STRATEGI AMERIKA SERIKAT DALAM MENGHADAPI ESKALASI *CYBERPOWER* CHINA TAHUN 2015-2019

Oleh : Ramadani Pasaribu
Ramadani0376@student.unri.ac.id
Pembimbing: Dr. Afrizal, S.IP., MA
Bibliografi : 7 Buku, 3 Dokumen Resmi, 33 Jurnal, 46 Website
Jurusan Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Riau
Kampus Bina Widya Jl. H.R Soebrantas Km. 12,5 Simp. Baru Pekanbaru
28293Telp/Fax 07561-63277

ABSTRAK

Pesatnya perkembangan dan kemajuan teknologi di abad ke-21 membawa istilah *cyberpower* sebagai konsep baru dalam hubungan internasional. Selama beberapa dekade terakhir China menjadi sangat agresif dalam kemajuan teknologi nya dan berkeinginan menjadi segara *cyberpower* sebagaimana pidato Xi-Jinping tahun 2013. Eskalasi *cyberpower* China memberikan efek tersendiri bagi Amerika. China dengan niatnya sebagai negara *cyberpower* dapat menggeser posisi Amerika Serikat sebagai "aktor dominan" dan di sisi lain eskalasi *cyberpower* China merugikan Amerika Serikat dengan banyaknya serangan yang ditujukan padanya. Perubahan signifikan dan demikian cepat pada China dalam dekade terakhir patut menjadi perhatian banyak negara terutama Amerika. Dalam upaya menanggapi kondisi tersebut, Amerika merilis strategi pertahan baru yang dikenal dengan istilah *defence-forward strategy*. Strategi *defence-forward* mencerminkan konsep dasar ofensif disamping pertahanan defensif. Strategi ini memungkinkan Amerika untuk melakukan operasi di luar batas geografis nya. *Defence-forward strategy* diimplementasikan dengan langkah-langkah diantaranya; meningkatkan kemampuan *cyberpower*, membangun kerjasama *cyber security* China-AS, membangun aliansi pertahanan kolektif global serta berupa untuk membangun pengaruh Amerika dalam *cyberspace* melalui partisipasi organisasi multilateral, merekomendasikan norma-norma serta tata kelola *cyberspace* yang sesuai dengan nilai-nilai nasional Amerika Serikat.

Kata kunci: Cyberpower, Cyberspace, Defence-forward Strategy,* AmerikaSerikat, China, *Cybersecurity-Dilemma.

Strategi Amerika Serikat dalam Menghadapi Eskalasi *Cyberpower* China Tahun 2015-2019

Oleh : Ramadani Pasaribu
Ramadani0376@student.unri.ac.id
Pembimbing: Dr. Afrizal, S.IP., MA
Bibliografi : 7 Buku, 3 Dokumen Resmi, 33 Jurnal, 46 Website
Jurusan Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Riau
Kampus Bina Widya Jl. H.R Soebrantas Km. 12,5 Simp. Baru Pekanbaru
28293Telp/Fax 07561-63277

ABSTRACT

The rapid development and advancement of technology in the 21st century brings the term cyberpower as a new concept in international relations. over the last few decades China has become very aggressive in its technological advancements and wants to become cyberpower immediately as Xi-Jinping's speech in 2013. The escalation of China's cyberpower has had its own effect on America. on the one hand China with its intention as a cyberpower country can shift the position of the United States as the "dominant actor" and on the other hand China's escalation of cyberpower harms the United States with the number of attacks aimed at it. Significant and rapid changes in China in the last decade deserve the attention of many countries, especially America. In an effort to respond to these conditions, America released a new defense strategy known as the Defense-forward strategy. The defense-forward strategy reflects the basic concept of offensive as well as defensive defence. This strategy allowed America to conduct operations beyond its geographic boundaries. The defense-forward strategy is implemented with the following steps; enhance cyberpower capabilities, build China-US cyber security cooperation, build global collective defense alliances and seek to build American influence in cyberspace through the participation of multilateral organizations, recommending cyberspace norms and governance in accordance with US national values.

Keywords: Cyberpower, Cyberspace, Defense-forward Strategy, United States of America, China, Cyber security-dilemma.

Pendahuluan

Perkembangan dan kemajuan teknologi di abad-21 menyebabkan banyak perubahan, terutama dalam konteks ukuran kekuatan negara. kemajuan adalah dampak dari persaingan yang menginginkan kekuatan. Abad ini kekuatan suatu negara tidak hanya diukur dari kemampuan fisik militer nya saja melainkan dilihat juga dari sisi kemampuan *cyberpower* nya.

Sistem siber yang kompleks menciptakan kerentanan baru bagi setiap negara dimana kerentanan sistem siber dapat dieksploitasi oleh aktor-aktor negara maupun non-negara. Konsep kekuasaan atau *power* antar negara pun telah diubah karena integrasi dunia maya ke dalam bentuk kekuatan yang sulit dinilai secara fisik.[1]

Pesatnya perkembangan dan dominasi *cyberspace* membuat dunia semakin bergantung pada jaringan informasi dalam segala aspek, termasuk di bidang pertahanan dan kekuatan negara. Bertambahnya ruang dalam interaksi, memperluas makna kekuasaan dalam hubungan antar negara.

