Strategi Keamanan Siber Amerika Serikat di Masa Pemerintahan Joe Biden Terkait Isu *State-Sponsored Cyber Espionage*

Rangga Dheo Chandra[1]
Andrea Abdul Rahman Azzqy[2]
Syahrul Awal[3]

Abstract

This paper aims to analyze the U.S. Cybersecurity strategy adopted by the President Biden after a series of state-sponsored cyber espionage incidents against the United States by its adversary (mainly by the Russian Federation). The series of state-sponsored cyber espionage starting from the interference of the 2016 and the 2020 US Presidential Election and the SolarWinds' Orion incident that leads to massive federal data breach in the U.S. and its allies throughout 2019-2020. Such incidents are becoming the main national security concern of the U.S. under Biden administrations. President Biden have to rethink and redesign the U.S. Cybersecurity strategy that aims to respond and preparing the nation's cyber defense systems against a various cyber threats that facing the U.S. This research is a qualitative-descriptive research that aims to describe the steps, efforts and policies made by Biden Administrations using the neoclassical realism perspective, the foreign policy theory, and the cyber security concepts as a framework of analysis. The results of this study indicate that the U.S. Cybersecurity Strategy is a form of a foreign policy taken by President Biden in response to Russian aggressiveness in cyberspace. Mr. Biden and his administrations took several steps and policies as follows: imposing economic and diplomatic sanctions on Russian Federation through Executive Order (EO) 14024; reforming the nation's cybersecurity strategies through EO 14028 which stressing the importance of public-private partnership for strengthening Federal cybersecurity; and also a Presidential Memorandum (Memo) for furthering President Biden's efforts for advancing and strengthening the U.S. National Cybersecurity in critical infrastructure, defense and intelligence agencies of the United States.

Keywords: *Cybersecurity, cybersecurity strategy, Joe Biden, state-sponsored cyber espionage, the U.S. foreign policy.*

[1] Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Budi Luhur. Email: ranggadheo@gmail.com.
[2] Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Budi Luhur.
[3] Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Budi Luhur.

Pendahuluan

Cyber espionage atau spionase siber merupakan sebuah bentuk serangan siber *(cyberattack)* yang tujuannya adalah untuk mendapatkan *unauthorized access* ke data dan informasi sensitif yang dimiliki oleh aktor negara maupun swasta (Baker, 2022). Spionase siber sendiri merupakan bentuk operasi intelijen modern yang dilakukan melalui domain siber dengan tujuan untuk mendapatkan keunggulan kompetitif, keuntungan ekonomi hingga mendukung tercapainya tujuan-tujuan politik – militer pihak agresor. Hal ini tentu memungkinkan dengan tingkat dependensi manusia terhadap Teknologi Informasi dan Komunikasi (TIK) yang semakin tinggi (Ghernaouti, 2013: 14). Dependensi manusia terhadap teknologi di satu sisi memberikan banyak sekali kemudahan serta manfaat, seperti efisiensi waktu dan tenaga melalui serangkaian bentuk konektivitas dan digitalisasi (Williams, 2018). Tetapi di sisi lain, dependensi terhadap teknologi membuat manusia semakin rentan terhadap bentuk-bentuk ancaman yang semakin berkembang mengikuti perkembangan teknologi.

Amerika Serikat merupakan sebuah negara yang digdaya dalam domain siber (IISS, 2022: 510). Kedigdayaan Amerika dalam domain siber tidak terlepas dari sejarah perkembangan teknologi internet dan komputer itu sendiri yang mana merupakan hasil dari investasi besar-besaran AS dalam sektor pengembangan teknologi untuk keperluan militer di masa lalu (MacKenzie, 1998: 161). Selain itu, teknologi juga merupakan salah satu sumber kekuatan ekonomi, politik hingga militer yang dimiliki AS (Trehan, 2020; Ryan, 2021). Sehingga, tidak dapat dinafikan jika dependensi Amerika terhadap teknologi digital dan domain siber sangat tinggi. Tetapi, dependensi ini dilihat sebagai sebuah pedang bermata dua sebagaimana pendapat ahli keamanan siber yang dikutip oleh Marks. Para ahli keamanan siber menilai bahwa dependensi Amerika terhadap teknologi membuat AS menjadi negara yang maju sekaligus negara yang paling rentan menjadi target serangan siber (Marks dan Schaffer, 2022).

Tingkat dependensi yang tinggi serta teknologi yang maju membuat Amerika menjadi salah satu target favorit serangan siber, khususnya spionase siber. Jika ditelusuri kembali, AS telah menjadi target operasi spionase siber sejak 1996 yang dikenal sebagai insiden *Moonlight Maze.* Insiden ini merupakan sebuah operasi siber pertama yang disponsori oleh negara, yang hingga kini diyakini bahwa Rusia merupakan dalang dibalik serangan tersebut. Pihak aggressor berhasil melakukan pencurian informasi rahasia dari berbagai agensi pemerintahan AS, termasuk NASA, Departemen Pertahanan serta Departemen Energi (Westby, 2020). Dalam periode 2014 – 2022, kelompok peretas yang "diduga" merupakan kelompok yang disponsori oleh pemerintah Rusia telah berulang kali menjalankan operasi siber yang ditujukan ke AS dan sekutunya.

