PERAN USCYBERCOM DALAM KEAMANAN NASIONAL AMERIKA SERIKAT TAHUN 2010-2018

Rahmat Aprilian Putra[1]

Abstract: *This research aims to analyze and describe the role of USCYBERCOM for maintaining United States national defense 2010-2018. The research method used is decriptive with secondary data types. The analysis technique is qualitative. The concepts used are National Security and Cyber Crime. The results of this research shows that the role which conducted by USCYBERCOM in maintaining United States national defense is by ensuring protection of national digital's infrastructure through intelligence analysis capacity optimalization, defense and cyber based forces to all national security institutions under the coordination from Department of Defense.*

Keywords: USCYBERCOM, United States, National Security, Cyber Crime

Pendahuluan

Teknologi informasi merupakan aspek penting dalam aktifitas manusia saat ini yang mendorong masyarakat sipil dan insitusi pertahanan mengalami ketergantungan terhadap ketersediaan akses serta komunikasi. Internet memungkinkan terjadinya hubungan antara jaringan komersil dan jalur pertukaran data sensitif milik negara akibat penggunaan infrastruktur digital, baik melalui koneksi kabel optik, antena radio hingga satelit. *United Nations Group of Governmental Experts* menyebutkan teknologi maya yang mendorong pertumbuhan ekonomi juga dapat memberikan ancaman terhadap keamanan (Edelman, 2013).

Pada 16 Mei 1943 dalam salah satu misi terbesar saat Perang Dunia II, pesawat pembom *Lancaster* melakukan serangan pada tiga bendungan hidroelektrik Jerman Selatan dengan tujuan untuk melumpuhkan industri militer di kawasan sungai Ruhr. Beberapa dekade kemudian tepatnya pada 1998 seorang anak berusia 12 tahun melakukan peretasan terhadap sistem pengendali bendungan *Arizona Roosevelt* dengan kapasitas 18.000.000 m^3 air. Menurut laporan pemerintah federal, jika peretas tersebut berkehendak untuk membuka seluruh pintu bendungan maka wilayah disekitarnya akan mengalami kerusakan yang besar. Fenomena tersebut memberikan gambaran ancaman keamanan akibat disrupsi jaringan melalui peretasan, sekaligus membuktikan adanya perubahan signifikan yang disebut sebagai *Revolution in Military Affairs* (Harrison, 2012).

Ruang siber mengalami perubahan dari disiplin teknis menuju studi strategis akibat globalisasi yang mendorong internet menjadi *new power domain* bagi individu, organisasi dan negara. Secara spesifik kemajuan teknologi memberikan kemudahan bagi pelajar, tentara, kelompok peretas bahkan teroris melalui digitalisasi informasi, komunikasi hingga penggalangan dana. Sebagai konsekuensi, seluruh konflik politik dan militer saat ini memiliki dimensi siber yang sulit diprediksi dengan adanya potensi perluasan konflik akibat propaganda di dunia maya. Dalam keterkaitannya dengan penyalahgunaan *cyber space* yang berhubungan dengan kejahatan seperti kelompok teroris dan peretas memperoleh keuntungan melalui manipulasi opini publik hingga

[1] Mahasiswa Program S1 Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Mulawarman. E-mail : rahmat.aprilian@gmail.com

pencurian data. Fenomena tersebut merupakan bentuk *asymmetric attack* yakni operasi fisik berupa invasi atau pemboman yang didukung dengan kapasitas penguasaan jaringan internet (Geers, 2011).

Serangan siber modern di negara-negara Baltik menandai dimulainya era baru *cyber warfare* yang terbukti mengakibatkan kerusakan fisik terhadap infrastruktur negara. Pada tahun 2007, serangan dalam bentuk *Distributed Denial of Service* (DDoS) terhadap Estonia yang dilakukan oleh Rusia dengan menggunakan *Botnets Virus* mengakibatkan kerusakan sistem komputer nasional termasuk pusat data infrastruktur perbankan yang tidak dapat beroperasi. Serangan siber tersebut merupakan respon pemerintah Rusia terhadap pemindahan patung *Bronze Soldier of Tallinn* dari era Uni Soviet berakibat pada memburuknya hubungan antara Estonia dan Rusia. Sedangkan di Georgia, serangan serupa mengakibatkan banyak layanan daring pemerintah tidak berfungsi termasuk lumpuhnya akses komunikasi sipil. Operasi siber tersebut dilakukan bersamaan dengan pergerakan tentara Rusia ke wilayah Ossetia Selatan (Kozlowski, 2014).

Serangan siber lainnya yang mendapatkan perhatian internasional terjadi pada Juni 2010 dengan sebutan *Stuxnet.* Serangan tersebut menginfeksi sekitar 50.000 – 100.000 komputer dan mengakibatkan kerusakan pada 2.000 mesin sentrifugal pengolah uranium reaktor nuklir Natanz di Iran. *Stuxnet* disebut sebagai operasi siber yang bertujuan untuk melumpuhkan kemampuan Iran dalam pengembangan senjata nuklir termasuk merusak 12 pembangkit listrik nasional. Perisitiwa tersebut dianggap lebih efektif apabila dibandingkan dengan *kinetic military operation* karena menghasilkan kerusakan yang besar, namun memberikan dampak atau kerugian yang sedikit pada masyarakat sipil (Pipyros, 2017).

Salah satu peristiwa peretasan yang memicu kekhawatiran publik secara luas yakni tindakan *Syrian Electronic Army* dengan melakukan pencurian akun *Twitter* kantor berita *Associated Press* pada tahun 2013 melalui cuitan bahwa Presiden mengalami luka akibat dua ledakan yang menargetkan Gedung Putih. Informasi palsu tersebut berdampak pada kerugian saham *Standard & Poor's 500 Index* hingga USD 136 miliar serta mengakibatkan instabilitas politik. Tiga orang pelaku ditangkap dengan pasal peretasan komputer oleh *Department of Justice* dan publik dapat ditenangkan setelah *Associated Press* memberikan klarifikasi. *Department of Defense* menyebutkan 85% pasokan energi untuk operasional pertahanan seperti komunikasi, rudal dan satelit berasal dari pembangkit listrik domestik yang rentan mengalami serangan siber seperti *Crash Override* dan *Stuxnet* dengan kemampuan memutus transmisi hingga meledakkan gardu listrik (US Senate, 2018).

Masyarakat yang terkoneksi dan bergantung dengan internet seperti Amerika Serikat menjadikannya rentan terhadap disrupsi jaringan terutama dari ancaman *cyber attack*. Ancaman yang selalu berkembang dan dinamis terhadap keamanan nasional tentunya mengganggu kedaulatan negara termasuk upaya penanggulangan *cyber attack* yang diwujudkan dalam bentuk *cyber defense*. Inovasi teknologi pada awalnya ditujukan untuk keperluan sipil seperti satelit komunikasi, pesawat komersil dan jaringan internet saat ini juga difungsikan sebagai bagian dari alat utama sistem persenjataan untuk kepentingan militer (Clarke, 2010).

