketahanan nasional suatu bangsa. Ketidakmampuan menghadapi era *cyber* dapat menjadi ancaman apabila suatu bangsa dan negara tidak memiliki kapabilitas atau kemampuan untuk memanfaatkan TIK secara baik, benar dan tepat guna. Berdasarkan hal itulah diperlukannya *cyber security* dan *cyber defense* dalam sebuah negara.

Cyber security atau keamanan dunia maya adalah proteksi perlindungan dunia maya dari sumber-sumber bahaya. Sedangkan *Cyber defense* atau pertahanan dunia maya adalah segala bentuk usaha untuk mempertahankan keamanan *cyber* atau dunia maya. *Cyber Security* berbeda dengan *security* atau keamanan biasa karena ancaman *cyber* tidak bisa dimasukan begitu saja ke dalam kategori keamanan tradisional.[4] Selain berasal dari dalam negeri, ancaman *cyber* atau *Cyber Threats* juga datang dari luar negeri. Namun, ancaman ini jarang mencapai taraf yang membutuhkan respon militer karena apapun yang akan dilakukan pemerintah dalam menanggapi ancaman *cyber* ini akan memiliki implikasi domestik dan internasional.

Amerika Serikat merupakan salah satu negara besar yang memiliki kapabilitas untuk menguasai serta memanfaatkan TIK dalam kehidupan sehari-hari maupun dalam bernegara. TIK sudah "mendarah-daging" bagi Amerika, setiap sektor baik dari sektor yang kecil hingga infrastruktur yang vital telah sangat bergantung pada teknologi yang berbasis jaringan ini. Ketergantungan pada teknologi jaringan secara

[2] Krisna. 2005. *Pengaruh Globalisasi Terhadap Pluralisme Kebudayaan Manusia di Negara Berkembang*. Public journal.

[3] menkominfo. 2007. kominfo.go.id. Diakses September 2014.

[4] Wallace, I. 2013. *The Military Role In National Cybersecurity Governance*. Brookings. Diakses dari http://www.brookings.edu/research/opinions/2013/12/16-military-role-national-cybersecurity-governance-wallace. Diakses September 2014.

massive ini tentu saja memiliki sedikit-banyak kekurangan yang disebabkan oleh rentannya keamanan ruang maya dan kapan saja dapat disusupi oleh pihak lain baik secara individu maupun negara. Hal tersebut akan menjadi ancaman bagi keamanan *cyber* Amerika, karena data-data serta informasi-informasi rahasia yang disimpan secara *digital* dapat dicuri, dimata-matai, dihancurkan atau diubah oleh pihak lain. Serangan-serangan secara *digital* juga akan meluas serta terang-terangan jika keamanan *cyber* tidak dibenahi secara baik dan akan menuntun Amerika kepada perang *cyber* yang akan sangat banyak mengancam sektor vital, infrastruktur dan kedaulatan Amerika Serikat.

Dalam beberapa serangan *cyber* yang ditujukan ke Amerika Serikat, Tiongkok juga merupakan salah satu dalangnya. Pada tahun 2007, peretas dari Tiongkok yang disponsori oleh pemerintahnya menyerang jaringan instansi pemerintah Amerika Serikat yang menargetkan sektor telekomunikasi, program angkasa, dan luar angkasa AS untuk memajukan program satelit dan kedirgantaraan Tiongkok sendiri. Beberapa tahun sebelum itu, Tiongkok juga melancarkan serangan *cyber* secara *massive* juga kepada Amerika yang diberi kode nama *Titan Rain*. Saat itu, Tiongkok berhasil meraup sekitar 20 *terabytes* data dari jaringan komputer AS. Dengan begitu majunya kapabilitas operasi *cyber* Tiongkok saat ini, mereka bisa menggunakannya untuk melakukan bermacam serangan *cyber* yang tak bisa dibalas Amerika, bahkan mungkin juga tidak bisa dideteksi.[5]

Dengan adanya kekhawatiran dunia terhadap ancaman *cyber warfare*, maka diperlukan penerapan keamaan cyber nasional yang baik untuk memberikan perlindungan terhadap informasi yang dimiliki warga negara, penegakan hukum, menjaga keamanan nasional, dan kedaulatan sebuah negara. Di Amerika Serikat, Presiden Obama mengidentifikasi *cybersecurity* sebagai salah satu tantangan keamanan nasional dan ekonomi paling serius yang dihadapi Amerika Serikat serta tidak cukup siap untuk dihapi. Tak lama setelah dilantik, Presiden Obama memerintahkan kajian menyeluruh kepada badan-badan dan lembaga terkait untuk mempertahankan informasi, komunikasi dan mengembangkan pendekatan yang komprehensif demi mengamankan infrastruktur digitalnya.

Pesatnya perkembangan ilmu hubungan internasional tidak terlepas dari perkembangan teknologi informasi dan komunikasi (TIK), terutama TIK bawah tanah (*underground*) yang merupakan sisi gelap dari TIK yang tidak banyak dikenal dewasa ini dan teknologi informasi dan komunikasi (TIK) *underground* ini merupakan tempat diletakkannya rahasia-rahasia penting negara. Seluas-seluasnya berbagai informasi yang dapat diakses saat ini, hanya 4% dari keseluruhan informasi yang tersedia, di mana 96% lagi terletak pada sisi TIK *Underground* yang hanya dapat diakses dengan cara tertentu[6]. Selain itu, TIK *Underground* memiliki berbagai macam pengaruh sebagai salah satu *Cybersecurity Strategi* Amerika Serikat dalam mengahadapi ancaman perang cyber (*Cyber Warfare*) dikarenakan TIK *Underground* ini memiliki berbagai macam fungsi. Berdasarkan paparan diatas, maka peneliti tertarik untuk mengangkat pertanyaan penelitian yang akan menjadi fokus pembahasan dalam penelitian ini, yaitu Bagaimana pengaruh C*yber Security Strategy* Amerika Serikat menghadapi ancaman *Cyber Warfare*?

KERANGKA TEORI

1. Perspektif Konstruktivisme

Pada dasarnya konstruktivisme merupakan sebuah pemikiran yang penting dalam Sosiologi terutama dalam Sosiologi institusional.[7] Pemikiran kunci dari konstruktivisme adalah dunia sosial termasuk hubungan internasional merupakan suatu konstruksi manusia. Dalam konstruktivis, terdapat asumsi tentang cyber warfare:

- Asumsi terakhir berbicara mengenai wacana dan intersubjektif. Wacana memerankan peran penting dalam pemikiran konstruktivis sosial. Bagi

[5]Serangan Cyber Dari China ke Amerika Makin Merajalela. 2008. http://mmibii.blogspot.com/2008/11/serangan-cyber-dari-china-ke-amerika.html. Diakses September 2014.

[6] Penelitian California Institute, disadur dari http://www.kaskus.co.id/post/527b6401becb174d0a000001#post527b6401becb174d0a000001. Diakses maret 2014.

