STRATEGI MILITER MENGENAI SIBER UNTUK KEUNGGULAN DUNIA MAYA DALAM PERANG ELEKTRONIK

Indra Kristian[1)], Atik Rochaeni[2)]

[1)]Program Studi Administrasi Negara, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas al ghifari, Indonesia

[2)] Program Studi Ilmu Pemerintahan, Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jenderal Achmad Yani Indonesia

e-mail: technician2007@gmail.com

Abstrak

Dalam Penelitian ini, Peneliti mengusulkan strategi militer siber yang tangguh dan operasional untuk keunggulan dunia maya dalam perang elektronika. Kami mempertimbangkan tenaga kerja pasukan siber, kemampuan intelijen siber, dan organisasi kekuatan siber untuk meningkatkan strategi militer perang elektronika. Di bidang kekuatan- kekuatan siber, kita harus membina pribadi-pribadi yang dapat melakukan operasi komputer jaringan dan menguasai teknologi keamanan siber seperti pengumpulan intelijen siber, serangan siber, pertahanan siber, dan forensik siber. Kemampuan intelijen siber mencakup pengawasan/pengintaian siber, tatanan pertempuran siber, dan penilaian kerusakan siber. Sebuah organisasi kekuatan perang elektonika harus mengubah struktur pohon menjadi struktur jaringan dan harus mengatur tugas atau organisasi sentris fungsional. Strategi militer dunia maya yang kami usulkan memberikan keputusan tindakan sebelumnya untuk mengoperasikan efek yang diinginkan di dunia maya.

Kata Kunci: strategi, militer, siber, perang elektronika

Abstract

In this paper, researcher propose a robust and operational cyber military strategy for cyberspace excellence in electronic warfare. We consider cyber force workforce, cyber intelligence capabilities, and cyber force organization to enhance electronic warfare military strategies. In the field of cyber forces, we must cultivate individuals who can perform network computer operations and master cyber security technologies such as cyber intelligence gathering, cyber attacks, cyber defense, and cyber forensics. Cyber intelligence capabilities include cyber surveillance/reconnaissance, cyber combat setup, and cyber damage assessment. An organization of electronic warfare forces must convert a tree structure into a network structure and must organize a task or functional centric organization. Our proposed cyber military strategy provides a prior course of action to operate the desired effect in cyberspace.

Keywords*: Strategy, military, Cyber, Electronic Warfare*

PENDAHULUAN

Baru-baru ini, serangan yang dilancarkan telah meningkat secara signifikan di dunia maya. Target dari semua serangan yang ditargetkan dapat dibagi menjadi beberapa baik organisasi tertentu serta perangkat lunak atau infrastruktur teknologi informasi tertentu. Jenis serangan terhadap yang

diarahkan pada organisasi tertentu dan tujuan penyerang adalah akses tidak sah kedalam rahasia intelijen seperti rahasia rencana pelaksanaan operasi. Jenis serangan yang terakhir tidak ditujukan pada organisasi tertentu dan targetnya adalah data yang terkait dengan jenis perangkat lunak tertentu. Bahkan saat ini para hacker melaksanakan serangan dengan meretas data pribadi para pejabat Negara termasuk para menteri dan bahkan Presiden.

Beberapa pakar keamanan setuju bahwa perang elektronika dengan memanfatkan dunia maya sebagai mandala perang telah berlangsung saat ini dan terjadi di antara negara-negara. Saat ini adalah waktu yang tepat untuk mempersiapkan pertempuran dengan mandala perang dunia maya. Banyak negara membuat kebijakan perang elektronika dan meningkatkan anggaran untuk pasukan yang dipersiakan untuk perang elektronika, dan mempercepat untuk mengembangkan senjata siber. Salah satu keunggulan perang di dunia maya adalah harus terlebih dahulu dicapai dengan melaksanakan serangan untuk menang dalam perang dunia maya. Peneliti akan mengusulkan strategi militer siber dalam perang elektronika untuk keunggulan dunia maya dalam hal strategi pertahanan negara.