Rangkaian serangan dan kerugian tersebut mendorong pemerintah Amerika Serikat untuk membentuk *US Cyber Command* (USCYBERCOM) yang merupakan penggabungan unit siber antara *National Security Agency* (NSA) dan *Department of Defense* (DoD) dengan tujuan mengefektifkan koordinasi dengan Presiden. Sistem *dual*

headed-structure menjadikan direktur NSA merangkap sebagai kepala satuan USCYBERCOM yang membawahi empat divisi siber lainnya yakni *US Army Cyber Command, US Fleet Cyber Command, Air Forces Cyber* dan *Marine Corps Forces Cyberspace Command* dengan total 11.000 tenaga ahli. USCYBERCOM dibentuk sebagai pusat koordinasi pertahanan jaringan informasi serta pengarahan operasi militer berbasis siber apabila terjadi serangan terhadap Amerika Serikat dan sekutunya.

Isu tentang *cyber war* menjadi perkara yang sering dibahas dalam berbagai forum internasional sebagai ancaman terhadap stabilitas, bahkan diprediksi dapat memicu ketegangan antar negara yang berdampak pada eskalasi konflik diberbagai kawasan. Toure Hamadoun sebagai Kepala Badan Telekomunikasi Perserikatan Bangsa Bangsa, menyebutkan bahwa Perang Dunia dapat terjadi di dunia maya. Serangan siber adalah salah satu bentuk ancaman terhadap kedaulatan negara yang dilakukan atas dasar politik atau ekonomi (Soewardi, 2013). Kapasitas siber suatu negara dalam praktiknya menciptakan situasi *security dilemma* diantara Amerika Serikat, Rusia, Tiongkok dan Korea Utara (Diamond, 2020).

Kerangka Teori

Konsep National Security

Konsep keamanan dalam analisis politik dan hubungan internasional merupakan teori yang selalu diuji relevansinya oleh dinamika hubungan internasional itu sendiri. Berbagai upaya untuk mendefinisikan konsep keamanan dilakukan oleh berbagai pakar studi ilmu hubungan internasional seperti Walter Lippman pada 1943, menjelaskan keamanan sebagai suatu kondisi negara yang tidak berada dalam keadaan terancam kemudian berakibat pada hilangnya legitimasi otoritas untuk menentukan tindakan yakni kemampuan negara untuk menghindari perang jika diinginkan dan memenangkannya apabila menghendaki (Lippman, 1943).

Barry Buzan memperluas konsep keamanan dengan argumentasi bahwa keamanan tidak hanya meliputi aspek militer dan aktor negara, namun juga meliputi faktor non militer dan melibatkan aktifitas aktor non-negara dengan pembagian topik pada 5 bidang yakni keamanan militer, politik, ekonomi, lingkungan dan masyarakat. Berdasarkan pendekatan ini, sektor militer merupakan salah satu faktor penting dalam konsep keamanan. Namun gagasan keamanan yang lebih luas dan menyeluruh pada kenyataannya dipengaruhi pula oleh sektor lainnya baik dari tingkat individu, nasional, regional serta global. Hubungan antara keamanan militer dengan kemanan non-militer (Buzan, 1983).

The International Encyclopedia of the Social Sciences menjelaskan bahwa istilah *national security* telah lama digunakan oleh politisi dan pimpinan militer untuk mendefiniskan suatu kebijakan yang berbasis pada permasalahan keamanan. Selain itu, ketika pakar ilmu sosial membahas konsep keamanan nasional, umumnya mereka merujuk pada kemampuan suatu negara untuk melindungi aset dan kepentingannya dari berbagai ancaman (Sills, 1968).

Sebagian besar konsep keamanan nasional hingga akhir abad ke 20 berfokus pada keamanan militer. Pesatnya perubahan dunia akibat globalisasi memposisikan suatu bentuk ancaman terhadap negara tidak lagi sebatas *total war* melalui penggunaan senjata nuklir, sehingga mendorong *National Security Council* pada 1947 untuk melakukan integrasi antara kebijakan domestik, luar negeri dan militer dalam mendefinisikan keamanan nasional.

Kim Holmes dalam *What is National Security* mendefinisikan *national security* dalam beberapa kategori (Wood, 2015).

a. *Political security* merujuk pada upaya untuk melindungi kedaulatan pemerintah, sistem politik domestik dan keamanan masyarakat dari ancaman yang berasal dari dalam atau luar negeri melalui perumusan kebijakan berbasis keamanan serta penegakan hukum oleh institusi terkait.
b. *Economic security* tidak hanya sebatas memberikan proteksi terhadap stabilitas *demand* dan *production* di masyarakat, namun juga memastikan pemerintah memiliki kebebasan untuk menentukan kebijakan moneter hingga fiskal. Keamanan ekonomi berkaitan erat dengan kemampuan negara untuk melindungi aset nasional dari ancaman melalui perumusan kebijakan ekonomi dan kerjasama perdagangan internasional.
c. *Energy and natural resources security* secara umum dapat dipahami sebagai kondisi suatu negara yang memiliki kedaulatan atas kekayaan alam berupa minyak bumi, gas, air dan mineral berharga lainnya tanpa intervensi dari pihak lain.
d. *Homeland security* berkaitan erat dengan upaya perlindungan domestik seperti pengamanan bandara, perbatasan, imigrasi dan aspek lain melalui pengawasan pergerakan penduduk baik lokal maupun yang datang dari mancanegara.
e. *Cybersecurity* merujuk pada perlindungan perangkat digital, infrastuktur jaringan dan *operating systems* dari interupsi berbahaya yang berasal dari dalam maupun luar negeri.
f. *Human security* merujuk pada konsep dasar kemanusiaan yang dikembangkan oleh Perserikatan Bangsa Bangsa setelah berakhirnya perang dunia dengan memastikan keamanan manusia dari kelaparan, penyakit dan penindasan termasuk tindakan represif lainnya yang dapat menganggu kehidupan publik. Seiring berjalannya waktu, konsep *human security* berkembang menjadi keamanan ekonomi, lingkungan, pangan, kesehatan, privasi, politik, perempuan dan isu minoritas.
g. *Environtmental security* merupakan konsep tradisional yang dapat diwujudkan melalui mitigasi terhadap kelangkaan air bersih, memadainya ketersediaan listrik serta mitigasi pemanasan global. Perubahan iklim dan kerusakan lingkungan berdampak pada kehidupan masyarakat yang dapat mempengaruhi stabilitas suatu negara. Saat ini permasalahan iklim telah menjadi isu pembahasan dalam keamanan nasional.