Selama beberapa dekade terakhir, China mejadi negara yang sangat agresif dalam berbagai kemajuan perkembangan teknologi nya. China bercita-cita menjadi negara *cyberpower*, dimana China mampu menggantikan posisi negaranya adidaya yakni Amerika Serikat. Perubahan menuju negara *cyberpower* dapat ditandai melalui pidatonya Xi-jinping tahun 2013, yang menekankan upaya modernisasi China dalam segala bidang termasuk pada PLA dan unit-unit pemerintah lainnya.

Xi-Jinping melakukan reorganisasi struktur tentara pembebasan rakyat (PLA). Reformasi bertujuan untuk meningkatkan kemampuan operasi *cyber warfare*, fokus pengembangan siber dan serta aset pengembangan ruang angkasa (cyber space). Reformasi ini merupakan usaha untuk memusatkan dan menekankan elemen militer dan pemerintah yang terlibat dalam semua aktivitas siber.[2]

A. Eskalasi *Cyberpower* China

Eskalasi *cyberpower* China dapat diukur melalui beberapa indikator, diantaranya;

a). *Legal and Policy Framework*
b). Domestic State Cyber Structures
c). Evidence of Attack
d).Cyber Vulnerability Mitigation
e).Private Sector, Trade, and Innovation.

Indikator ini di dikenal dengan *National Cyber Power Index* (NCPI) Belfer 2020. Indikator ini memusatkan pengukuran yang dikelompokkan dalam beberapa bidang diantaranya; sektor swasta, perdagangan dan inovasi teknologi yang diukur dari segi kualitas dan kuantitas, hukum dan standarisasi, struktur siber domestik suatu negara, kekuatan yang dibuktikan dengan serangan, mitigasi ancaman siber.

Kemajuan China dari segi *private sector, trade, and innovation* menunjukkan pertumbuhan yang sangat signifikan pada pertumbuhan perusahan teknologi di China. Setidaknya total ada 32.027 perusahaan teknologi tinggi di China pada tahun 2017. Total kenaikan 7.342

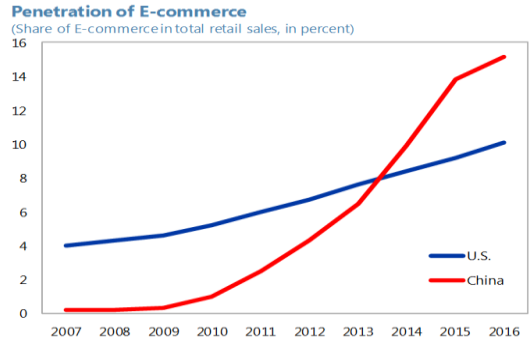
[1]Cyril K Yancey and Richard Stahler-Sholk, 'Cyber Security: China and Russia'S Erosion of 21 St Century United States' Hegemony', *McNair Scholars Research Journal*, 12.1 (2019), 9.

[2]FireEye."RedLine: China Recalculates Its Use Of Cyber Espionage. Https://Www.Fireeye.Com/Content/Dam/Fireeye-Www/Current-Threats/Pdfs/Rpt-China-Espionage.Pdf

perusahaan atau 24 % dalam rentang tahun 2013-2017.[3]

Pada tahun 2013, volume barang dagangan kotor pada belanja online berjumlah sekitar 1,9 triliun yuan. Pada tahun 2016, volume pasar mobile e-commerce di Cina telah mencapai sekitar 4,5 triliun. Meningkat sekitar 151 % dari tahun 2015. Sedangkan transaksi e-commerce pada tahun 2019 secara keseluruhan sekitar 34,8 triliun yuan, yang meningkat sekitar 31.6 triliun yuan dari tahun sebelumnya (2018).

Perbandingan E-commerce China-AS



Kemajuan dan perkembangan China dalam bidang siber juga di ukur dari segi keberadaan hukum dan aturan yang mengatur segala aktivitas yang berkaitan dengan sistem siber di negara tersebut.

Pada 7 November 2016, pemerintah China mengesahkan undang-undang keamanan siber China atau *Cyber Security Law* (CSL) melalui komite tetap kongres nasional, sebagai bagian dari rangkaian undang-undang yang lebih luas terkait dengan keamanan nasional China. Sebagai upaya meningkatkan keamanan nasional negara nya, China dinilai sangat ketat dalam aturan, hukum maupun regulasi.

Undang-undang yang baru ini dibuat untuk mengikat seluruh elemen dan sektor serta melakukan kolaborasi dalam berbagai sektor yang dianggap perlu bagi keamanan dunia maya jangka panjang China. Undang-undang dalam tata kelola yang baru dibentuk ini bukan hanya mencakup sektor nasional dan perusahaan nasional akan tetapi juga berlaku bagi perusahaan asing yang beroperasi di China.