[7] Smit, Reus. 2001. Constructivism, in; Scott Burchill, et al, *Theories of International Relations,* London: Palgrave.

para konstruktivis, wacana merupakan sinonim dari komunikasi.

Berdasarkan asumsi-asumsi yang diusung oleh perspektif konstruktivisme, keamanan *cyber* serta perang *cyber* Amerika Serikat merupakan konteks wacana yang dibuat oleh aktor. Hal ini akan berimbas pada norma dan perilaku masyarakat yang bukan hanya dalam negeri, tetapi juga masyarakat internasional. Ancaman *Cyber Warfare* dipandang anarki dalam perspektif ini, maksudnya adalah wacana ancaman perang secara dunia maya ini akan tetap menjadi fiksi jika Amerika Serikat bersikap kooperatif terhadap Negara lain. Sebaliknya, ancaman perang *cyber* akan menjadi nyata dan akan berimbas menjadi *"real war"* jika Amerika Serikat bersikap konfliktual. Sebab konstruktivisme memandang tidak ada sifat yang sebenarnya dari anarki internasional. Anarki adalah apa yang diperbuat oleh negara. Jika negara-negara berperilaku secara konfliktual terhadap satu sama lain, maka tampak bahwa sifat dari anarki internasional adalah konfliktual. Namun jika negara berperilaku kooperatif terhadap satu sama lain, maka tampak bahwa sifat dari anarki internasional adalah koperatif.[8]

2. Teori Sekuritisasi

Teori ini dipelopori oleh Barry Buzan[9], teori ini berpandangan bahwa masalah keamanan merupakan hasil konstruksi, sejalan dengan perspektif konstruktivisme. Artinya, suatu isu menjadi masalah keamanan karena ada aktor-aktor yang mewacanakannya dengan mengatakan bahwa isu tersebut merupakan ancaman eksistensial bagi suatu entitas. Teori yang diusung Buzan ini memiliki tiga model[10] dalam mengkaji sector cyber secara spesifik, yaitu:

1. *Hypersecuritization*: diperkenalkan Buzan untuk mendeskripsikan ancaman dan bahaya sekuritisasi jaringan sebuah negara diatas level normal. Sebab jaringan yang rusak akan mengakibatkan runtuhnya berbagai system dan banyak sektor yang akan diserang seperti sektor finansial dan militer;
2. *Everyday Security Practice*: dimaksudkan untuk mengamankan aktor, termasuk organisasi privat dan bisnis, memobilisasi individu "normal" dengan dua cara: mengamankan kemitraan individu dan pemenuhan dalam menjaga jaringan keamanan serta membuat skenario *hypersecuritization* lebih masuk akal dengan cara menggabungkan elemen skenario ancaman dan pengalaman yang sudah tidak asing lagi dalam kehidupan sehari-hari;
3. *Technification*: menggunakan pakar-pakar dalam bidang teknologi cyber yang akan memain peran besar dalam *hypersecuritization*.

3. Teori Strategi

Strategi adalah pendekatan secara keseluruhan yang berkaitan dengan pelaksanaan gagasan, perencanaan, dan eksekusi sebuah aktivitas dalam kurun waktu tertentu.[11] Dalam konsep *use of power,* strategi didefinisikan sebagai kemampuan untuk menggunakan kekuatan sebagai alat dan/atau ancaman. Teori strategi terdiri dari beberapa konsep diantaranya politik, sosio-budaya, ekonomi, teknologi, strategi militer, faktor geografis, dan sejarah.

Teknologi Informasi dan Komunikasi (TIK) *Underground* merupakan salah satu instrumen dalam bidang teknologi pada konsep *use of power.* Penggunaan TIK Underground merujuk pada istilah inteliijen. Menurut Sun Tzu,[12] pada tataran operasional, memberikan titik berat pada intelijen, pengelabuhan, dan pendekatan tidak langsung kepada musuh adalah cara yang paling efektif untuk memenangkan pertempuran. Proses intelijensi (memata-matai) menggunakan TIK Underground merupakan faktor penting dalam *Cyber Warfare*.

PEMBAHASAN

Penelitian ini akan menjelaskan pengaruh *Cyber Security Strategy* Amerika Serikat dalam mengamankan serta mempertahankan data-data digital penting serta infrastruktur vital milik

[8] Weber. Cynthia. 2005. *International Relations Theory, A Critical Introduction.* Routledge.

[9] Buzan, Barry. 1998. *Security: A Framework for Analysis*. Boulder: Lynne Reinner Publishers.

[10] Hansen, Lene. 2009. *Digital Disaster, Cyber Security, and the Copenhagen School*. International Studies Association.

[11] Mahnken, Thomas & Maiolo, Joseph A. 2008. *Strategic Studies: A Reader*. New York: Taylor and Francis e-Library. Hlm 22.

[12] dalam bukunya *"The Art of War"*.

Amerika Serikat dari ancaman *cyber warfare*. Apakah *Cyber Security Strategy* berhasil ini berhasil dalam mengamankan data-data digital penting serta infrastruktur vital tersebut tergantung pada implementasinya.

Internet

Sejarah Internet dimulai pada tahun 1960-an, yaitu ketika Levi C. Finch dan Robert W. Taylor mulai melakukan penelitian tentang jaringan global dan masalah interoperabilitas.[13] Pada tahun 1969, Robert Taylor yang baru dipromosikan sebagai kepala kantor pemrosesan informasi di DARPA (Badan Riset Angkatan Bersenjata Amerika Serikat) bermaksud mengimplementaskan ide untuk membuat sistem jaringan yang saling terhubung. Bersama Larry Robert dari MIT, Robert Taylor memulai proyek yang kemudian dikenal sebagai ARPANET.[14]

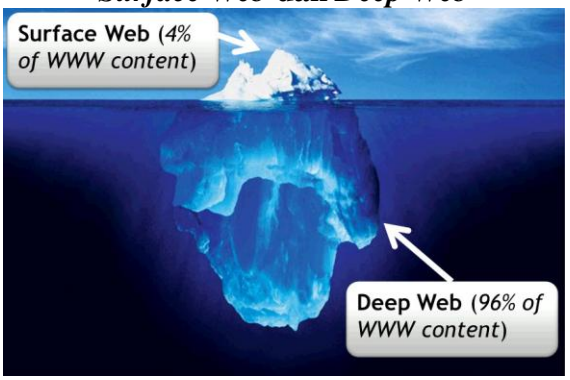
Tidak lama kemudian proyek ini berkembang pesat di seluruh daerah, dan semua universitas di negara tersebut ingin bergabung, sehingga membuat ARPANET kesulitan untuk mengaturnya. Oleh sebab itu ARPANET dipecah manjadi dua, yaitu "MILNET" untuk keperluan militer dan "ARPANET" baru yang lebih kecil untuk keperluan non-militer seperti, universitas-universitas. Gabungan kedua jaringan akhirnya dikenal dengan nama DARPA Internet, yang kemudian disederhanakan menjadi Internet.