Pemerintah Amerika Serikat memposisikan negara untuk melakukan respon terhadap berbagai ancaman dan agresi. Pada Mei 2011, Barack Obama menyebutkan bahwa segala tindakan yang dilakukan di ruang siber dan mengancam keamanan nasional akan ditanggulangi melalui upaya diplomasi, operasi militer dan sanksi ekonomi. Pernyataan tersebut menyimpulkan bahwa serangan siber terhadap Amerika Serikat adalah bentuk konfrontasi bersenjata. Oleh karenanya keberadaan institusi khusus yang berfokus pada operasi berbasis keamanan dan pertahanan siber bagi Amerika Serikat merupakan suatu keharusan (Yates, 2013).

Konsep Cyber Crime

Dimensi sosial baru yakni *cyber space* selain membawa banyak manfaat terhadap kehidupan manusia, dilain sisi juga memberikan peluang bagi pelaku kejahatan untuk memperoleh keuntungan melalui pemanfaatan jaringan maya yang dikenal dengan istilah *cyber crime*. Cohen dan Felson menyebutkan *cyber crime* pada dasarnya memiliki karakteristik yang sama dengan kejahatan konvensional namun dengan karakteristik, pola interaksi, batasan dan probabilitas yang lebih beragam. Umumnya istilah ini sering digunakan untuk mendefinisikan aktifitas ilegal yang dilakukan pada sistem jaringan informasi dan teknologi yakni internet. Thomas dan Loader mendefinisikannya sebagai aktifitas berbasis elektronik melalui jaringan internet yang melanggar ketentuan hukum (Yar, 2008).

Dalam *Cybercrime in Progress*, kejahatan siber terbagi berdasarkan empat kategori (Holt, 2016). Pertama, *cyber-trespass* yang merujuk pada upaya untuk memasuki wilayah virtual pihak lain tanpa seizin pemilik, seperti pengunaan akses jaringan dan perangkat elektronik melalui pembobolan kata sandi atau metode lainnya. Menurut *Symantec Corporation* tindakan *cyber-trespass* sering ditujukan pada aktifitas peretasan yang bermaksud melakukan *log in* pada sistem komputer, akun surat elektronik atau jaringan terenkripsi dengan paksa yang berdampak pada kerusakan perangkat, hilangnya dokumen berharga hingga *computer cloning* jarak jauh.

Kedua, *cyber-deceptions and thefts* yakni tindakan pencurian uang, pemalsuan kartu kredit, pelanggaran hak cipta hingga pembajakan konten elektronik akibat jaringan maya yang saling terkoneksi memungkinkan pihak tertentu untuk memperoleh informasi dan data daring secara ilegal. *Cyber thefts* dan *cyber trespass* memiliki keterkaitan karena pada dasarnya peretas memerlukan akses terlebih dahulu sebelum melakukan pencurian data pribadi berupa informasi rekening, identitas elektronik dan dokumen terkait yang digunakan untuk penipuan. Transformasi konten akibat kehadiran internet seperti film, musik, *games*, serta perangkat lunak saat ini dapat diakses melalui fitur *direct download* tanpa harus memiliki *hard copy* berdampak pada beredarnya salinan ilegal yang melanggar hak cipta tanpa persetujuan pemilik konten.

Ketiga, *cyber-pornography* merujuk pada konten elektronik tertentu seperti tulisan erotis, lukisan, foto, audio dan video dengan tujuan memberikan stimulus seksual yakni merepresentasikan seluruh tindakan ekspresi seksual yang dapat diakses secara daring. Jaringan internet memungkinkan ketersediaan ruang untuk melakukan distribusi hingga konsumsi pornografi tanpa batasan usia, latar belakang pengguna dan negara, sehingga berdampak pada sulitnya pihak berwenang untuk melakukan penyaringan konten berdasarkan yurisdiksi hukum di wilayahnya. Cunningham dan Kendall menyebutkan, pesatnya perkembangan teknologi maya juga dimanfaatkan oleh industri prostitusi melalui forum daring maupun *website* yang ditujukan untuk menghubungkan pengguna dengan pekerja seks terkait harga, kategori hingga lokasi.

Keempat, *cyber-violence* merupakan bentuk kekerasan psikologis serta ancaman kekerasan fisik yang menimbulkan trauma dan tidak jarang berakibat pada aksi bunuh diri melalui *bullying* hingga *hate speech*. Pada dasarnya, *cyber violence* merujuk pada penggunaan teknologi komunikasi untuk melakukan pelecehan dan diskriminasi terhadap perorangan atau kelompok tertentu. Hiduja dan Patchin berpendapat bahwa kasus *cyber bullying* banyak dilakukan oleh populasi remaja yang membagikan konten *bullying* atau pesan ancaman terhadap pihak lain melalui media sosial, sedangkan populasi dewasa didominasi oleh tindakan pelecehan serta *cyber stalking*.

Besarnya potensi keuntungan dan kecilnya peluang terdeteksi oleh pihak otoritas menjadikan *cyber crime* sebagai salah satu pilihan rasional untuk melakukan tindak kejahatan. Kelompok kriminal yang tidak memiliki kemampuan teknis dapat menggunakan jasa peretas dengan *budget* tertentu, berdampak pada kehadiran pelaku kejahatan siber dengan pola organisasi yang terstuktur dan profesional. Jaringan internet memungkinkan pelaku kriminal baik yang dilakukan oleh perorangan, kelompok atau negara untuk memperluas jangkauan operasi ke seluruh dunia (Kramer, 2009).

Berdasarkan sumber dan motifnya, *Government Accountability Office* memberikan kategori terhadap kejahatan siber yakni (Revenon, 2011).

a. Negara lain melalui institusi intejilen asing menggunakan peralatan siber sebagai metode untuk mengumpulkan informasi dan melakukan spionase. Upaya tersebut termasuk dengan mengekploitasi, merusak hingga menghancurkan infrastruktur fisik yang terkoneksi dengan jaringan internet.
b. Kelompok kriminal menggunakan teknologi siber untuk memperoleh keuntungan finansial.
c. Peretas atau *hackers* seringkali melakukan pembobolan keamanan jaringan dengan motif hiburan serta adanya tantangan dari peretas lain untuk mencari kelemahan suatu sistem komputer. Peretas umumnya akan menjual atau membagikan secara gratis perangkat lunak tertentu yang dapat merusak infrastruktur jaringan suatu perusahaan hingga negara.
d. Kelompok aktivis peretas atau *hacktivist* bertindak atas motif politik dengan mengganggu operasional situs tertentu dan merusak layanan surat elektronik. Umumnya korban akan menerima pesan politik yang berusaha disampaikan oleh peretas tersebut.
e. Karyawan merupakan pihak yang memiliki akses dan mengetahui kelemahan sistem jaringan kemudian dengan sengaja memberitahukan atau menjual informasi keamanan perusahaan kepada pihak lain bahkan dalam beberapa kasus, karyawan berperan dalam melakukan injeksi *virus* ke komputer perusahaan.
f. Teroris menargetkan infrastruktur vital negara yang dapat menyebabkan kerusakan dan korban dalam jumlah besar dengan tujuan menciptakan rasa takut. *Central Intelligence Agency* menyebutkan kelompok teroris juga menggunakan peralatan siber untuk melakukan tindakannya.