Untuk lebih focus dalam menyususn strategi yang tepat serta menangkal efek dari serangan siber maka peneliti tertarik membuat penelitian yang berjudul "Strategi Militer mengenai Siber untuk Keunggulan Dunia Maya dalam perang elektronika." Adapun pertanyaan penelitian yang peneliti ajukan adalah strategi apa yang paling tepat untuk mendapat keunggulan pertempuran di dunia maya ketika kita terlibat dalamperang elektronika.

METODE PENELITIAN

Metode penelitian yang digunakan adalah metode deskriptif kualitatif yang bersifat eksploratif, dengan teknik observasi yang dilakukan dari berbagai kegiatan yang berkaitan dengan penggunaan dunia maya. Kemudian sumber data sekunder diperoleh melalui studi literatur dan internet diantaranya melalui situs situs yang berkitan menganai penyaipan pasukan Siber di Negara-negara maju. Metode deskriptif adalah proses

pemecahan masalah yang diselidiki, dengan menggambarkan atau melukiskan keadaan objek penelitian pada saat sekarang, berdasarkan fakta-fakta yang tampak atau sebagaimana adanya. Penelitian dengan metode ini memusatkan perhatiannya pada penemuan fakta-fakta (fact finding) sebagaimana keadaan sebenarnya (nawawi, 2006). Sedangkan penelitian eksploratif memiliki tujuan menggali secara luas tentang sebab-sebab atau hal-hal yang mempengaruhi terjadinya sesuatu (Arikunto, 2006). Dengan demikian, metode deskriptif eksploratif adalah penelitian dengan pemecahan masalah yang digali secara luas tentang sebab-sebab atau hal-hal yang mempengaruhi terjadinya sesuatu berdasarkan fakta-fakta yang terjadi di lapangan.

Penggunaan metode deskriptif kualitatif dalam penelitian ini, diharapkan mampu menganalisis permasalahan penelitian secara empirik dan eksploratif menggunakan jenis studi kepustakaan yang memfokuskan pada analisis teori mengenai perang elektronika, sehingga mampu merekomendasi model satuan termpur yang efektif sebagai pasukan Perang Elektronika yang handal.

PEMBAHASAN

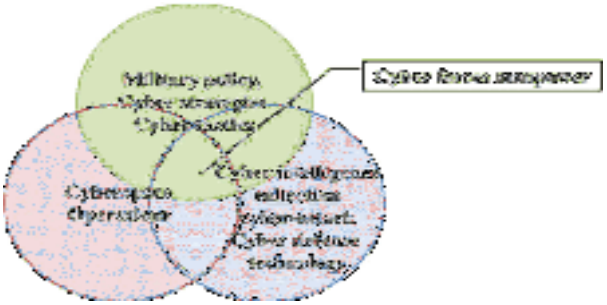
I. Strategi Militer Siber

a. Tenaga kerja pasukan Siber.

Misalkan strategi operasi siber, taktik, infrastruktur siber, dan senjata siber sudah lengkap. Namun jika para pejuang siber yang dapat menerapkan strategi dan taktik siber pada operasi siber dengan senjata siber di dunia maya tidak, apa yang akan terjadi? Dalam perang elektronika didunia maya, ketergantungan kekuatan pasukan siber yang semakin besar pada dunia maya membutuhkan pejuang dunia maya yang terdidik dan terlatih. Mereka terdiri dari operator dan pemimpin dunia maya yang siap memberikan kemampuan dan kapasitas yang dibutuhkan untuk pencapaian tujuan operasional. Prajurit dunia maya atau profesional dengan keahlian teknis dan taktis adalah individu berbasis misi operasional. Prajurit dunia maya harus memiliki pengetahuan teknis tingkat tinggi, keterampilan analitis yang kuat,

dan pemahaman yang luar biasa tentang perang dunia maya. Kekuatan dunia maya harus mengembangkan dan mengelolanya dengan cara pendidikan dan pelatihan yang paling efektif.