Namun, pesatnya perkembangan internet ini tidak hanya melahirkan sisi positif, tapi juga lahir sisi negatif atau sisi gelap yang berada dibalik bayang-bayang cahaya peradaban maju dunia teknologi saat ini. Sisi tersebut dinamakan *Underground Internet / deep web,* yang mana merujuk pada situs-situs yang tidak terindeks oleh mesin pencari standar seperti *Google/Yahoo/Bing*. Sehingga kita tidak dapat mencarinya pada mesin pencari tersebut. Hal tersebut dikarenakan situs-situs tersebut bersifat dinamis yang hanya akan terbentuk oleh pencarian-pencarian spesifik.

Teknologi Informasi dan Komunikasi *Underground*

Internet terbagi dalam dua sisi, yaitu *Surface Web* dan *Deep Web*.[15] *Surface Web* adalah segala informasi yang terdapat di Internet dan dapat dicari oleh mesin pencari biasa, sedangkan *Deep Web* adalah segala informasi yang terdapat di Internet namun tidak terdeteksi oleh mesin pencari biasa. Terlebih lagi, segala informasi yang terdapat di internet dari yang bersifat umum sampai yang bersifat rahasia 96% disimpan/diletakkan di *Deep Web*. Melalui *Deep Web* inilah segala macam serangan *cyber* diluncurkan. Negara, kelompok, atau individu manapun yang dapat menguasai dan mengendalikan *Deep Web* ini, akan memiliki pengaruh yang sangat besar dalam dunia *cyber* internasional.

Surface Web* dan *Deep Web



Sumber:
http://www.extremetech.com/extreme/168277-silk-road-how-to-be-a-deep-web-criminal-and-get-away-with-it

Sebagian besar konten *deep web* berisi tentang *database-database* dari hasil penelitian/riset yang dilakukan oleh lembaga-lembaga akademis dan lembaga-lembaga pemerintahan serta situs-situs pribadi. Ini mungkin salah satu penyebab "*hidden*" nya situs-situs pada *deep web* karena memang bukan untuk konsumsi umum. Namun pada sebagian *deep web* juga terdapat situs-situs yang tidak biasa. Misalnya situs tempat jual-beli narkoba, pornografi ilegal, jasa pembunuh bayaran, eksperimen-eksperimen ilegal pada manusia, jasa *hacking*, serta penjualan informasi kartu kredit. Ada yang beranggapan bahwa situs pada *deep web* yang menyediakan jasa pembunuh bayaran

[13] Yunita, Lestari. 2013. *Sejarah dan Perkembangan Internet Dunia*. http://lestariyunita10.blogspot.com/2013/09/sejarah-dan-perkembangan-internet-di.html. Diakses pada September 2014.

[14] *Ibid*. http://lestariyunita10.blogspot.com/2013/09/sejarah-dan-perkembangan-internet-di.html. Diakses pada September 2014.

[15] Martin, Jeremy. 2013. *The beginner's Guide to The Internet Underground.* Information Warfare Center.

dan eksperimen ilegal tersebut palsu. Transaksi yang ada di *deep web* menggunakan *Bitcoin*.[16]

Faktanya, informasi publik yang ada di *deeb web* lebih besar 400 -500 kali dari yang ada pada web biasa, atau yang terindeks *Deep Web* mempunyai sebanyak 7500 TB (*terabytes)* informasi dibandingkan dengan 19 TB informasi yang ada pada web biasa, atau yang terindeks ada sekitar 550 miliar dokumen rahasia atau publik yang ada di *Deep Web* dibandingkan dengan 1 Miliar dokumen yang ada pada web biasa, atau yang terindeks lebih dari 200.000 website aktif dan dan dapat diakses tanpa enskripsi.[17] Kuantitas informasi *deep web* lebih besar dari *website* yang sudah terindeks di mesin pencari standar (Karena semua file rahasia) lebih dari 95% informasi dari website yang ada pada *DEEP WEB* dapat diakses tanpa registrasi atau bayar.

Deep Web adalah kategori terbesar dari Internet, lebih besar dari yang telah terindeks pada mesin pencari, ditambah lagi semua yang ada di *Deep Web* adalah, identitas asli hacker internasional, ilmuwan yang bergerak dibidang non-kemanusian, gembong narkoba insternasional, pembunuh bayaran, para astronom, ahli psiskis, revolusioner, Anggota Pemerintah, Polisi, individu jenius yang gila, teroris, penganggu, pencuri data, penculik, sosiolog eksak yang gila, pedophilia, dan lain-lain. *Deep Web* adalah tempat dimana semua hal yang orang pada umumnya tidak menyangka akan ada dan nyata. Sama seperti *Deep Sea* yang sangat sulit ditembus oleh cahaya, begitu juga dengan *Deep Web*, banyak sekali sisi buruk dan gelap dari *Deep Web*, karena memang sisi baiknya hanya sedikit. Itulah kenapa dinamakan *Deep Web.*

Cyber Warfare

Cyber warfare serta kejahatan telematika merugikan banyak negara, karena merupakan perang yang sudah mengunakan jaringan komputer dan internet atau ruang *cyber* dalam bentuk strategi pertahanan atau penyerangan sistem informasi strategi lawan.[18] *Cyber warfare* juga di kenal sebagai perang *cyber* yang mengacu pada pengguna fasilitas www (*world wide web*) dan jaringan komputer untuk melakukan perang di dunia maya. Perang *cyber* juga didefinisikan sebagai peperangan yang menggunakan peralatan elektronik dan komputer untuk menghancurkan atau mengganggu peralatan elektronik dan jalur komunikasi lawan/musuh. Perang *cyber* dapat berupa konflik antara negara, maupun melibatkan aktor-aktor non-negara. Sangat sulit dalam perang *cyber* untuk mengarahkan kekuatan yang tepat dan proporsional, target yang dituju bisa militer, industry, atau sipil atau bisa hanya sebuah ruang server yang membawahi berbagai klien, dengan hanya satu diantara mereka yang menjadi sasaran.

Dalam perkembangan *Cyber Warfare*, penggunaan teknologi sistem informasi juga dimanfaatkan untuk mendukung kepentingan komunikasi antar prajurit atau jalur komando yang difasilitasi oleh sistem komando kendali militer moderen, yaitu sistem NCW (*Network centric warfare*). *Network Centric Warfare* atau NCW adalah konsep operasi militer moderen yang mengintergrasikan seluruh komponen atau elemen militer kedalam satu jaringan komputer militer NCW berbasis teknologi satelit dan jaringan internet rahasia militer yang disebut jadingan SIPRNet(*Secret internet Protocol Router Network*).[19] Teknologi NCW didukung infrastuktur SIPRNet sebagai komponen militer atau elemen militer dapat saling terhubung secara *online* sistem dan *real-time*, sehingga keberadaan lawan dan kawan dapat di ketahui melalui visualisasi di layar komputer atau laptop. Teknologi NCW ini telah dimiliki dan diaplikasikan oleh militer Amerika Serikat.