Metode Penelitian

Penelitian ini menggunakan tipe deskriptif yaitu penulis menggambarkan dan menjelaskan bagaimana peran USCYBERCOM terhadap pertahanan nasional Amerika Serikat. Jenis data yang dimuat dalam penelitian ini adalah data sekunder sedangkan teknik pengumpulan menggunakantelaah pustaka (*library research*) yang bersumber dari berbagai referensi buku, *e-book*, jurnal hingga situs internet.

Hasil dan Pembahasan

Amerika Serikat melalui USCYBERCOM membentuk kapasitas operasi siber berbasis tempur untuk menopang elemen keamanan nasional. Konsep tersebut kemudian berkembang pesat beriringan dengan upaya Departemen Pertahanan untuk merubah paradigma negara dari tahapan konseptual kepada tataran operasional, yakni dimana Amerika Serikat memiliki kapasitas mumpuni berkaitan dengan *cyber power*

sejak USCYBERCOM pertama kali terbentuk hingga tahun 2018. Rangkaian tindakan USCYBERCOM dalam memastikan terjaminnya keamanan nasional yakni dengan membangun sistem pertahanan siber terintegrasi dan menyediakan proteksi taktis terhadap setiap upaya *cyber trespass* jaringan infrastruktur nasional.

A. Peran USCYBERCOM Dalam Integrasi Sistem Pertahanan Siber

Integrasi sistem pertahanan siber nasional mencakup upaya sinkronisasi tiga lapisan infrastruktur komunikasi yakni *physical network layer, logical network layer* dan *cyber-persona layer* yang dilakukan dengan memaksimalkan penggabungan sumber daya nasional berbasis siber baik dari institusi komersil, sipil hingga institusi pertahanan untuk menunjang keberhasilan suatu *Cyberspace Operations* (CO).

Cyberspace Operations (CO) berkaitan langsung dengan eksekusi misi tempur, pencapaian saat dan pasca operasi yang menunjang peran penting USCYBERCOM sebagai pusat komando siber nasional maupun sebagai institusi penyedia dukungan taktis. Kesuksesan CO memerlukan integrasi antara *Department of Defense Information Networks* (DODIN), *Defensive Cyberspace Operations* (DCO) dan *Offensive Cyberspace Operations* (OCO) yang berada dibawah tanggung jawab USCYBERCOM antara lain

1. *Department of Defense Information Networks* (DODIN): Untuk menciptakan DODIN yang tangguh, maka upaya pembentukan, pengamanan dan memastikan berjalannya operasional sistem komunikasi Departemen Pertahanan harus dilakukan melalui integrasi menyeluruh terhadap jaringan komunikasi, *configuration control and patching*, penyediaan personel, perlindungan sistem serta *firewall*. DODIN merupakan komponen vital milik Departemen Pertahanan yang menunjang pelaksanaan operasi tempur di dalam dan luar negeri.

2. *Defensive Cyberspace Operations* (DCO): Merupakan upaya pertahanan yang ditujukan untuk melindungi ruang siber Departemen Pertahanan dan sekutu dari serangan siber. Secara spesifik, DCO merujuk pada operasi perlindungan aktif serta pasif sehingga mampu memastikan keamanan siber serta fleksibilitas misi tempur. Fungsi taktis yakni (1) Kapasitas untuk mendeteksi kehadiran ancaman siber terhadap DODIN (2) Intelijen (3) *Counter Intelligence*/CI, dan (4) *Law Enforcement*/LE dengan tujuan membatalkan serangan siber musuh atau mengurangi dampak kerusakan yang ditimbulkan.

Operasional DCO berkaitan erat dengan komponen *Active Cyberspace Defense* (ACD) yang dimiliki oleh Departemen Pertahanan. Dalam dokumen *The Department of Defense Strategy for Operating in Cyberspace* mendefinisikan ACD sebagai kemampuan unit siber nasional untuk melakukan sinkronisasi operasi serta pengamanan berkelanjutan seperti (1) Deteksi dini (2) Menemukan sumber ancaman (3) Menganalisa jenis serangan (4) Mitigasi dampak, dan (5) Perbaikan kerusakan apabila terjadi. DCO terdiri dari

a. DCO *Internal Defensive Measures* (DCO-IDM): Merupakan program pertahanan siber yang berlangsung di dalam jaringan DODIN dengan melakukan upaya terhadap pelacakan potensi ancaman sekaligus menetralisir ancaman.

b. DCO *Response Actions* (DCO-RA): Merupakan program pertahanan siber yang beroperasi di luar jaringan DODIN untuk mencegah serangan siber memasuki sistem digital Departemen Pertahanan. Dalam beberapa kasus, DCO-RA dapat difungsikan untuk melakukan serangan siber balasan secara terbatas kepada musuh yakni menutup akses lalu lintas jaringan dari sumber ancaman.
c. *Offensive Cyberspace Operations* (OCO): Ditujukan sebagai program yang mampu melancarkan serangan siber berskala penuh kepada target. OCO harus melalui rangkaian perumusan misi tempur layaknya operasi kinetis yang disebut dengan *Execute Order* (EXORD).
d. *Cyberspace Actions:* Saat tugas-tugas tempur berbasis siber seperti OCO, DCO dan DODIN dilaksanakan, maka diperlukan alokasi sumber daya dan manajemen lapangan untuk mencapai kesuksesan misi secara optimal. Seluruh personel harus memahami tujuan perencanaan, rincian operasi dan evaluasi pasca tempur, antara lain

1. *Cyberspace Information Collection* merupakan operasi intelijen yang bertugas untuk mengumpulkan informasi dan data dari target operasi dalam menunjang kesuksesan DCO serta OCO.
   a. *Cyberspace Intelligence, Surveillance, and Reconnaissance* (ISR): Upaya unit tempur siber untuk melakukan tindakan intelijen melalui otorisasi EXORD yang kemudian akan digunakan sebagai landasan komandan satuan dalam merumuskan kebijakan operasi saat ini dan yang akan datang.
   b. *Cyberspace Operational Preparation of the Environment*: Merupakan salah satu simulasi operasi sebelum pelaksanaan serangan siber dengan fungsi mengindentifikasi data, perangkat lunak, sistem digital, target dan infrastruktur komunikasi yang terhubung.
2. *Cyber Attack*: Operasi siber yang dilakukan untuk menciptakan kerusakan, menghambat kinerja dan memanipulasi data milik target dengan tujuan memberikan kerugian.
   a. *Degrade*: Upaya membatasi akses, fungsi perangkat dan menurunkan performa sasaran operasi siber.
   b. *Disrupt*: Merupakan serangan tingkat lanjut dari *degrade* namun dengan jangka waktu yang lebih lama. Umumnya pelaku telah menentukan durasi serangan terhadap beberapa sistem untuk menciptakan efek berantai.
   c. *Destroy*: Memberikan kerusakan secara permanen terhadap suatu sistem atau infrastruktur digital sehingga mampu menghentikan aktivitas target.
   d. *Manipulate*: Ditujukan untuk merubah informasi serta data yang ada di dalam perangkat target, kemudian menyebabkan miskomunikasi serta ketimpangan informasi.
3. *Cross-Domain Synergy* adalah integrasi kekuatan tempur seluruh angkatan bersenjata di udara, laut, darat, antariksa dan ruang siber. CO mampu meningkatkan efektifitas operasi militer sekaligus memperkuat daya tempur kinetis di lapangan (Dunford, 2016).