Undang ini mengharuskan setiap perusahaan untuk tunduk atas regulasi pemerintah domestik dan aturan nasional pemerintah China. selain itu China juga membentuk aturan hukum dan standarisasi lainnya termasuk *Data Security Law.* Sebuah aturan perlindungan terhadap data dan keamanan nasional, undang-undang ini mengambil peran penting dalam mengatur penciptaan, penggunaan dan transfer data di China.

China mempunyai *Domestic State Cyber Structures*, dimana ini menjadi salah satu poin penting dalam mengukur kemampuan *cyberpower* negara. poin ini menjadi indikator apakah negara mempunyai struktur siber domestik dan apakah struktur tersebut terstruktur dengan jelas. China dalam struktur siber domestik tergolong sangat kompleks. Dimana setiap bagian dari unit lembaga pemerintahan saling terkait dan terhubung satu sama lain. Komponen militer, Ekonomi maupun pemerintahan terintegrasi dan terhubung dalam komponen siber yang sangat kompleks.

Kemampuan China dalam *syberpower* nya juga ditunjukkan melalui bukti serangan siber atau evidence of attack baik yang bersifat internal maupun bersifat external. Salah satu bukti kemampuan tinggi dan kecanggihan China ialah Ghosnet yang berhasil menyerang 103 negara dengan menembus sekitar 1000 komputer. Journal *analytic of china cyber attack* menyebutkan setidaknya 10 dari

[3] "Number of high-tech companies in China from 1995 to 2017" https://www.statista.com/statistics/234116/number-of-high-tech-companies-in-china/ diakses 28 agustus 2021

peretasan komputer terburuk yang pernah ada, China terlibat di dalamnya.

Kemampuan melakukan serangan juga berbanding lurus dengan kemampuan China dalam memproteksi atau me mitigasi serangan maupun ancaman siber terhadap China. Great firewall merupakan salah satu diantara bentuk proteksi terhadap akses masuk berbahaya yang datang dari luar. The Great Cannon of China ini merupakan alat offensive sekaligus defensive yang bekerja serangkaian dengan GFWoC. Alat ini mampu menolak sekaligus merusak sistem penyerang yang datang dari luar. Selain itu China juga memiliki "Great Cannon of China" merupakan alat atau senjata teknologi berkapasitas tinggi yang berfungsi sebagai penolakan jaringan serangan DoD.

B. *Cyberpower* China Menjadi Ancaman bagi Amerika Serikat

Kemajuan dan perkembangan China dalam cyberspace tidak dapat di pungkiri dan menjadi perhatian banyak negara diantaranya Amerika Serikat. Amerika Serikat menjadi negara yang paling banyak dirugikan atas eskalasi *cyberpower* China. hal ini dibuktikan dengan dengan banyaknya jumlah serangan berupa penyusupan, peretasan, cyber espionage, cyber crime China terhadap Amerika Serikat.

China merupakan negara sumber serangan utama cyber terhadap Amerika berupa cyber attack, cyber espionage dan berbagai serangan jaringan lainnya. serangan APT 1, Serangan APT 3 dan APT 10.[4] Singkatannya, kemajuan kemampuan cyber China adalah ancaman bagi Amerika.

Permasalahan *cyber attack* merupakan hal yang krusial dalam hubungan antara Amerika Serikat dan China. *Cyber attack* merupakan suatu masalah global yang harus di selesaikan dengan kerjasama internasional yang konstruktif yang didasarkan pada rasa saling percaya dan rasa saling hormat antar negara guna membentuk peraturan-peraturan terkait dengan dunia maya.

Pada tahun 2013 China dan Amerika memprakarsai dialog bilateral formal terkait dunia maya. Namun hingga mei 2014 pemerintah China memutuskan untuk tidak melanjutkan dialog tersebut, bersamaan dengan dijatuhkannya hukum dakwaan atas lima perwira PLA atas tuduhan *cyber espionage* terhadap perusahaan Amerika oleh Departemen Kehakiman Amerika Serikat.

Penafsiran yang berbeda tentang ruang siber membawa perselisihan terhadap kedua negara. Amerika Serikat lebih menempatkan keamanan siber sebagai prioritas dalam kebijakan luar negerinya dengan semakin agresif nya tindakan China dalam mencapai tujuannya sebagai negara kekuatan siber.[5]

C. *Stratrategy* Amerika Menghadapi Eskalasi *Cyberpower* China

Amerika merilis *defense-forward* strategi sebagai acuan dasar as dalam semua aktifitas yang berkaitan dengan aktifitas siber. *Defense-forward strategy* memiliki tiga prinsip utama yakni; kekuatan dan pertahanan strategis, bertahan ke depan dan siap untuk berperang. Secara eksplisit strategi ini merupakan respon atas ancaman siber yang sering melibatkan negara rival

[4] Clayton, M. "US indicts five in China's secret 'Unit 61398' for cyber-spying". https://www.csmonitor.com/World/Passcode/2014/0519/US-indicts-five-in-China-s-secret-Unit-61398-for-cyber-spying-on-US-firms

[5] Dewi Triwahyuni, 'American Foreign Policy in Cyberspace', 391 (2020), 48–51 <https://doi.org/10.2991/assehr.k.200108.010>.