Pelaku ancaman dapat berasal dari negara *(state actor)* atau non pemerintah *(non state actor),* sehingga pelaku dapat berasal dari individu, kelompok, maupun organisasi lain yang dapat berasal dari negara sendiri, maupun antar negara. Sumber ancaman dapat berasal dari dalam maupun dari luar, kondisi sosial, sumber daya manusia, dan perkembangan teknologi. Sumber-

[16] Bitcoin adalah mata uang yang digunakan di internet yang tidak dapat di lacak serta tidak terpengaruh oleh kondisi ekonomi global.

[17] Eko, William. 2013. *Deep Web / The Hidden Internet.* http://princewilliamjr.blogspot.com/2013/11/deep-web-hidden-internet.html. Diakses September 2014.

[18] Soeparna, Intan. 2008. *Kehahatan Telematika sebagai Kejahatan Transnasional.* Surabaya: Universitas Airlangga.

[19] Darmawan, Ibnu. 2012. *Network Centric Warfare.* http://ibnewd.blogspot.com/2012/11/makalah-cyber-war.html. Diakses September 2014.

sumber ancaman *cyber* dapat berasal dari berbagai sumber, seperti:

- Intelijen Asing *(foreign intelligence service);*
- Kekecewaan *(Dissaffected employees)*;
- Investigasi Jurnalis *(investigatives Journalist);*
- Oragnisasi Ekstrimis *(Ectrimist Organization)*;
- Aktivitas Para *Hacker (Hacktivist)*;
- Kelompok Kejahatan Terorganisir *(Organised Crime Groups)*.

Cyber Security Strategy Amerika Serikat tahun 2009-2014

Setelah habisnya periode pemerintahan Presiden Bush, Barack Obama maju menggantikannya, Obama menjadi Presiden Amerika yang ke-56 dan juga menjadi Presiden Amerika Serikat pertama yang berkulit hitam. Pada awal-awal masa pemerintahannya, Obama memerintahkan kajian menyeluruh kepada badan-badan dan lembaga terkait untuk mempertahankan informasi, komunikasi dan mengembangkan pendekatan yang komprehensif demi mengamankan infrastruktur digital.

Di Amerika Serikat President Obama pada 2009 menyatakan bahwa infrastruktur digital Amerika adalah aset nasional. Pada May 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.[20]

1. Cyber Policy Review

Hasil dari kajian menyeluruh awal pemerintahan Presiden Obama tersebut adalah *Cyber Policy Review* yang langsung diluncurkan pada tahun itu juga yaitu tahun 2009. Ulasan ini menganalisa tentang kebijakan-kebijakan terdahulu, mengamati celah-celah ataupun kekurangan-kekurangan dari yang bersifat *massive* hingga yang terkecil. Hasilnya, masih banyak terdapat aktivitas-aktivitas cyber crime baik dari dalam negeri sendiri maupun dari luar negeri. Hal tersebut mengakibatkan degradasi privasi serta lumpuhnya sektor-sektor umum yang mana sangat banyak orang bergantung padanya. Sebagai contoh:[21]

- Kerusakan infrastruktur kritis: CIA melaporkan adanya aktivitas teknologi informasi berbahaya yang mengakibatkan gangguan terhadap kapasitas tenaga listrik di berbagai daerah;
- Ekslploitasi layanan keuangan publik. Pada November 2008 terdapat banyak sekali kecurangan-kecurangan dalam transaksi melalui ATM *(Automatic Teller Machine)* di 49 kota, selain itu banyak pengusaha AS yang kehilangan identitas kartu kredit dan kartu debit;
- Kehilangan sistemik nilai ekonomi AS. Industri-industri kehilangan data properti intelek dan memperkirakan kerugian sekitar $1 triliyun;

Setelah mengenali peluang dan tantangan tersebut, Obama mengidentifikasi bahwa *Cybersecurity* termasuk sebagai salah satu prioritas utama pemerintahannya. Hal tersebut masuk akal, karena jika dilihat dari ulasan ini, Obama sangat bersungguh-sungguh merencanakan *Cybersecurity Strategy* ini. Dalam kajian ini juga dibahas mengenai kebijakan apa yang akan diambil untuk mengamankan ruang maya baik dari dalam maupun luar negeri. Strategi-strategi dari kebijakan tersebut diantaranya:[22]

- Memimpin melalui pemimpin tertinggi;
- Membangun kapasitas *digital* bangsa;
- Berbagi tanggung-jawab dalam *cybersecurity*;
- Membangun badan respon insiden dan berbagi informasi secara efektif;
- Mendorong inovasi,;
- Rencana aksi.

[20] Ismail, Jul. 2014. Cyber Warfare in Indonesian Military. http://julismail.staff.telkomuniversity.ac.id/cyber-warfare-in-indonesian-cyber-military/. Diakses September 2014

[21] United States of America. 2009. *Cyberspace Policy Review.* Washington: The White House.

[22] *Ibid.* hlm 37.

Pada Mei 2009, Presiden menerima rekomendasi hasil dari *Cyberspace Policy Review* ini, termasuk pemilihan cabang Koordinator Eksekutif *Cybersecurity* yang akan mendapatkan akses penuh pada presiden. Koordinator Eksekutif *Cybersecurity* juga akan bekerjasama dengan pemain kunci utama dalam *cybersecurity* AS, termasuk pemerintah lokal dan Negara bagian, sektor swasta, Koordinator Eksekutif *Cybersecurity* juga akan memperkuat hubungan kerjasama publik dan swasta untuk mencari solusi teknologi baru untuk memastikan keamanan dan kemakmuran cyber.

2. Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

Di tahun 2011, Presiden AS mengeluarkan *executive order* tentang reformasi struktural untuk meningkatkan keamanan jaringan dan berbagi tanggung jawab dalam mengamankan informasi rahasia. Terdapat beberapa bagian dalam *executive order* ini, diantaranya:

- Memerintahkan reformasi struktural dalam mengamankan informasi rahasia;
- Tanggung jawab umum agen;
- Membuat komite senior pengamanan dan pembagian informasi rahasia;
- Membangun kantor pengamanan dan pembagian informasi rahasia;
- Memilih agen eksekutif pengamanan dan pembagian informasi rahasia pada jaringan komputer, dalam bagian ini dapat disebut mata-mata;
- Mengadakan satuan tugas untuk mengahadapi ancaman;

Menurut laporan BBC[23], yang bertepatan dengan pengumuman strategi baru departemen pertahanan yang juga terkait dengan anggaran baru untuk tahun 2011 menyebutkan bahwa untuk anggaran militer di tahun 2011, pemerintah AS telah menganggarkan dana sebesar 700 miliar dolar, meningkat 2 persen dari tahun sebelumnya

3. Executive Order 13636 - Improving Critical Infrastructure Cybersecurity

Setelah mengeluarkan *Executive Order* tentang reformasi struktural untuk meningkatkan keamanan jaringan dan berbagi tanggung jawab dalam mengamankan informasi rahasia, Selanjutnya di tahun 2013 Presiden AS kembali mengeluarkan Perintah Eksekutif *(Executive Order)* untuk meningkatkan keamanan *cyber* dalam infrastruktur-infrastruktur yang dirasa kritis/vital. Butir dari perintah tersebut antara lain adalah:

- Kebijakan. Merupakan suatu keharusan bagi Amerika untuk meningkatkan keamanan dan ketahanan infrastruktur vital bangsa dan menjaga lingkungan cyber tetap efisien, inovatif, serta menopang ekonomi, bersamaan juga dengan mempromosikan rasa aman, kepercayaan bisnis, privasi, dan kebebasan sipil. Tujuan tersebut dapat diraih dengan kerjasama dengan Negara lain, pemilik usaha dan operator infrastruktur demi menunjang keamanan *cyber* dan mengimplementasikan standar berbasis resiko;
- Infrastruktur vital. Merujuk pada aset, baik secara fisik atau virtual yang jika terkena serangan akan berdampak pada keamanan, ketahanan ekonomi nasional, kesehatan masyarakat, atau gabungan keduanya.
- Koordinasi kebijakan;
- Berbagi informasi tentang *cybersecurity.* Baik dengan Negara kerjasama, antar lembaga, ataupun dengan sektor swasta.
- Privasi dan menjaga kebebasan sipil;
- Proses konsultatif. Menteri akan menetapkan proses konsultatif untuk berkoordinasi meningkatkan keamanan cyber;
- Kerangka basis untuk mengurangi resiko *cyber attack*. Kerangka *cybersecurity* terdiri dari seperangkat standar operasi, metodologi, prosedur, dan proses pendekatan mengahadapi resiko *cyber attack*. Kerangka ini juga harus sesuai dengan standar nasional;

[23] Lyne, James. 2012. *We Must Resist over-hyping security thread*. http://www.bbc.com/news/technology-16320582. Diakses September 2014.

- Merancang program-program yang mendukung adaptasi kerangka basis *cybersecurity.*

4. Presidential Proclamation - National Cybersecurity Awareness Month, 2014

Presiden Amerika Serikat Barack Obama mengakui bahwa Amerika Serikat sendiri sangat bergantung pada teknologi informasi dan komunikasi ini baik dalam kehidupan masyarakat sehari-hari, jalannya pemerintahan serta pertahanan Negara. Obama juga menyadari bahaya yang ditimbulkan ancaman cyber ini, Obama mengatakan ketika property intelektual Amerika dicuri, hal tersebut akan dapat membahayakan ekonomi Negara, mengancam kehidupan rakyat, identitas negara, dan mencegah kebebasan individu.

Melihat dari ancaman dan bahaya yang ditimbulkan ini, Obama sebagai Presiden Amerika Serikat memproklamirkan bulan Oktober tahun 2014 sebagai bulan Kesadaran *Cybersecurity* Nasional, agar setiap lapisan masyarakat dapat mengerti dan memahami teknologi informasi dan komunikasi bukan hanya sebagai pengguna, namun juga menyadari dampak negatif yang dapat ditimbulkannya bagi pribadi maupun negara. Pada bulan kesadaran ini juga ditunjang dengan sosialisasi-edukasi *cybersecurity* pada masyarakat, agar mereka lebih peka lagi terhadap teknologi jaringan ini.

5. Cyber Security and International Cooperation

Pada May 2011, pemerintahan Obama mengeluarkan kebijakan *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Kebijakan ini merupakan hasil *ouput* Amerika untuk melawan serangan cyber bersama dengan partner internasional. Prinsip-prinsip dalam kebijakan ini, adalah kebebasan yang mendasar, privasi, kebebasan arus informasi yang bersamaan dengan dilindunginya keamanan jaringan nasional. Kebijakan ini merekomendasikan membangun norma perilaku internasional dan meningkatkan kerjasama internasional daripada memaksakan struktur pemerintahan cyber secara global.

Ancaman *cyber warfare* terhadap Amerika Serikat

Amerika Serikat merupakan negara adidaya dalam berbagai bidang termasuk teknologi informasi dan komunikasi. Pada tulisan ini, penulis mengkaji negara Amerika Serikat Amerika Serikat karena memiliki teknologi informasi dan komunikasi yang maju serta ditunjang dengan terlaksananya dengan baik kebijakan-kebijakan yang diambil oleh kepala negara untuk melindungi keamanan ruang *cyber* dari ancaman *cyber warfare.* Namun perlu digaris bawahi, semaju apapun kapabilitas yang dimiliki, sebaik apapun kebijakan terimplementasi, yang namanya teknologi jaringan ini tetap akan mempunyai celah atau *bug* yang dapat dimanfaatkan sebagai celah masuk untuk melakukan serangan *cyber* walaupun hanya dalam skala yang sangat kecil. Pada poin selanjutnya akan dijelaskan serangan-serangan yang dilancarkan terhadap dan oleh Amerika Serikat serta regulasi hukum tentang *cyber warfare* yang dimiliki Amerika Serikat.

Amerika Serikat dikenal sebagai negara yang memiliki pertahan *cyber* terkuat, namun tetap saja masih ada pihak-pihak yang mencoba melakukan serangan *cyber* terhadap Amerika Serikat ini. Hal ini diperkuat dengan meningkatnya serangan *cyber* menempatkan informasi-informasi rahasia dalam keadaan bahaya yang akan berdampak pada operasi federal, aset dan rakyat Amerika sendiri. Dalam kurun waktu 6 tahun terakhir, terjadi peningkatan kuantitas serangan *cyber* dari 5.503 kasus serangan *cyber* di tahun fiscal 2006 menjadi 42.887 kasus pada tahun 2011. Peningkatan ini mencapai 680%.[24] Beberapa contoh kasus serangan *cyber* terhadap Amerika Serikat adalah sebagai berikut:

- Sistem POS perusahaan bernama Michaels diserang peretas dan 2,6 juta kartu pembayaran pelanggan terserang virus pada Mei 2013 hingga Januari 2014;
- Perusahaan komunikasi Yahoo, diretas pada Januari 2013 dan diduga sebanyak 273 juta akun surat elektronik diretas;
- 400.000 informasi kartu kredit dan debit pelanggan perusahaan Aaron Brothers dicuri dengan menggunakan *malware* pada system POS;
- Informasi pengguna, termasuk informasi keamanan sosial pelanggan

[24] Wilshusen, Gegory C. 2014. *Cybersecurity Thread Impacting the Nation*. GAO Report of US-CERT.

perusahaan komunikasi AT&T diakses oleh pihak luar selama 2 minggu pada April 2014;