USCYBERCOM merealisasikan keamanan nasional melalui perannya dalam melindungi kedaulatan siber Amerika Serikat, melakukan proyeksi kekuatan di dan melalui ruang siber serta membangun kemitraan lintas agensi maupun antar negara yang kemudian diaplikasikan dalam tiga kebijakan yakni (a) Menetralisir ancaman strategis terhadap kepentingan nasional dan infrastruktur vital Amerika Serikat (b) Memastikan keberlangsungan misi tempur Departemen Pertahanan (c) Mencapai keberhasilan operasi *Joint Force* (Alexander, 2015).

1. *Joint Directorates* - USCYBERCOM dalam menjalankan perannya menggunakan panduan dokumen fungsional *10 J-Directorates* sebagai berikut
    a. J0 - *Chief of Staff*: Menyediakan tenaga ahli, perancangan pola pertukaran informasi, peyediaan logistik dan manajemen bisnis.
    b. J1 - *Manpower & Personnel*: Memimpin komando tempur terintegrasi, responsif dan siap siaga untuk melakukan operasi siber berskala penuh diseluruh domain angkatan bersenjata.
    c. J2 - *Intelligence*: Menyediakan pengambilan keputusan yang efektif dan analisis intelijen terkini.
    d. J3 - *Operations*: Mempersiapkan perencanaan, melakukan koordinasi dan menjalankan misi tempur hingga pertahanan terhadap infrastruktur DODIN serta keamanan nasional.
    e. J4 - *Logistics*: Memastikan pemenuhan kebutuhan logistik untuk menunjang pelaksanaan operasi siber.
    f. J5 - *Plans and Policy*: Bertanggung jawab terhadap penyusunan strategi siber, perumusan kebijakan, sosialisasi doktrin operasi, evaluasi misi dan membangun kemitraan.
    g. J6 - *Command and Control* (C2) *and Information Technology* (IT): Menyediakan kebutuhan komando operasi dan peralatan siber dalam setiap misi tempur.
    h. J7 - *Joint Exercises and Training*: Mengembangkan dan mempersiapkan personel siber yang terstandarisasi untuk keperluan misi, menjalin kemitraan, pendidikan, pelatihan hingga simulasi tempur.
    i. J8 - *Capability and Resource Integration*: Menyusun panduan *Planning, Programming, Budgeting and Execution* (PPBE) dalam rangka memenuhi keperluan operasi.
2. *Administrative Support* meliputi manajemen formil dan koordinasi lintas agensi siber nasional. Pemerintah melalui USCYBERCOM menyediakan penunjang administratif antara lain *Command Section*, *Public Affairs Office*, *Records Management Office*, *Publications Management Office*, *Knowledge Management Office* serta *History Office*.
3. *Knowledge Management* menyediakan dukungan strategis, perumusan kebijakan serta prosedur operasional berdasarkan rekomendasi *Chief Knowledge Officer* (CKO) Departemen Pertahanan.
4. *Project Analysis* yakni membantu pengadaan tenaga ahli untuk menunjang keberhasilan operasi siber yang dirancang, dijalankan dan dievaluasi dengan baik.
5. *Cyberspace Operations Support* (COS) didefinisikan sebagai peran penyediaan personel ahli dalam perencanaan, koordinasi serta sinkronisasi OCO, DCO dan perlindungan infrastruktur DODIN. Realisasi peran USCYBERCOM tersebut

mendorong ketepatan responsif terhadap serangan siber yang selanjutnya dideskripsikan dalam teknis operasi sebagai berikut

a. Memberikan pendampingan teknis terkait manuver operasi, peluncuran senjata siber dan evaluasi dampak pelaksanaan misi.
b. Memastikan *mission assurance* terhadap instruksi operasi pertahanan berbasis siber sesuai dengan ketentuan Departemen Pertahanan.
c. Melakukan riset kritis dan teknis sebagai rekomendasi untuk departemen fungsional dibawah wewenang USCYBERCOM yang kemudian bertanggung jawab penuh untuk mendukung eksekusi misi suatu operasi siber.

6. *Cyberspace Planning* didefinisikan sebagai strategi komprehensif untuk mendorong pengembangan kekuatan siber nasional melalui perancangan program yang efektif, sinkronisasi misi tempur bersama *Combatant Commanders*, satuan lintas angkatan bersenjata, mentransformasikan tujuan-tujuan strategis nasional kedalam tahap implementatif serta menyediakan berbagai pilihan taktis di lapangan. Upaya tersebut diikuti dengan integrasi USCYBERCOM dengan *Cyber National Mission Force* (CNMF) dalam mencapai target-target pertahanan siber nasional.
7. *All-Source Intelligence* merupakan aktifitas USCYBERCOM dalam melakukan riset, analisis operasi, pengumpulan informasi strategis, sistem deteksi peringatan dini dan mitigasi serangan melalui
   a. Melakukan analisis *All Source Intelligence* secara menyeluruh untuk memproduksi catatan evaluasi, laporan misi, artikel, rekomendasi ancaman serta studi strategis.
   b. Memastikan ketersediaan pusat informasi data untuk menunjang akses intelijen siber di seluruh komponen Departemen Pertahanan.
   c. Menggabungkan laporan intelijen dari *Human Intelligence* (HUMINT), *Signals Intelligence* (SIGINT), *Imagery Intelligence* (IMINT), *Measurement and Signatures Intelligence* (MASINT) serta *Open Source Intelligence* untuk memperkuat analisis tempur.
   d. Melakukan *screening* terhadap seluruh sumber informasi intelijen dan merangkum analisis operasi tempur menjadi *actionable intelligence.*
   e. Melakukan *monitoring* keakuratan data intelijen lintas agensi untuk kemudian diolah kedalam perencanaan operasi siber.
   f. Melakukan identifikasi serta evaluasi terhadap *intelligence gaps* yang terkumpul.
8. *Capability Management and Development* merupakan fungsi strategis USCYBERCOM dalam menyediakan pendampingan perumusan dokumen strategis yang akan digunakan dalam perumusan kebijakan siber nasional dan panduan operasi siber di lapangan.
9. *Cyberspace Training and Exercises* didefinisikan sebagai penyediaan tenaga ahli teknis untuk merancang, mengembangkan dan mengadakan pelatihan siber dalam rangka meningkatkan kualitas personel tempur serta kebutuhan operasi yang terus meningkat seiring berjalannya waktu. Setiap tahunnya, USCYBERCOM akan menentukan penyelenggaraan pelatihan kepada *Geographic* COCOM serta menyediakan pendampingan teknis.
10. *Integrated Technology* merupakan inisiasi USCYBERCOM untuk menjaga kredibilitas infrastruktur penunjang operasi siber agar tetap berfungsi dengan