Jadi, para pejuang cyber harus memiliki tiga jenis pengetahuan. Pertama, mereka harus memahami kebijakan militer, strategi dan taktik dunia maya. Mereka harus mampu menyusun strategi dan taktik sesuai dengan kebijakan pertahanan negara untuk mencapai tujuan peperangan. Terutama, komandan siber memiliki kepemimpinan untuk memimpin para pejuang siber dan harus menempatkan para pejuang siber di tempat yang tepat pada waktu yang tepat. Kedua, mereka harus fasih dalam operasi dunia maya. Mereka harus memiliki kapasitas dan kapabilitas terkait eksploitasi siber, serangan siber, dan pertahanan siber. Mereka juga harus menerapkan operasi dunia maya ke perang dunia maya sesuai dengan perubahan lingkungan ruang maya musuh. Meskipun mereka memiliki serangan cyber dan teknologi keamanan yang kuat, bahkan jika mereka tidak mengetahui operasi dunia maya, keunggulan dunia maya tidak dapat dicapai. Akhirnya, mereka harus mendapat informasi yang baik tentang pengumpulan intelijen siber, serangan siber, dan teknologi pertahanan. Pengumpulan intelijen siber menghitung spesifikasi sistem dan mengeksploitasi kerentanan jaringan dan sistem musuh dengan memindai alat. Teknologi serangan siber termasuk seperti hacking, sniffing, spoofing, hijacking, Teknologi pertahanan siber memiliki sistem deteksi intrusi, firewall, sistem pencegahan intrusi, dan lain lain. Prajurit siber harus tahu bagaimana menerapkan siber- teknologi penyerangan dan pertahanan sesuai dengan operasi ruang siber.



Gambar 1
Kebutuhan Sumberdaya Manusia

b. Kemampuan intelijen siber

Kemampuan intelijen siber harus menjadi prasyarat untuk menjaga keunggulan dunia siber. Dalam perang fisik, prioritas pertama adalah memperoleh kecerdasan seperti gambar 2.

Gambar 2
Konsep K4IPP

ISR (Intelligence, Surveillance, and Reconnaissance) sedang berlangsung sebelum pecahnya peperangan, dan berarti awal dari pertempuran. Tidak terkecuali dalam perang siber. Sangat penting untuk melakukan pengawasan serangan siber dan mengumpulkan informasi tentang aspek serangan siber. Jadi, Peneliti mengusulkan sistem pengawasan berlapis untuk memantau serangan siber secara efektif seperti gambar 3. Sistem pertahanan siber global berarti sistem respons global awal, sistem pertahanan siber nasional memantau intruksi ke infrastruktur kritis pemerintah, dan sistem pertahanan siber militer melakukan pengawasan tentang Kementarian Pertahanan, Angkatan Darat, Angkatan Laut, dan Udara. Akhirnya, sistem pertahanan siber personel mengawasi sistem perwira, bintara, tamtama dan pegawai negeri sipil.

Gambar 3
Sistem pengawasan siber berlapis

Kedua, kita harus membuat tatanan pertempuran dunia maya. Ini termasuk informasi terperinci tentang sistem target atau sistem kami seperti jaringan, server, dan basis data, dll. Ini berguna untuk serangan respons siber jika kami mengidentifikasi informasi tentang sistem target. Jika kami mengetahui dengan tepat informasi tentang sistem kami, kami dapat menetapkan ukuran keamanan yang kuat dalam hal respons.