- Perusahan eBay terkena serangan cyber pada akhir Februari hingga awal Maret 2014 yang berakibat tidak dapat diaksesnya 233 juta akun pelanggan. Sebab itu eBay langsung meminta para pelanggan untuk segera mengganti kata sandi mereka;
- Lima orang peretas asal Tiongkok diindikasi melakukan peretasan komputer dan mematai-matai ekonomi perusahaan asal Amerika Serikat sejak tahun 2006 hingga tahun 2014. Perusahaan yang menjadi target adalah perusahaan energy Westinghouse, industry SolarWorld, industry US Steel, perusahaan teknologi Allegheny, perusahaan layanan Workers Union dan industry Alcoa;
- Menurut laporan dari *Departemen Homeland Security*, sebuah perusahaan yang tidak disebut namanya telah diakses oleh peretas secara paksa melalui kata sandi pegawai;
- Jaringan Kontraktor Komando Transportasi AS diserang hingga lima puluh kali antara Juni 2012 hingga Mei 2013. Setidaknya, dua puluh serangan berasal dari Tiongkok;
- Su bin, peretas asal Tiongkok berusia 49 tahun diindikasi meretas industry pertahanan Boeing antara tahun 2009 dan 2013. Ia bekerja dengan dua peretas lainnya dengan tujuan mencuri rencana program pembangunan pertahanan seperti F-35 dan jet temput F-22;
- Yang terbaru dan terheboh adalah diretasnya perusahaan Sony Pictures yang dituduhkan dilakukan oleh pemerintah Korea Utara, namun sebuah kelompok peretas bernama *The Guardian of Peace* mengklaim mereka yang melakukan peretasan tersebut. Sebuah propaganda yang dilakukan untuk menaikkan pamor film yang akan dirilis oleh *Sony Pictures* berjudul *The Interview* dengan segala kehebatan leberalisme dalam ceritanya.

Implementasi Cyber Security Strategi Amerika Serikat

Serangan *cyber* atau *cyberattack* dapat melumpuhkan dan merusak sistem jaringan komputer maupun internet sehingga berdampak besar bagi kelangsungan operasional lembaga-lembaga besar baik milik negara maupun swasta. Saling serang antar pengguna *cyberspace* ini merupakan fenomena yang membentuk mandala perang baru tanpa melihat jarak, waktu, dan aktor pelakunya. Melihat kejadian dan fenomena yang ada, menjadikan negara pengguna jaringan *cyber* terutama Amerika Serikat merespon serius dengan menciptakan organisasi-organisasi guna menghadapi kemungkinan yang terburuk akibat dari serangan-serangan *cyber* yang dapat melumpuhkan dan merusak sistem jaringan dan operasional. Pembentukan organisasi-organisasi *cyber* merupakan salah satu bentuk strategi dan aplikasi pertahanan *cyber* sebagai antisipasi datangnya serangan-serangan yang dapat merusak dan melumpuhkan sistem. Dengan berbagai strategi yang dikeluarkan oleh Amerika Serikat terkait *cybersecurity*, maka kebijakan tersebut dijalankan atau diimplementasikan oleh beberapa organisasi/agensi sebagai perpanjangan tangan pemerintah dalam menghadapi ancaman *cyber warfare.*

Jika dilihat dari serangan-serangan *cyber* yang dilancarkan terhadap Amerika Serikat pada bab sebelumnya, belum terlihat adanya serangan yang membahayakan, berdampak besar, dan dapat melumpuhkan jaringan infrastruktur vital Amerika Serikat. Serangan-serangan *cyber* tersebut banyak menargetkan sektor swasta, yang tidak berakibat pada rusaknya jaringan pemerintahan walaupun kuantitas serangannya dapat dikatakan tinggi. Seharusnya, serangan dengan rasio tinggi secara berkala tersebut dapat melumpuhkan sistem informasi dan komunikasi sebuah negara, contohnya adalah Estonia dan Iran. Estonia dan Iran merupakan contoh negara yang lumpuh akibat serangan *cyber*. Kualitas serangan yang ditujukan pada Estonia dan Iran sama seperti serangan-serangan yang pernah dilancarkan pada Amerika Serikat, malahan kuantitasnya tidak setinggi serangan yang ditujukan pada negara adidaya tersebut. Estonia

dan Iran lumpuh, Amerika Serikat tetap bertahan. Dengan penguasaan dan pemanfaatan teknologi informasi dan komunikasi yang baik serta ditunjang oleh *cyber security strategy*-nya, Amerika Serikat berhasil mengamankan data-data digital serta infrastruktur vitalnya dari ancaman *cyber warfare*.

Cyber security strategy Amerika Serikat ini mengharuskan adanya kerjasama antar lembaga atau badan baik pemerintah maupun swasta secara domestik ataupun kerjasama internasional. Kerjasama ini dibagi dengan level strategis dan level operasional. Pada penerapan *cyber security strategy* ini, setiap badan/agensi memiliki peran dan fungsi masing-masing dalam menghadapi ancaman *cyber warfare*. Badan-badan/agensi ini memiliki satuan tugas, standar operasi, metode, prosedur, dan program tersendiri. Jadi, keberhasilan Amerika Serikat dalam mengamankan data-data digital serta infrastruktur vitalnya bertumpu pada kinerja dari badan-badan tersebut. Malahan, operasi dari badan-badan intelijen milik Amerika Serikat ini yang merupakan ancaman bagi negara lain.

1. Department of Defense (Kementerian Pertahanan Amerika Serikat) sebagai Badan Level Strategis

Department of Defence (DoD) bertanggung jawab menjalankan pertahanan dan keamanan Amerika Serikat setelah kebijakan nasional atau kebijakan luar negeri dari presiden ditetapkan, termasuk pertahanan dan keamanan *cyber.* Untuk menciptakan pertahanan dan keamanan *cyber* tersebut, DoD sebagai Kementerian Pertahanan Amerika Serikat memiliki lima agensi intelijen utama yang disebut *"the big five"* dan beberapa sub-agensi yang menjalankan operasional pertahanan dan keamanan cyber. Kelima agensi intelijen tersebut adalah lembaga independen *Central Intelligence Agency* (CIA), *National Security Agency* (NSA), *Defense Intelligence Agency* (DIA), *National Geospatial-Intelligence Agency* (NGA) dan *The National Reconnaissance Office* (NRO). *Department of Defense* (DoD) yang bertugas dalam level strategis memiliki lima strategi inisiatif dalam pertahanan dan keamanan *cyber*,[25] yaitu:

1. Memperlakukan ruang *cyber* sebagai wilayah operasional untuk mengkoordinir, melatih dan melengkapkan diri sehingga DoD dapat mengambil keuntungan penuh dalam potensi ruang cyber;
2. Mengembangkan sistem operasi pertahanan yang baru untuk melindungi sistem dan jaringan DoD;
3. Bekerjasama dengan departemen dan agensi lainnya dalam (*Department of Homeland Security* dan beberapa agensi bawahannya) serta sektor swasta untuk menciptakan *cybersecurity strategy* antar pemerintah;
4. Membangun hubungan yang kuat dengan aliansi Amerika Serikat serta partnet internasional untuk memperkuat *cybersecurity* secara kolektif;
5. Memberi pengaruh pada kecerdasan bangsa melalui pengembangan *cyber* dan inovasi-inovasi teknologi secara luar biasa maju.

Kebijakan-kebijakan yang diambil oleh level strategis ini merupakan kebijakan yang selalu revisi atau diperbarui menurut perkembangan ancaman cyber warfare yang akan dihadapi Amerika Serikat. Informasi-informasi akan masuk sebagai input dari badan-badan intelijen lalu akan dikaji dan dianalisa. Jika terdapat ancaman yang sangat membahayakan, akan dikeluarkan kebijakan baru untuk mengatasi ancaman tersebut. Selanjutnya, kebijakan yang dibuat tersebut akan diteruskan dan dijalankan oleh badan-badan atau agensi yang berada pada level operasional.