Amerika seperti China, rusia, Iran dan Korea Selatan. Fokus strategi ini jelas tidak lagi hanya menjadikan pencegahan sebagai pilar utama namun pada level tingkat lanjut pada posisi siap pada level *ofensif* terbatas.[6] Pertama strategi *defense-forward* berusaha untuk menggunakan atau mengerahkan segenap opsi sumber daya yang ada untuk pertahanan siber dan penegakan hukum untuk untak mengurangi potensi atau resiko yang membahayakan keamanan nasional AS dan kepentingannya.

Meskipun cenderung pada strategi pertahanan dari, serangan cyber dan peningkatan kemampuan internal, Amerika Serikat memiliki strategi internasional terkait dengan cyberspace, terutama karena jaringan cyber sekarang terkenal di seluruh dunia sehingga tidak mungkin untuk fokus hanya pada kemampuan domestik.

Setelah merilis strategi nasional untuk menangani keamanan siber pada tahun 2003, pada Mei 2011 Gedung Putih merilis Strategi Internasional untuk Dunia Siber dan menyatakan: "Amerika Serikat akan bekerja secara internasional untuk mempromosikan informasi dan infrastruktur komunikasi yang memiliki potensi besar untuk mempengaruhi aktivitas dunia Barat di dunia maya karena beberapa alasan.

Strategi Dunia Maya Amerika Serikat Meskipun cenderung pada strategi pertahanan dari serangan cyber dan peningkatan kemampuan internal, Amerika Serikat memiliki strategi internasional terkait dengan cyberspace, terutama karena jaringan cyber sekarang terkenal di seluruh dunia sehingga tidak mungkin untuk fokus hanya pada kemampuan domestik.

Setelah merilis strategi nasional untuk menangani keamanan siber pada tahun 2003, pada Mei 2011 Gedung Putih merilis Strategi Internasional untuk Dunia Siber dan menyatakan: "Amerika Serikat akan bekerja secara internasional untuk mempromosikan informasi dan infrastruktur komunikasi yang mendukung perdagangan dan perdagangan internasional, memperkuat keamanan internasional, dan mendorong kebebasan berekspresi dan inovasi.

Dokumen tersebut, Amerika Serikat menegaskan bahwa negaranya terus melakukan tindakan untuk membantu membangun dan memelihara jaringan yang terbuka, aman, dan terpercaya baik di dalam maupun di luar negeri, baik bagi warga AS maupun komunitas global. Amerika Serikat berfokus pada tujuh bidang penting yang sebenarnya saling terkait dan membutuhkan kolaborasi dari pemerintah, mitra internasional, dan sektor swasta yang ada.

Paradigma yang dianut China mengenai internet dan *cyberpower* memiliki perbedaan dengan paradigma AS. Perbedaan ini tidak hanya mengarah pada arah perkembangan internet yang berbeda, tetapi dalam beberapa kasus menyebabkan konflik kepentingan antara China dan AS, China melihat internet dan mengarahkan perkembangan *cyberpower* nya pada dua hal utama.

Pertama, China mengembangkan teknologi komunikasi untuk memperkuat efisiensi organisasi pemerintah. Kedua, China ingin menggunakan teknologi komunikasi untuk menjaga legitimasi Partai Komunis. Pengetahuan tersebut berbenturan dengan asumsi AS yang lebih condong pada Pengetahuan tersebut

[6] Nina kollars and jacquelyn Schneider, "Defending forward: the 2018 cyber strategy is here" https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/ 02/09/2021

berbenturan dengan asumsi AS yang lebih condong pada asumsi terkait teknologi informasi dan hubungannya dengan komunikasi politik. AS berasumsi bahwa teknologi informasi dan demokrasi memiliki paradigma yang sama, yaitu arus informasi yang bebas.

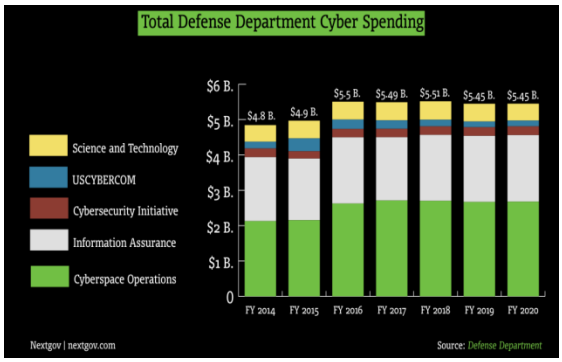
Amerika merilis *defense-forward* strategi sebagai acuan dasar as dalam semua aktifitas yang berkaitan dengan aktifitas siber. *Defense-forward strategy* memiliki tiga prinsip utama yakni; kekuatan dan pertahanan strategis, bertahan ke depan dan siap untuk berperang. Secara eksplisit strategi ini merupakan respon atas ancaman siber yang sering melibatkan negara rival Amerika seperti China, rusia, Iran dan korea Selatan. Fokus strategi ini jelas tidak lagi hanya menjadikan pencegahan sebagai pilar utama namun pada level tingkat lanjut pada posisi siap pada level ofensif terbatas.[7]