Ketiga, kita harus mengembangkan pre-CTO (*Prepositional-Siber Task Order*). Pra-CTO dibuat sebagai pra-ATO (*Prepositional-Air Tasking Order*) Angkatan Udara. Pra-ATO didefinisikan sebagai metode yang digunakan untuk menugaskan dan menyebarluaskan ke komponen, unit bawahan, dan badan komando dan kontrol yang memproyeksikan serangan mendadak, kemampuan dan/atau pasukan ke target dan misi tertentu selama tiga hari sejak pecahnya perang. Biasanya memberikan instruksi khusus untuk memasukkan tanda panggilan pejuang, target, senjata, dan badan pengendali, dll, serta instruksi umum. Pra-CTO mencakup sistem target, kerentanan, alat peretasan, server master/zombie, dan waktu serangan, dll. Kita juga harus memperhatikan eksploitasi dan serangan waktu nyata. Tentu saja, kita sudah mengetahui serangan *zero-day*, tetapi kita perlu menetapkan proses serangan yang kuat pada sistem target. Proses penyerangan adalah sebagai berikut gambar 4; identifikasi target – eksploitasi MPI (*Main Point of Impact*) - rencana peretasan - penembak peretasan - penilaian kerusakan.

Gambar 4

Proses Serangan Siber

- Identifikasi target: memutuskan sistem target yang paling rentan yang dapat mendatangkan malapetaka.
- Eksploitasi MPI: memilih salah satu titik lemah yang paling rentan dari kerentanan yang teridentifikasi.
- Rencana peretasan: menentukan tujuan serangan, metode, waktu, dan sebagainya.
- Hacking shooter: sebenarnya melakukan hacking pada sistem target.
- Penilaian kerusakan: memperkirakan tingkat kerusakan setelah serangan.

Keempat, kita harus mengembangkan metode CDA (Siber Damage Assessment) untuk penilaian kerusakan yang akurat oleh serangan siber. BDA (Battle Damage Assessment) adalah perkiraan kerusakan akibat penerapan kekuatan militer yang fatal atau non-fatal dalam peperangan fisik. BDA terdiri dari penilaian kerusakan fisik dan fungsional, dan penilaian sistem target . CDA adalah perkiraan kerusakan akibat serangan siber oleh musuh, tetapi termasuk penilaian tingkat kerusakan setelah kita melakukan serangan siber respond kepada musuh. CDA terdiri dari penilaian kerusakan operasional, fungsional, dan komponen pada sistem target.

Terakhir, kita harus meningkatkan kemampuan operasi psikologis siber. Operasi psikologis siber didefinisikan sebagai propaganda dan lainnya yang direncanakan semua kegiatan yang mempengaruhi pendapat, perasaan, sikap semua negara dan kelompok untuk secara efektif mencapai tujuan kebijakan pertahanan negara di dunia maya. Dalam perang Irak, sekutu pernah melakukan operasi psikologis siber yang rumit yang membujuk suaka atau menyerah kepada orang-orang berpangkat tinggi menggunakan e-mail dan telepon seluler di dunia maya. Operasi psikologis siber lebih efektif dilakukan dengan operasi urusan publik.

c. Organisasi kekuatan siber/Konsep Batalyon Pernika.

Organisasi kekuatan siber adalah organisasi yang berpusat pada misi atau fungsional, tidak seperti organisasi lainnya. Misalnya, departemen yang terus memantau serangan siber harus bekerja selama 24 jam, tetapi

departemen respon serangan siber harus menyelesaikannya dalam beberapa menit atau detik segera setelah serangan siber terjadi. Departemen analisis serangan siber meneliti pola serangan setelah menyelesaikan serangan siber. Organisasi kekuatan siber harus diatur dalam struktur jaringan untuk berbagi informasi serangan siber secara *real-time*.

KESIMPULAN

Penelitian ini mengusulkan strategi militer siber yang kuat dan operasional untuk keunggulan dunia maya dalam perang siber. Kami menyajikan strategi militer dunia maya dalam tiga cara.

Pertama, kita harus memperkuat tenaga kerja siber force (Pasukan Siber/Batalyon Siber). Kami membutuhkan prajurit siber yang terdidik dan terlatih. Mereka harus memiliki setidaknya tiga jenis pengetahuan. Pertama, mereka harus memahami kebijakan militer, strategi dan taktik dunia maya. Kedua, mereka harus fasih dalam operasi dunia maya. Terakhir, mereka harus mendapat informasi yang baik tentang pengumpulan intelijen siber, serangan siber dan teknologi pertahanan.