2. *US Strategic Command* (USSTRATCOM) sebagai Badan Level Operasional

US Strategic Command merupakan badan di bawah DoD dan induk dari badan intelijen "*the big five"* yang menjalankan level operasional keamanan dan pertahanan *cyber*, USSTRATCOM mempunyai tugas diantaranya:[26]

1. Melaksanakan operasi dan pertahanan *Global Information Grid (GIG)* Dephan AS;
2. Merencanakan untuk melawan bakal ancaman *cyberspace;*

[25] United States of America. 2011. *Strategy for Operating Cyberspace.* Department of Defense.

[26] GAO. 2011. *Defense Departement Cyber Effort: DOD Faces Challenges In Its Cyber Activity.* Washington: US Government Accountability Office.

3. Mendukung untuk kemampuan *cyberspace;*
4. Melaksanakan operasi *cyberspace;*
5. Berkoordinasi dengan komando kombatan lainnya dan badan pemerintah AS terkait untuk permasalahan-permasalahan yang berhubungan dengan *cyberspace.*

3. US Cyber Command (USCYBERCOM) sebagai Badan Pertahanan Cyber Militer

Badan ini bertugas untuk memfasilitasi integrasi operasi *cyberspace* untuk dinas militer dan mengsinkronisasi misi *cyber* dephan dan usaha peperangan, serta menyediakan dukungan untuk otoritas sipil dan partner internasional. Selain *"the big five",* elemen-elemen *US Cyber Command* terdiri dari *US Army Cyber Command, the Twenty-fourth Air Force/AFCYBER, the US Fleet CyberCommand/US 10th Fleet,* dan *Marine Corps Cyber Command.*[27] Adapun misi dari USCYBERCOM adalah[28] pertama, merencanakan, mengkoordinasikan, mengintegrasikan, mensinkronisasikan dan melakukan kegiatan untuk operasi langsung dan pertahanan jaringan informasi Departemen Pertahanan Amerika Serikat. Kedua, mempersiapkan diri untuk diarahkan melakukan operasi militer penuh dalam spektrum dunia maya untuk memungkinkan aksi dalam semua *domain* internet dan memastikan Amerika Serikat dan sekutunya terbebas dari serangan dunia maya dan menangkal setiap serangan *cyber* dari musuh Amerika Serikat/Sekutunya.

4. *National Security Agency* (NSA) sebagai Pelindung Informasi dan Infrastruktur Vital

NSA bertugas untuk mengumpulkan dan menganalisis komunikasi negara lain, serta melindungi informasi milik Amerika Serikat. NSA mengkoordinasi, mengarahkan, serta menjalankan aktivitas-aktivitas amat istimewa bertujuan untuk mengumpulkan informasi intelijen dari luar negeri, terutama menggunakan kriptoanalisis. Selain itu, NSA melindungi komunikasi pemerintah dan sistem informasi di AS dari agensi lainnya, yang melibatkan kriptografi tingkat tinggi. Kegiatan-kegiatan NSA meliputi penyadapan dan pengamanan. Penyadapan NSA meliputi telepon, komunikasi Internet, komunikasi radio, serta komunikasi-komunikasi lainnya yang dapat disadap. Pengamanan NSA meliputi komunikasi militer, diplomatik, serta komunikasi-komunikasi rahasia atau sensitif pemerintah. NSA merupakan organisasi yang mempekerjakan ahli matematika dan memiliki superkomputer terbanyak di dunia.[29]

Dalam *cyber warfare,* NSA memiliki peran ganda. Peran sebagai pelindung (*defense*) data-data digital penting dan infrastruktur vital serta berperan sebagai penyerang (*offense*). NSA memiliki banyak sekali program-program dan perangkat lunak (*software*) berbasis teknologi infomasi dan komunikasi *underground* yang berguna untuk mencuri bermacam-macam data dari berbagai belahan dunia. Salah satu contohnya adalah *XKeyScore.*[30] *XKeyScore* ini merupakan *software* yang dimiliki NSA untuk menggali informasi dan mengeksploitasi mengenai apa saja yang ingin diketahui selama hal tersebut berbentuk data digital secara *real-time.* Jika pernah mendengar istilah *"god's eye"*, mata yang dapat melihat segalanya, *XKeyScore* inilah versi manusianya. Jika terjadi serangan cyber, NSA dengan segala program dan *software* canggihnya dapat melakukan serangan balik kepada penyerang.

PENUTUP

Cyber warfare telah menjadi ancaman yang sama bahayanya dengan ancaman perang fisik bagi Amerika Serikat. Serangan-serangan yang dilancarkan melalui ruang *cyber* mampu melumpuhkan infrastruktur vital, sistem informasi, hingga dapat menggoyahkan kredibilitas pemerintah dan pada akhirnya mengancam kedaulatan negara. Tuntutan akan keamanan *cyber* meningkat akibat ancaman *cyber warfare* ini. Untuk menciptakan *cybersecurity*/keamanan *cyber* tersebut

[27] *Ibid.*

[28] Bambang, Den. 2012. *Cyber Defense : Sebuah Kebutuhan Pertahanan Di Era Globalisasi.*https://denbambang.wordpress.com/2012/11/24/cyber-defense-sebuah-kebutuhan-pertahanan-di-era-globalisasi/. Diakses Januari 2015.

[29] NSA Mission. https://www.nsa.gov/about/mission/index.shtml. Diakses Maret 2015.

[30] E, Dilipraj. 2014. *Xkeyscore, NSA's Digital Cluster*. CAPS.

diperlukan strategi. Pada titik inilah *cybersecurity strategy* Amerika Serikat memegang peran penting dalam mengamankan infrastruktur vital, aset, perbankan, hingga jaringan internet.

Banyak serangan *cyber* yang dilancarkan terhadap Amerika Serikat, dapat dilihat dari contoh insiden yang telah dijabarkan sebelummnya, mulai dari sektor swasta hingga ke sektor pemerintahan namun dalam skala lebih kecil yang tidak berbahaya atau mengkhawatirkan. Perbedaan kuantitas serangan *cyber* di sektor swasta dan pemerintahan ini dikarenakan implementasi *cybersecurity strategy* Amerika terlalu dititik beratkan pada pemerintah. Alasannya sangat sederhana, jika negara sebesar Amerika Serikat mudah dipenetrasi melalui serangan-serangan *cyber*, maka Amerika Serikat bukanlah negara yang patut menyandang julukan *superpower* lagi. Amerika tidak mau kehilangan pamor sebagai negara adidaya, akan terlihat lemah dalam *bargaining position* di dunia internasional dan segala rahasianya akan terbongkar. Maka dari itulah Amerika Serikat menitik beratkan *cybersecurity strategy* pada sektor pemerintahan. Walaupaun Amerika Serikat menitik beratkan *cybersecurity* di sektor pemerintahan, bukan berarti keamanan *cyber* sektor swastanya lemah. Bagi negara lain, tetap saja itu terlihat kuat bagi mereka. Hanya saja yang namanya teknologi cyber pasti memiliki celah walau sekuat apapun keamanannya.