Pertama strategi *defense-forward* berusaha untuk menggunakan atau mengerahkan segenap opsi sumber daya yang ada untuk pertahanan siber dan penegakan hukum untuk untak mengurangi potensi atau resiko yang membahayakan keamanan nasional AS dan kepentingannya. Strategi *Defense-forward* dalam istilah lain ialah konsep bertahan ke depan, artinya AS menekankan pada dasar-dasar pertahanan yang kuat yang dibarengi dengan aktivitas yang proaktif.

a). Meningkatkan Pertahanan dan Kemampuan *Cyber*

Dalam upaya memperkuat keamanan dan meningkatkan pertahanan terhadap ancaman cyber, Departemen Pertahanan Amerika serikat membentuk cyber mission forced (SMF) pada tahun 2013. SMF bertujuan dalam merekrut ahli siber untuk ditempatkan di beberapa unit satuan cyber Amerika serikat. Upaya peningkatan kemampuan dan pertahanan, AS menambah jumlah anggota operator cyber hingga mencapai target yang telah ditentukan.

Sejak tahun 2013 SMF menargetkan pasukan misi siber terdiri dari 133 tim yakni 3100 hingga mencapai target 6100 operator siber di tahun 2018. Dari rentang tahun 2014-2018, misi ini telah menghabiskan $1,878 miliar dolar untuk membayar pasukan misi siber. Upaya misi siber ini juga dilengkapi dengan peralatan kasus untuk mendukung operasi di dunia maya.[8]



Amerika Serikat mengalokasikan budget yang cukup besar sepanjang tahun 2014 hingga 2020. AS bahkan mengalokasikan dana sebesar 1 miliar dollar USD dalam rentang lima tahunan. Alokasi itu ditujukan untuk mengatur maneuver pertahanan jaringan, pertahanan dari ancaman serta serangan ofensif. Tahun 2014, pasukan didanai sebesar 546 juta USD. Sementara tahun 2015, diperkirakan akan mencapai 509 juta USD.

[7] Nina kollars and jacquelyn Schneider, "Defending forward: the 2018 cyber strategy is here" https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/ 02/09/2021

[8]Steven, Aftergood."Pentagon's Cyber Mission Force Takes Shape." https://fas.org/blogs/secrecy/2015/09/dod-cmf/ diakses pada 24 agustus 2021

b). Mejalin Dialog Kerjasama *Cyber Security* China-AS

Pada 24-25 September 2015, Xi-Jinping dan Barack Obama membuat kesepakatan bersama tentang keamanan siber. Pertemuan kedua negara menjadi sangat berarti setelah beberapa tahun sebelumnya hubungan kedua negara diwarnai dengan saling kritik dalam masalah *cyber crime*. Perjanjian ini setuju untuk tidak saling meretas perusahaan pribadi masing-masing untuk keuntungan komersial dan aktivitas dunia maya yang merugikan lainnya.

Intinya, China dan Amerika Serikat sepakat untuk bersama-sama:1) Memberikan tanggapan yang tepat waktu atas permintaan informasi dan bantuan terkait aktivitas siber yang berbahaya. 2) Menahan diri untuk tidak terlibat atau dengan sengaja/sadar mendukung pencurian kekayaan intelektual. 3) Mengejar upaya untuk mempromosikan norma-norma perilaku negara yang sesuai di dunia maya di masyarakat internasional, dan membangun mekanisme dialog bersama tingkat tinggi untuk memerangi kejahatan dunia maya dan isu-isu terkait.

Berdasarkan kesepakatan dalam kesepakatan khususnya poin keempat, sejak tahun 2015 kedua negara secara konsisten mengadakan dialog tingkat tinggi secara terus menerus untuk terus meningkatkan kesepakatan keamanan siber kedua negara.[9]

c). Membangun Aliansi Pertahanan Kolektif

Kerentanan terhadap ancaman siber memerlukan upaya kolektif dalam menghadapi ancaman yang sama dalam *cyberspace*. Amerika dalam hal ini terus membentuk aliansi dan membangun mitra kerja sama global untuk meningkatkan kapasitasnya serta proteksi terhadap ancaman bersama. Membangun aliansi dan pertahan bersama di level internasional menjadi suatu upaya efektif dalam menerapkan kebijakan dan praktik pencegahan ancaman dan kejahatan siber. Amerika membangun aliansi kolektif yang menjangkau berbagai awasan diantaranya; *United Kingdom–United States of America Agreement* (UKUSA), mitra perjanjian Timur tengah, Asia-Pasifik dan Eropa.[10]

Pada 7 Desember 2015 Amerika Serikat dan Uni Eropa menjalin kerjasama bilateral maupun multilateral dalam konteks isu-isu terkait siber. Kerjasama ini didasarkan pada nilai-nilai yang sama atas isu keamanan siber, kebebasan internet, dan aturan tata kelola dalam dunia maya. Dialog strategis AS-UE menjadi platform koordinasi antar dua negara.