maksimal melalui pemanfaatan berbagai perangkat berteknologi canggih secara bersamaan, yakni

a. Melakukan pengujian sistem serta perangkat jaringan secara berkala.
b. Memastikan ketersediaan jaringan komunikasi dan kelancaran operasional perangkat lunak. Berbagai tindakan sebelum, saat maupun setelah pelaksanaan operasi siber harus memastikan konsep taktis *Command, Control, Communications and Computers* (C4) terintegrasi dengan baik terhadap seluruh komponen Departemen Pertahanan.

11. *Risk Management Framework* (RMF) merupakan peran USCYBERCOM dalam memastikan keamanan siber nasional agar sejalan dengan panduan implementasi dokumen perlindungan jaringan infrastruktur digital dari Departemen Pertahanan
12. *Engagement Activities* adalah rangkaian aktifitas USCYBERCOM untuk bersinergi dengan seluruh komponen pertahanan nasional serta membangun kemitraan aliansi dengan negara lain (Alexander, 2015).

Sentralisasi *Command and Control* (C2) memberikan Amerika Serikat berbagai keuntungan berupa penghematan anggaran operasi siber dalam upaya akuisisi, pelatihan dan optimalisasi eksekusi tempur. Adanya pemusatan tersebut mendorong penguatan kapasitas siber Departemen Pertahanan oleh USCYBERCOM melalui

1. Menyatukan sumber daya siber nasional yang telah ada sebelumnya, menciptakan sinergi lintas agensi dan melakukan sinkronisasi operasi tempur untuk melindungi keamanan informasi.
2. Memusatkan komando siber nasional untuk mengintegrasikan dan memperkuat kapasitas siber Departemen Pertahanan.
3. Meningkatkan kemampuan Departemen Pertahanan untuk memastikan tersedianya perlindungan informasi, jaringan komunikasi, ketahanan dan keamanan akses siber.
4. Memberikan dukungan kepada angkatan bersenjata untuk mencapai keberhasilan misi tempur sekaligus melindungi infrastruktur penunjang operasi dari serangan siber.

B. Peran Perlindungan Taktis USCYBERCOM Dari *Cyber Trespass*

Perlindungan taktis dari upaya *cyber trespass* dapat dimaknai sebagai rangkaian tindakan USCYBERCOM untuk mendeteksi kemudian menghentikan serangan siber terhadap jaringan infrastruktur nasional yang dimaksudkan untuk melakukan pencurian data, merusak sistem komunikasi digital hingga bentuk serangan lainnya yang dapat menimbulkan kerusakan fisik.

Dalam proses selanjutnya, USCYBERCOM memberikan pendampingan perencanaan hingga operasi taktis untuk merumuskan dan mengarahkan satuan tempur di bawah *Operation Order* (OPORD) oleh komandan militer melalui *Joint Operation Planning Process* (JOPP) yang merupakan panduan operasi taktis dengan penjelasan detail mengenai prosedur pelaksanaan suatu misi. JOPP dapat memberikan gambaran mengenai simulasi lapangan kepada komandan tempur, personel dan mitra koalisi terkait untuk memecahkan permasalahan-permasalahan yang berpotensi menganggu kesuksesan operasi tertentu. Pengembangan serta sinkronisasi konsep tempur berbasis militer ditujukan sebagai prasyarat optimalisasi operasi, antara lain

1. *Initiation*: Perencanaan dimulai ketika otoritas domestik memandang perlunya respon militer terhadap suatu ancaman atau serangan yang sedang terjadi. Analisa krisis tahap awal dihasilkan dari instruksi Presiden, *Secretary of Defense* (SecDef) dan *Chairman of the Joint Chiefs of Staff* (CJCS) melalui inisiasi perencanaan operasi militer yang didasarkan pada analisa lapangan, jenis permasalahan dan ketersediaan pilihan-pilihan respon.
2. *Mission Analysis*: Merupakan upaya yang dilakukan untuk mempelajari instruksi-instruksi secara mendalam dengan tujuan mengidentifikasi kebutuhan, kekurangan dan kelebihan operasi tempur. Tahapan ini merupakan komponen penting bagi personel untuk menemukan permasalahan yang dapat menghambat kesuksesan misi (Dunford, 2016).
3. *Course of Action* (COA) *Development*: Unit analisa khusus selanjutnya memberikan pilihan-pilihan COA kepada komandan tempur yang berisi konsep sebelum dan pasca operasi militer. Tahapan ini mendeskripsikan (1) Siapa yang akan bertindak (2) Jenis operasi militer apa yang akan digunakan (3) Waktu pelaksanaan (4) Lokasi tempur (5) Alasan atas opsi-opsi yang tersedia, dan (4) Bagaimana eksekusinya.
4. COA *Analysis, Comparison and Approval*: Merupakan tahapan akhir bagi komandan tempur untuk menentukan beberapa COA yang akan digunakan kemudian melakukan perbandingan melalui identifikasi kelebihan dan kekurangan. Setelah selesai, COA terbaik kemudian menjadi referensi operasi dengan harapan tercapainya kesuksesan misi.
5. *Plan or Order Development*: Personel yang berwenang akan melakukan koordinasi dengan berbagai institusi terkait untuk merancang COA menjadi instruksi spesifik yang disebut dengan *Operations Order* (OPORD) melalui pengembangan operasi taktis *Concept of Operations* (CONOPS). Kedua proses tersebut bertujuan untuk mendeskripsikan target-target pencapaian menggunakan sumber daya militer yang tersedia.

Untuk menunjang operasi militer Amerika Serikat diseluruh dunia dalam rangka mencegah terulangnya peristiwa 9/11, USCYBERCOM menjalankan perannya dengan membentuk dua unit yang berfungsi memberikan dukungan taktis yakni *Cyber Support Element* (CSE) dengan penugasan di markas *Geographic Combatant Commander* dan *Expeditionary Cyber Support Element* (ExCSE) untuk penempatan strategis di wilayah konflik bersama komandan satuan khusus dibawah supervisi *US Strategic Command* (USSTRATCOM).