Kedua, kemampuan intelijen siber harus menjadi prasyarat untuk menjaga keunggulan dunia siber. Kami mengusulkan sistem pengawasan berlapis untuk memantau serangan siber secara efektif. Kedua, kita harus membuat tatanan pertempuran dunia maya. Ini termasuk informasi rinci tentang sistem target atau sistem kami seperti jaringan, server, dan database, dll. Ketiga, kami harus mengembangkan pra-CTO. Pra-CTO mencakup sistem target, kerentanan, alat peretasan, server master/zombie, dan waktu serangan, dll. Keempat, kita harus mengembangkan metode CDA untuk penilaian kerusakan yang akurat oleh serangan siber. Terakhir, kita harus meningkatkan kemampuan operasi psikologis siber. Operasi psikologis siber didefinisikan sebagai propaganda dan semua kegiatan yang direncanakan lainnya yang mempengaruhi pendapat, perasaan, sikap semua negara dan kelompok untuk secara efektif mencapai tujuan kebijakan nasional di dunia maya.

Akhirnya, organisasi kekuatan siber adalah organisasi yang berpusat pada misi atau fungsional, tidak seperti organisasi lainnya Organisasi kekuatan siber harus diatur dalam struktur jaringan untuk berbagi informasi serangan siber secara real-time.

Sampai dengan saat ini TNI khususnya TNI AD belum memiliki Satuan Tempur khusus yang menangani atau berkemampuan siber, saat ini hal yang berkaitan dengan elektronika masih ditangani tingkat kompi yang merupakan bagian dari Batalyon Perhubungan dibawah Pusat Perhubungan Angkatan Darat (Pushubad) untuk itu peneliti menyarankan agar dibentuk batalyon Perang Elektronika (Yon Pernika) yang memiliki kemampuan siber, sandi dan perang elektronika di bawah Pusat Perhubungan Angkatan Darat.

DAFTAR PUSTAKA

Aleksander Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, “Stuxnet uder the microscope”, www.eset.com, 2011.

Thomas M. Chen, “Stuxnet, the Real Start of Siber Warfare?”, the magazine of global internetworking, 2010.

Jung ho Eom, Nam uk Kim, Sung hwan Kim and Tai Myoung Chung, “An Architecture of Document Control System for Blocking Information Leakage in Military Information System” International Journal of Security and Its Applications, Vol.6 No.2, pp.109-114, 2012.

William Tl Lord, “Siberspace Operations; Air Force Space Command Takes the Lead”, High Frontier, Vol.5 No.3, pp.3-5, 2009.

Siberspace operations”, Air Force Doctrine Document 3-12, Air force U.S, 2010.

Patrick Beggs, “Securing the Nation’s Critical Siber Infrastructure”, Department of Homeland Security, 2010.

“Department of Defense Dictionary of Military and Associated Terms”, Joint Publication 1-02, Joint chiefs of staff, 2010.

Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, “On Siber Warfare”, A Cahtham House Report, 2010.

“Siberspace Operations Concept Capability Plan 2016-2028”, TRADOC Pamphlet 525-7-8, 2010

Jungho Eom, et al, “An introduction of Siber Warfare-Attack and Security Techniques”, hongpub, 2012.

Hong seob Lee, “siber attack prevention and the advancement of response system for IT839 infrastructure protection”, Information Security Review, Vol.1 No.3, 2004.

Jung-hoEom, Min-woo Park, Seon-ho Park and Tai-myoung Chung, "A Framework of Defense System for prevention of Insider's Malicious Behaviors", ICACT2011, 2011.

Kristian, I. (2022). Pengambilan keputusan dalam operasi penanggulangan bencana: tantangan dan peluang. Jurnal Manajemen Publik Dan Kebijakan Publik (JMPKP), 4(2).

Ki joong Lee, “A study on Alternatives of Siber Psychological Warfare of republic of Kore”, Journal on KIAS, Vol.8 No.1, 2008].