Kolaborasi AS-UE meresmikan dan memperluas hubungan kedua negara tersebut melalui KTT AS-UE pada tahun 2014. Pembahasan KTT mencakup beberapa poin diantaranya: a. perkembangan dunia maya Internasional, b. peningkatan kapasitas keamanan dunia maya di negara ketiga, c. mempromosikan perlindungan hak asasi manusia secara online, serta d. membahas masalah norma perilaku di dunia maya, langkah-langkah membangun kepercayaan keamanan dunia maya dan penerapan hukum internasional dalam dunia maya.[11] Di depan internasional, Departemen Luar Negeri, program di Departemen Kehakiman, dan Badan Pembangunan Internasional Amerika Serikat bekerja untuk

[9] ATLANTIS PRESS. Opcit., hlm. 225

[10]The White House, 'National Cyber Strategy of the United States of America', September, 2018, 1–40 .

[11]FACT SHEET: U.S.-EU Cyber Cooperation. https://obamawhitehouse.archives.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation

membangun kapasitas sistem peradilan pidana global untuk menyelidiki dan menuntut kejahatan dunia maya dan meningkatkan kerja sama internasional dalam upaya ini.[12]

Amerika bermitra dengan pemerintah dan entitas asing untuk meningkatkan postur pertahanan keamanan siber global . Ini mendukung keterlibatan bilateral, seperti kegiatan berbagi informasi/pembangunan kepercayaan antar CERT, peningkatan yang terkait dengan kolaborasi global, dan kesepakatan tentang standar berbagi data. US-CERT bertanggung jawab untuk menganalisis dan mengurangi ancaman dunia maya, kerentanan, menyebarkan informasi peringatan ancaman dunia maya, dan mengkoordinasikan kegiatan respons insiden.[13]

d). Membangun pengaruh AS dalam Cyberspace

Pilar ke empat dalam dokumen *National Cyber Strategy* Amerika disebutkan tujuan amerika untuk mempertahankan postur kepemimpinan internasional yang aktif untuk memajukan pengaruh Amerika. Amerika aktif dalam melakukan kerjasama, bermitra maupun berafiliasi baik dengan negara maupun organisasi internasional utama dalam upaya membangun dan menciptakan pengaruhnya. Amerika serikat terus berpartisipasi aktif untuk mempromosikan ide-ide serta nilai-nilai keterbukaan di lingkup *cyberspace.*

Amerika sangat gencar mempromosikan model tata kelola internet yang terbuka agar menang melawan model tata kelola tertutup (seperti China) yang hanya berpusat pada kepentingan satu negara. selain itu amerika juga terus mempromosikan norma atau aturan main dalam *cyberspace* yang mendorong tindakan bertanggungjawab dalam aktivitas di domain *cyberspace*.

Amerika Serikat terus aktif mempromosikan kedua hal tersebut dalam forum multilateral dan internasional melalui keterlibatan secara aktif dalam organisasi-organisasi utama seperti; *Internet Corporation for Assigned Names and Numbers* (ICANN), *International Telecommunication Union* (ITU), *United Nation* (PBB) serta Forum Tata Kelola Internet lainnya.[14]

Amerika telah ikut berpartisipasi dalam forum internasional selama beberapa dekade dalam membangun konsensus seputar kerangka perilaku negara yang bertanggungjawab dalam dunia maya. Terutama melalui rekomendasi pembentukan norma-norma tidak mengikat yang direkomendasikan Amerika melalui *Group of Governmental Experts* (GEE). Dalam rangka memajukan hukum dan norma internasional, Presiden Obama meminta kelompok ahli pemerintah (GEE) untuk mempertimbangkan keamanan internasional dan teknologi siber internasional.[15] Permintaan presiden Obama dipertimbangkan oleh GEE, hingga pada tahun 2013 menawarkan norma-norma yang tidak mengikat untuk dipertimbangkan oleh PBB, termasuk dua

[12] THIRD WAY 2015. Opcit., hlm 8

[13]DHS Cyber Security. US-CERT United States Computer Emergency Readiness Team. https://us-cert.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf 22/07/2021

[14]The White House., hlm. 35

[15] David P. Fidler. 2017. The U.S. Election Hacks, Cybersecurity, and International Law. https://core.ac.uk/download/pdf/232678154.pdf diakses pada 23 agustus 2021

point yang dipromosikan Amerika Serikat.[16]

Amerika sebagai keanggotaannya dalam negara-negara yang tergabung dalam G7 turut mempromosikan perilaku bertanggung jawab dalam dunia maya. Negara-negara yang tergabung dalam G7 diantaranya Amerika, Inggris, Kanada, Prancis, Jerman, Italia, dan Jepang mengeluarkan *G7 Declaration On Responsible States Behavior In Cyberspace* pada 11 april 2017 di Lucca, Italia. Deklarasi tersebut menggarisbawahi 12 poin penting yang menjadi sorotan utama dalam aturan dan tanggung jawab dalam perilaku dunia maya.[17]

Amerika beserta negara-negara yang tergabung dalam G7 sepakat untuk melakukan kerjasama dalam mengembangkan dan menetapkan langkah-langkah untuk meningkatkan stabilitas keamanan dunia maya dan mencegah praktik yang dapat merugikan keamanan internasional. Selain itu negara juga dilarang melakukan atau mendukung pencurian kekayaan intelektual serta negara dilarang untuk membiarkan wilayahnya digunakan untuk tindakan yang melanggar keamanan.