CSE dan ExCSE bertugas melalui fungsi perencanaan maupun eksekusi operasi ditambah dengan otoritasnya untuk meminta dukungan taktis dari markas pusat USCYBERCOM di Fort Meade. Sejak awal pendiriannya pada 2010, ExCSE beroperasi di Irak dan Afghanistan dengan total lima personel yakni satu *team chief-lead planner*, satu *cyber attack planner*, satu *cyber defense planner* dan dua *cyber-intelligence analyts.* Dalam praktiknya, USCYBERCOM sukses melaksanakan peran CSE dan ExCSE pada

1. *Joint Task Force - Computer Network Defense* (JTF-CND) menerapkan konsep *Network Operations* (NetOps) dengan tujuan untuk menjaga keberlangsungan dan daya tahan jaringan *Global Information Grid* (GIG) milik departemen

pertahanan yang merupakan saluran koordinasi utama seluruh operasi angkatan bersenjata Amerika Serikat diberbagai belahan dunia. Kesimpulan yang dapat kita ambil bahwa USCYBERCOM telah melihat adanya kebutuhan untuk mereformasi skala tempur strategis kepada operasi lapangan dengan otoritas penuh di dalam dan luar negeri. Berkaitan dengan fungsi perlindungan jaringan Departemen Pertahanan, USCYBERCOM memiliki kewajiban untuk memastikan operasi siber berbasis pertahanan dan tempur dapat berjalan dengan baik. Unit ini melaksanakan misi pertahanan siber nasional yang disebut dengan *Operation Gladiator Shield* (OGS) sejak awal pendiriannya dibawah koordinasi USSTRATCOM dengan tujuan melindungi jaringan *Department of Defense Information Network* (DODIN) (Dunford, 2016).

2. Operasi tempur USCYBERCOM banyak menargetkan kelompok teroris melalui otorisasi Menteri Pertahanan Ashton Carter untuk membentuk *Joint Task Force ARES* (JTF-ARES) tahun 2016 hingga 2018 sebagai bagian integral dari misi pasukan *Operation Inherent Resolve* (OIR) yang ditujukan kepada jaringan *Islamic State in Iraq and Syria* (ISIS) dengan penugasan taktis yakni memberikan bantuan siber kepada seluruh koalisi gabungan multinasional dalam operasi tersebut.

Selanjutnya, Letnan Jenderal Stephen Townsend selaku perwira OIR memberikan kesaksian kepada publik yang disimpulkan oleh Dina Temple Raston, salah satu reporter *The Fifth Domain*

> *Pasukan koalisi telah mengetahui letak pos komando ISIS namun belum menemukan pos-pos cadangan lainnya. Pilihan untuk menyerang lokasi tersebut menggunakan rudal dikhawatirkan dapat menghilangkan jejak operasi para teroris tersebut. Letnan Jenderal Stephen Townsend menyebutkan bahwa pasukan koalisi lebih memilih memanfaatkan "multidomain operations", yakni menggunakan serangan siber untuk memancing musuh memindahkan saluran komunikasi ke pos-pos alternatif sehingga membongkar keberadaannya. Setelah lokasi pos alternatif tersebut diketahui, personel tempur di lapangan melakukan penyergapan ke markas operasi musuh yang berukuran kecil kemudian bergerak mengepung markas utama. Walaupun misi berjalan dengan baik, namun perencanaan lapangan memerlukan waktu beberapa bulan dan operasi penyergapan selama satu minggu.*

Jenderal Joseph L. Votel sebagai pimpinan tertinggi *US Central Command* (USCENTCOM) memberikan apresiasinya kepada USCYBERCOM

> *Pada tingkatan taktis, kami telah berhasil mengintegrasikan (operasi siber) dengan satuan tempur khusus di lapangan. Kerjasama ini mampu mengefektifkan misi dan berhasil mengacaukan koordinasi musuh melalui disrupsi jaringan yang ditargetkan pada pusat kendali mereka (ISIS).*

Menteri Pertahanan Ashton Carter dan Jenderal Joseph L. Votel juga menyoroti kesuksesan operasi siber dalam menghambat penyebaran propaganda dan menutup saluran media yang berafiliasi dengan ISIS. Salah satu keberhasilan yang memperoleh apresiasi publik secara luas yakni melakukan kontra narasi berskala internasional untuk

menekan pergerakan ISIS di dunia maya. Selain itu, perwira tinggi di USCENTCOM menyebutkan bahwa kesuksesan dalam misi tersebut memberikan dampak kerusakan yang besar terhadap kemampuan siber ISIS dan menghambat koordinasi tempur mereka di lapangan (Warner, 2020).

Pada November 2016, personel tempur JTF-ARES menerima otorisasi penuh untuk memutus akses pusat komando siber ISIS beserta infrastruktur digital yang tersebar di dunia maya. Dina Temple Raston dalam publikasinya menjelaskan

> *Setelah JTF-ARES mengambil alih 10 jaringan siber inti milik ISIS, mereka kemudian mengunci akses operator agar tidak dapat masuk ke dalam sistem. Selain itu, pasukan JTF-ARES terus menerus menghalangi upaya serangan balasan yang coba dilakukan oleh ISIS. Salah satu personel memberikan keterangan: "Kami menghabiskan sekitar lima sampai enam jam untuk menembaki ikan di dalam drum. Momen seperti ini sudah kami tunggu sejak lama, kami melihat banyak hal-hal buruk terjadi, kami merasa bangga karena dapat mengatasi mereka".*

Jenderal Paul M. Nakasone yang memimpin operasi JTF-ARES menjelaskan

> *Saat enam puluh menit pertama berjalannya misi, saya mengetahui kami sudah berhasil. Target mampu dilumpuhkan satu persatu, sulit menggambarkannya namun saya bisa merasakan atmosfir kemenangan dari ekspresi prajurit, semuanya berjalan dengan baik dan mereka (prajurit) juga menyadari hal itu.*

Selama beberapa bulan setelahnya, satuan tempur JTF-ARES dengan bantuan pasukan koalisi berhasil merusak jaringan media ISIS. Walaupun kehadiran kelompok simpatisan teroris akan selalu ada, misi USCYBERCOM tidak dapat dikatakan gagal karena *Operation Inherent Resolve* yang bertujuan untuk mempersempit wilayah teritorial dan memblokir jaringan komunikasi global ISIS dipandang oleh Jenderal Paul M. Nakasone sebagai penghalang utama mereka untuk kembali beroperasi

> *Mereka (ISIS) saat ini hanya mampu mendistribusikan propaganda berbasis teks apabila dibandingkan dengan produk multimedia sebelumnya yang jauh lebih beragam, diterjemahkan keberbagai bahasa kemudian disebarluaskan secara mudah melalui jaringan internet. Kini mereka bahkan mengalami kesulitan untuk mempublikasikan propaganda berbahasa arab akibat terbatasnya sarana distribusi yang mereka miliki. Hilangnya wilayah teritorial dan rangkaian kekalahan operasi militer ISIS juga menghambat mereka untuk melibatkan diri di dunia maya, namun upaya USCYBERCOM melalui JTF-ARES masih merupakan misi penting dalam menghambat pertumbuhan virtual mereka.*

Setelah serangkaian operasi siber berjalan dengan baik, USCYBERCOM mengkategorikan JTF-ARES sebagai misi tempur terumit yang pernah dieksekusi. Banyak pakar menyebutkan kesuksesan tersebut memiliki dampak positif sebagai tolak ukur *cyber offensive operations* dimasa mendatang. Jenderal Joseph L. Votel

memandang JTF-ARES telah memberikan contoh kesuksesan yang perlu ditiru oleh satuan komando tempur Amerika Serikat di seluruh dunia (Warner, 2020).