Penguasaan Teknologi Informasi dan Komunikasi (TIK) *Underground* atau teknologi jaringan *deep web* secara baik dan dengan peralatan maju oleh Amerika Serikat sebagai implementasi dari *cybersecurity strategy* membuahkan hasil. Dari sekian banyak ancaman *cyber warfare,* baik ancaman terhadap sektor pemerintahan ataupun swasta, Amerika Serikat **berhasil** mengamankan data-data digital dari berbagai infrastruktur vital. Hal ini dapat dibuktikan dengan tidak adanya kepanikan besar *(big chaos)* seperti yang seharusnya terjadi jika suatu infrastruktur vital terancam dan tidak adanya kelumpuhan sistem pemerintahan yang menghambat jalannya pemerintahan. Bahkan sebaliknya, Amerika Serikat yang melakukan serangan *counter*. Amerika menerapkan TIK underground sebagai *tools* dari *cybersecurity strategy* untuk melakukan spionase *cyber* melalui agensi intelijensinya yaitu *the big five* di bawah USCYBERCOM. Lima badan intelijen ini terdiri dari *National Security Agency* (NSA), *Defense Intelligence Agency* (DIA), *National Geospatial-Intelligence Agency* (NGA) dan *The National Reconnaissance Office* (NRO) dan lembaga independen *Central Intelligence Agency* (CIA).

Kelima badan intelijen tersebut merupakan level operasional dari pengimplementasian strategi, dimana level strategis diperankan oleh *Department of Defense* (DoD). Kebijakan-kebijakan dalam level strategis memunculkan pemikiran-pemikiran bersifat strategis berupa doktrin-doktrin yang kemudian direspon dalam level operasional berupa tindakan-tindakan yang bersifat taktik, teknik, dan operasional guna mengontrol perkembangan *cyber* di negara tersebut. Kolaborasi dan integrasi kedua level tersebut merupakan modal utama dalam menghadapi ancaman *cyber warfare* serta mengamankan infrastruktur vital pemerintahan itu sendiri. Dapat dikatakan kolaborasi ini memiliki peran ganda, berperan sebagai penjaga keamanan *cyber* Amerika Serikat, juga berperan dapat sebagai penyerang dalam *cyber warfare*.

DAFTAR PUSTAKA

Jurnal

E, Dilipraj. 2014. *Xkeyscore, NSA's Digital Cluster*. CAPS.

Kurnia, Erwin. 2014. *Kebijakan Strategi Keamanan Cyber Nasional Dalam Menghadapi Perang Cyber (Cyber Warfare*). Jakarta: Faculty of Defense Strategy, Indonesian Defense University.

Krisna. 2005. *Pengaruh Globalisasi Terhadap Pluralisme Kebudayaan Manusia di Negara Berkembang*. Public journal.

Soewardi, Bagus A. 2013. *Perlunya sistem pertahanan siber yang tangguh bagi Indonesia*. Media Informasi: Ditjen Pothan.

Sulistyo, Adi. 2014. *Sejarah dan Perkembangan Perang Cyber*. Jakarta: Faculty of Defense Strategy, Indonesian Defense University.

Soeparna, Intan. 2008. *Kehahatan Telematika sebagai Kejahatan Transnasional.* Surabaya: Universitas Airlangga.

Buku

Buzan, Barry. 1998. *Security: A Framework for Analysis*. Boulder: Lynne Reinner Publishers.

GAO. 2011. *Defense Departement Cyber Effort: DOD Faces Challenges In Its Cyber Activity.*

Washington: US Government Accountability Office.
Hansen, Lene. 2009. *Digital Disaster, Cyber Security, and the Copenhagen School*. International Studies Association.
James Clavell, Ikon. 2002. The Art of War Sun Tzu, Yogyakarta.
Mahnken, Thomas & Maiolo, Joseph A. 2008. *Strategic Studies: A Reader*. New York: Taylor and Francis e-Library. Hlm 22.
Smit, Reus. 2001. Constructivism, in; Scott Burchill, et al, *Theories of International Relations,* London: Palgrave.
Steans, Jill and Pettiford, Lloyd & Diez, Thomas, 2005. *Introduction to International Relations, Perspectives & Themes,* 2nd edition, Pearson & Longman.
United States of America. 2009. *Cyberspace Policy Review*. Washington: The White House.
United States of America. 2011. *Strategy for Operating Cyberspace.* Department of Defense.
Wilshusen, Gegory C. 2014. *Cybersecurity Thread Impacting the Nation*. GAO Report of US-CERT.
Weber. Cynthia. 2005. *International Relations Theory, A Critical Introduction.* Routledge.

Website

Bambang, Den. 2012. *Cyber Defense : Sebuah Kebutuhan Pertahanan Di Era Globalisasi.*https://denbambang.wordpress.com/2012/11/24/cyber-defense-sebuah-kebutuhan-pertahanan-di-era-globalisasi/. Diakses Januari 2015.
Darmawan, Ibnu. 2012. *Network Centric Warfare.* http://ibnewd.blogspot.com/2012/11/makalah-cyber-war.html. Diakses September 2014.
Eko, William. 2013. *Deep Web / The Hidden Internet.* http://princewilliamjr.blogspot.com/2013/11/deep-web-hidden-internet.html. Diakses September 2014.
Martin, Jeremy. 2013. *The beginner's Guide to The Internet Underground.* Information Warfare Center.
Ismail, Jul. 2014. Cyber Warfare in Indonesian Military. http://julismail.staff.telkomuniversity.ac.id/cyber-warfare-in-indonesian-cyber-military/. Diakses September 2014
Lyne, James. 2012. *We Must Resist over-hyping security thread*. http://www.bbc.com/news/technology-16320582. Diakses September 2014.
Menkominfo. 2007. kominfo.go.id. Diakses September 2014.
NSA Mission. https://www.nsa.gov/about/mission/index.shtml. Diakses Maret 2015.
Penelitian California Institute, disadur darihttp://www.kaskus.co.id/post/527b6401becb174d0a000001#post527b6401becb174d0a000001. Diakses maret 2014.
Serangan Cyber Dari China ke Amerika Makin Merajalela. 2008. http://mmibii.blogspot.com/2008/11/serangan-cyber-dari-china-ke-amerika.html. Diakses September 2014.
Wallace, I. 2013. *The Military Role In National Cybersecurity Governance*. Brookings. Diakses dari http://www.brookings.edu/research/opinions/2013/12/16-military-role-national-cybersecurity-governance-wallace. Diakses September 2014.
Yunita, Lestari. 2013. *Sejarah dan Perkembangan Internet Dunia*. http://lestariyunita10.blogspot.com/2013/09/sejarah-dan-perkembangan-internet-di.html. Diakses pada September 2014.