Selain itu Amerika berpartisipasi dalam CCD COE (The NATO Cooperative Cyber Defence Centre of Excellence) yang merupakan sebuah aliansi pusat keunggulan pertahanan yang dibentuk di Tallinn, Estonia. Amerika Serikat ikut berpartisipasi dengan menjadi salah satu anggota dari CCD COE.[18] Dengan menjadi bagian dari aliansi ini berarti Amerika menunjukkan perannya dalam meningkatkan keamanan dan pertahan dunia maya.

KESIMPULAN

Eskalasi *cyberpower* yang dilakukan China tersebut di satu sisi menjadi ancaman bagi keamanan nasional Amerika Serikat dan kepentingannya dalam hubungan internasional. Eskalasi *cyberpower* China sangat memberikan potensi ancaman besar bagi Keamanan nasional Amerika dikarenakan hubungan kedua negara yang sangat fluktuatif. China menunjukkan keinginannya yang kuat untuk menjadi negara *cyberpower* menggantikan posisi Amerika. Eskalasi *cyberpower* China berpotensi untuk melakukan serangan yang lebih besar terhadap Amerika khususnya dalam dunia maya berupa *cyber attack*.

Hubungan Amerika dan China sudah sejak lama ditandai dengan perlombaan dan persaingan yang kompetitif. Kedua negara seolah tidak ingin didahului oleh kekuatan negara lain kecuali juga turut menambah kekuatan. Ancaman baru di era baru menuntut untuk merespon dengan strategi baru untuk mengurangi kerentanan, memitigasi serangan, menghalangi dan melindungi potensi dari ancaman keamanan nasional amerika.

Amerika menggunakan pendekatan *Defend-forward Strategy* dalam menghadapi China dalam konteks hubungan *cyberpower*. Strategi ini merupakan strategi baru yang dikeluarkan oleh departemen pertahan siber sebagai respon atas vitalitas atas rentan nya domain siber dari ancaman serangan

[16]Joseph, Marks. U.N. body agrees to U.S. norms in cyberspace. https://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900

[17]"G7 Declaration On Responsible States Behavior In Cyberspace'.

[18]Anna-Maria Osula and Henry International Cyber Norms Legal, Policy & Industry Perspectives. https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf

terhadap Amerika terutama yang berasal dari China dan Rusia.

Defend-forward Strategy mendasari upaya Amerika Serikat untuk meningkatkan pertahanan nya dalam menghadapi maupun mencegah dari kemungkinan ancaman disamping juga mempersiapkan kemampuan yang memadai dan siap melakukan serangan balik apabila diperlukan. Sementara itu, strategi ini juga mengharuskan AS untuk memperkuat postur pertahanan AS dengan meningkatkan kerjasama dengan sekutu dan mitra hubungan internasional AS disamping menjalin kerjasama dengan sektor swasta dalam bidang pertahanan lainnya dalam level domestik.

Strategi defend-forward ini diimplementasikan dalam beberapa langkah strategis yaitu dengan meningkatkan keamanan nasional terutama infrastruktur digital, melakukan optimalisasi unit-unit siber & meningkatkan kapabilitas ketahanan dan keamanan siber domestik, menjalin hubungan kerjasama dengan China dan negara-negara lain seperti Inggris, Brazil, dan Jepang, serta melakukan turut serta dalam mempromosikan pembentukan aturan-aturan atau norma-norma dalam dunia maya.

Defend-forward strategy Amerika serikat merupakan langkah logis dalam menghadapi eskalasi *cyberpower* China. *Strategi defensive-forward ini* digambarkan dalam dua konsep pertahanan, yakni pertahanan kedalam dan pertahanan keluar. Bertahan ke dalam dengan memperkuat postur keamanan negara dan pertahanan keluar me mungkinkan menyiapkan serta meningkatkan kemampuan jika sewaktu-waktu serangan ofensif diperlukan.

Defense-forward strategy menggambarkan disamping meningkatkan kemampuan dan pertahanan namun di sisi lain juga "Strategi bertahan" merujuk makna memaksimalkan kemampuan negara dari serangan atau potensi ancaman yang membahayakan kepentingan nasional. "Strategi maju" merujuk pada makna menempati posisi terdepan dalam mitigasi kemungkinan serangan dengan operasi intelegensi dan melakukan ancaman atau serangan balik atas serangan yang masuk. Strategi ini menjadi efektif, disamping dapat meminimalisir resiko maupun serangan yang kepada Amerika serikat dan di sisi lain juga tetap menjaga eksistensi Amerika Serikat dalam ukuran kemampuan siber nya.

Strategi ini menempatkan AS pada posisi yang seimbang dimana Amerika berupaya mampu bertahan atas ancaman maupun serangan yang datang dan di sisi lain juga mempunyai kemampuan ofensif dengan melakukan serangan balik atas serangan yang ditujukan pada Amerika Serikat.