Berdasarkan pemaparan di atas mengenai peranan vital USCYBERCOM terhadap keamanan nasional Amerika Serikat, memberikan gambaran spesifik kepada kita mengenai posisi strategis unit pertahanan siber bagi kedaulatan suatu negara. Amerika Serikat melakukan berbagai upaya reformasi dan penguatan terhadap satuan siber yang dimilikinya sebagai respon terhadap kasus pencurian data-data penelitian universitas, institusi militer, perusahaan swasta hingga peretasan infrastruktur vital nasional seperti pembangkit listrik, sistem pengelolaan air dan pusat data pemilihan umum. Efek domino dari rangkaian serangan siber yang terjadi adalah menurunnya kepercayaan publik terhadap keamanan nasional secara keseluruhan serta berkurangnya dominasi militer berbasis siber milik Amerika Serikat apabila dibandingkan dengan Rusia, Tiongkok, Iran hingga Korea Utara.

Oleh karenanya, kehadiran USCYBERCOM untuk melaksanakan perannya sebagai pusat komando siber strategis dan taktis dalam menjaga keamanan nasional sekaligus menjamin kedaulatan Amerika Serikat terhadap domain siber yang dimilikinya. Memastikan tersedianya lapisan pertahanan siber diseluruh lini sipil dan militer secara menyeluruh terbukti mampu memberikan perlindungan efektif dari ancaman serangan siber. Selain itu, berbagai tindakan tersebut merupakan langkah rasional yang dapat dilakukan oleh para pemangku kebijakan untuk memastikan terjaganya kepercayaan publik dan memperkuat dominasi Amerika Serikat sebagai negara adidaya.

Kesimpulan

Permasalahan keamanan siber sebagai salah satu isu keamanan dunia akibat fenomena *Revolution in Military Affairs* yang mendorong dimensi siber menjadi domain kedaulatan baru setelah darat, laut, udara dan antariksa. Komunitas internasional memandang penyalahgunaan ruang siber sebagai senjata terbukti mampu menciptakan eskalasi konflik serta kerusakan layaknya pertempuran konvensional akibat serangan rudal atau bom nuklir.

Amerika Serikat sebagai negara adidaya juga rentan terhadap serangan siber berupa peretasan data, sabotase hingga malfungsi infrastruktur vital nasional. Oleh karenanya pembentukan unit khusus yang berperan menjaga keamanan siber Amerika Serikat seperti USCYBERCOM dipandang perlu untuk menjawab tantangan keamanan melalui perlindungan jaringan, operasi pertahanan dan tempur taktis berbasis siber.

Dalam menjalankan tugasnya, USCYBERCOM menyediakan dukungan penuh terhadap upaya pertahanan nasional dari berbagai ancaman melalui integrasi sistem pertahanan siber nasional dan upaya perlindungan taktis dari *cyber trespass.* Kapasitas untuk melakukan operasi militer sekaligus analisis intelijen yang dimiliki USCYBERCOM terbukti berhasil meningkatkan kedaulatan dalam negeri dan kualitas pertahanan nasional Amerika Serikat secara menyeluruh.

Daftar Pustaka

Alexander, Keith. 2015. “Request For Proposal (RFP) USCYBERCOM Support Contract”. FEDSIM Project. Washington.

Buzan, Barry. 1987. “An Introduction To Strategic Studies: Military Technology and International Relations”, MacMillan Press, London.

_____ 1983. "People, States, and Fear: The National Security Problem in International Relations", Harvester Press Group, Sussex.

Clarke, Richard A. dan Robert K. Knake. 2010. "Cyber War The Next Threat to National Security and What to Do About It", Harper Collins, New York.

Diamond, Celeb. Center for Strategic and International Studies, "Significant Cyber Incidents 2020", tersedia di https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents/

Dunford, Joseph. 2016. "Strategic Cyberspace Operations Guide", US Army War College, Philadelphia.

Edelman, David. 2013. "Cyberattacks In International Relations", University College.

Geers, Kenneth. 2011. "Strategic Cyber Security", CCD COE Publication. Tallin.

Harrison, Heather. 2012 "Cyber Warfare and the Laws of War". Cambridge University. Cambridge.

Holt, Thomas. 2016. "Cybercrime in Progress: Theory and Prevention of Technology Enabled Offenses", Routledge Taylor, London.

Kozlowski, Andrzej. 2014. "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan" dalam European Scientific Journal Volume 3, Poland.

Kramer, Franklin. 2009. "Cyberpower and National Security", Potomac Books, Nebraska.

Lippman, Walter. 1943. "U.S. Foreign Policy: Shield of the Republic", Atlantic Press Group, Boston.

Pipyros, Kosmas, Lilian Mitrou dan Dimitris Gritzalis. 2017. "Evaluating the Effects of Cyber Attacks on Critical Infrastructures in the Context of Tallinn Manual". Athens University. Athens.

Revenon, Derek. 2011. "Human Security in a Borderless World", Routledge, New York.

Senate, US. 2018. "The Cost of Malicious Cyber Activity to the US Economy". The Council of Economic Advisers. Washington.

Sills, David. 1968. "International Encyclopedia of the Social Sciences Volume 1", Macmillan, New York.

Soewardi, Bagus. 2013. "Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) Yang Tangguh Bagi Indonesia" dalam Jurnal Media Informasi Ditjen Pothan Kemenhan (Halm. 31-35). Kementerian Pertahanan. Jakarta.

Warner, Michael. 2020. "US Cyber Command's First Decade". Hoover Institution, New York.

Wood, David. 2015. "2015 Index of US Military Strength", The Heritage Foundation, Washington.

Yar, Majid. 2008. "The Novelty of Cybercrime". University of Kent. Canterburry.

Yates, Joel. 2013. "Cyber Warfare: An Evolution in Warfare not Just War Theory", United States Marine Corps, Philadelphia.