Melalui *Defend-forward Strategy* Amerika Serikat menjaga keunggulan dalam kemampuan siber dengan mengkoordinasikan semua unit untuk berkolaborasi dalam pengembangan kemampuan siber sebagaimana yang dilakukan China. sedangkan di sisi lain Amerika juga mampu membalas serangan yang datang yang menunjukkan Amerika mempunyai kemampuan ofensif yang harus dipertimbangkan.

DAFTAR PUSTAKA

Nocetti, Julien. 2018. "CyberPower." *Routledge Handbook of Russian Foreign Policy*, no. May: 182–98. https://doi.org/10.4324/9781315536934.

Valeriano, Brandon, and Ryan C. Maness. 2018. "International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain." *The Oxford Handbook of International Political Theory*, no. April: 259–72. https://doi.org/10.1093/oxfordhb/9780198746928.013.19.

"Scan Book-English School.Pdf." n.d.

Vinsensio Dugis. 2018. *Teori Hubungan Internasional Perspektif-Perspektif Klasik. Neorealisme*. https://www.researchgate.net/profile/Vinsensio_Dugis/publication/321709080_Teori_Hubungan_Internasional_Perspektif-Perspektif_Klasik/links/5a2c36a00f7e9b63e53adfed/Teori-Hubungan-Internasional-Perspektif-Perspektif-Klasik.pdf.

THE DEPARTMENT OF DEFENSE CYBER STRATEGY (April 2015) dari https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/dod_cyber_2015.pdf

Jensen, Benjamin, and Brandon Valeriano. 2019. "What Do We Know About Cyber Escalation? Observations From Simulations and Surveys." *Atlantic Council*, 1–14.

Elisa, Samuel. 2020. "Analisis Kehadiran China Sebagai Superpower Country Sekaligus Rival Amerika Serikat Dalam Perspektif Realisme Struktural Ofensif," no. June.

TRIWAHYUNI, D. 2017. "The Impact of China'S Cyberpower Development on the Interest of the United States." *Academia.Edu*, no. December: 2015–18. https://www.academia.edu/download/55836200/1261-151748611126-29.pdf

ITU. 2015. "Cybersecurity Index of Indices." https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Index_of_Indices_GCI.pdf.

CNNIC. 2019. "Statistical Report on Internet Development in China (August 2019)." *China Internet Network Information Center*, no. August: 57. http://www1.cnnic.cn/IDR/ReportDownloads/201302/P020130221391269963814.pdf.

Olender, Michael. 2015. "Keeping Pace with Cyber Power, Defense, and Warfare." *Journal of International and Global Studies* 6 (2): 55–61.

Serikat, Kepentingan Amerika. 2018. "JIPSi" VIII (1).

Triwahyuni, Dewi, Yanyan Mochamad Yani, and Arry Bainus. 2019. "Foreign Policy of The United States of America in Addressing China's Cyberpower" 225 (Icobest): 302–6. https://doi.org/10.2991/icobest-18.2018.66.

Zhang, Li. 2013. "A Chinese Perspective on Cyber War." *International Review of the Red Cross* 94 (886): 801–7. https://doi.org/10.1017/S1816383112000823.

Triwahyuni, Dewi. 2020. "American Foreign Policy in Cyberspace" 391: 48–51. https://doi.org/10.2991/assehr.k.200108.010.

Lai, Robert. 2012. "Analytic of China Cyberattack." *The International Journal of Multimedia & Its Applications* 4 (3): 37–56. https://doi.org/10.5121/ijma.2012.4304.

Yayat Rahmat Hidayat. 1967. "済無No Title No Title No Title." *Angewandte Chemie International Edition, 6(11), 951–952.* 4: 763–73.

Spade, Jayson M. 2011. "China's Cyber Power and America's National Security." *Information as Power*, no.

October: 3. http://www.carlisle.army.mil/featured_articles/teaser1_8Jul12-SRP.htm.

Domingo, Francis C. 2016. "China's Engagement in Cyberspace." *Journal of Asian Security and International Affairs* 3 (2): 245–59. https://doi.org/10.1177/2347797016645456.

Demchak, Chris, Jason Kerben, Jennifer Mcardle, and Francesca Spidalieri. 2015. "Principal Investigator: Melissa Hathaway CYBER READINESS INDEX 2.0 CYBER READINESS INDEX 2.0," no. November.

Janczewski, Lech J., and William Caelli. 2020. "National Cyber Security Organisation." *Cyber Conflicts and Small States*, 87–196. https://doi.org/10.4324/9781315575650-14.

Cai, Cuihong. 2015. "Cybersecurity in the Chinese Context: Changing Concepts, Vital Interests, and Prospects for Cooperation." *China Quarterly of International Strategic Studies* 1 (3): 471–96. https://doi.org/10.1142/S2377740015500189.

"Data and Cybersecurity Compliance in China 1421 Consulting Group." 2020, no. February: 1–21.

Isaacs, Julien, and Jake Cohen. 2019. "Digital Expansionism: Exploring the U.S.-China Technology Dynamic Through Cybersecurity Policy and International Marketing Strategies in the Cloud Computing Sector Signature Redacted Digital Expansionism: Exploring the U.S.-China Technology Dynamic Throug," 94.www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-.