Insiden spionase siber dengan metode serangan *supply-chain* terhadap Solarwinds dalam rentang 2019-2020 dinilai sebagai sebuah insiden spionase siber terbesar dalam sejarah berdirinya Amerika. Alex Stamos sebagaimana dikutip oleh Temple-Raston berpendapat bahwa serangan *supply-chain* ini merupakan operasi spionase siber paling efektif sepanjang masa (Tempel-Raston, 2021). *Joint Cybersecurity Advisory* (CSA) yang terdiri atas *the National Security Agency* (NSA), *the Cybersecurity and Infrastructure Security Agency* (CISA) serta *the Federal Bureau of Investigation* (FBI) sebagai investigator dalam insiden ini menyimpulkan bahwa operasi spionase siber tersebut dilakukan oleh kelompok Cozy Bear yang berasal dari Rusia (CISA, 2021).

Cozy Bear (APT-29) sendiri merupakan kelompok peretas Rusia yang sangat dipercaya sebagai unit siber dalam Foreign Intelligence Service (SVR) atau juga dipercaya merupakan bagian dari Federal Security Service (FSB). Hal ini merujuk pada pemilihan target yang merefleksikan kepentingan politik-militer Rusia. Metode operasi yang

digunakan oleh Cozy Bear cenderung mengadopsi operasi *clandestine* (Smith, 2021). Selain Cozy Bear, Fancy Bear (APT-28) juga merupakan kelompok peretas yang berfokus pada operasi spionase siber. Namun metode yang digunakan sangat berbeda dengan Cozy Bear. Fancy Bear memiliki kecenderungan untuk membocorkan serta mempublikasikan dokumen, data maupun informasi yang berhasil mereka curi dari target operasinya. Hal ini tergambar dari keterlibatan Fancy Bear dalam interferensi asing terhadap Pemilu Presiden AS pada 2016 dan 2020. Pada 2016, Fancy Bear dipercaya berhasil meretas Democratic National Committee (DNC) yang bertanggung jawab dalam kampanye Calon Presiden Hillary Clinton pada 2016 (Rid, 2016). Selain itu, Fancy Bear juga merupakan kelompok yang secara terang-terangan mengakui bahwa mereka adalah aktor yang meretas World Anti-Doping Agency (WADA) dan Komite Olimpiade Internasional (IOC) sebagai respon atas pelarangan atlet Rusia untuk bertanding dalam olimpiade akibat tudingan penggunaan doping (Duchon, 2016).

Rusia menjadi salah satu *key adversary* yang cukup mendapat sorotan dari komunitas intelijen Amerika karena agresitivitasnya dalam operasi siber. Selain itu, Tiongkok, Iran dan Korea Utara juga merupakan negara yang dipersepsikan sebagai ancaman bagi kepentingan nasional Amerika dalam domain siber (the U.S. Director of National Intelligence, 2022: 4). Keempat *major adversary* tersebut dinilai terus berusaha untuk meningkatkan kapabilitas siber dan militernya, hal ini tentu meningkatkan risiko bagi Amerika Serikat dan sekutunya untuk menjadi target dari serangan siber ofensif yang dilakukan negara-negara tersebut.

Meski begitu, bukan berarti posisi Amerika dalam konteks ini sebagai korban. Sebaliknya, Amerika Serikat juga merupakan negara yang bisa dikatakan sangat aktif dalam menjalankan operasi siber baik untuk tujuan ofensif seperti operasi Stuxnet maupun untuk tujuan defensif seperti spionase dan *surveillance* (Kolbe, 2020). Amerika Serikat sendiri memiliki kelompok peretas APT bernama The Equation Group yang diklaim oleh Kaspersky sebagai *"god of cyberespionage"* karena merupakan kelompok yang disinyalir menjadi *pioneer* dalam operasi spionase siber (Kaspersky, 2015). Banyak spekulasi yang beredar bahwa Equation Group merupakan Tailored Access Operation (TAO) atau sebuah unit peretas ofensif rahasia milik NSA yang berhasil diidentifikasi saat kelompok peretas Shadow Brokers berhasil membobol jaringan milik NSA untuk mencuri peralatan siber dari kelompok peretas tersebut yang kemudian dibocorkan kepada publik (Burgess, 2017). Ini mengindikasikan bahwa baik AS maupun pihak musuhnya sama-sama menjalankan operasi siber khususnya spionase siber untuk mencapai tujuan-tujuan strategis masing-masing negara. Jika dielaborasi lebih lanjut, spionase siber merupakan sebuah praktik umum yang dilakukan oleh seluruh aktor dalam HI.

Meskipun spionase siber merupakan aktivitas umum yang dilakukan tiap aktor. Tidak dapat dipungkiri bahwa ancaman keamanan siber semakin meningkat seiring berkembangnya waktu. Ini dibuktikan dengan meningkatnya agresi musuh terhadap AS dalam domain siber yang tercermin dari rangkaian insiden serangan siber skala besar yang menimpa AS seperti interferensi Pemilu, serangan *supply-chain* yang mengarah pada operasi spionase siber terbesar serta paling efektif dalam sejarah berdirinya Amerika, hingga serangan ransomware terhadap Colonial Pipeline yaitu sistem pipa penyalur produk minyak sulingan terbesar di Amerika. Serangan ransomware ini menyebabkan terputusnya suplai bahan bakar ke bagian pantai timur AS. Meningkatnya agresivitas ini juga berkaitan dengan *uncertainty* dan *instability* dalam domain siber sehingga memaksa seluruh negara untuk selalu skeptis dan bertindak sedemikian rupa untuk mengamankan kepentingannya dari ancaman yang berasal dari domain siber. Untuk itu dibutuhkan sebuah strategi keamanan siber yang mampu secara efektif mempersiapkan sistem keamanan siber dari potensi terburuk yang suatu waktu dapat terjadi. Hal ini yang kemudian mendorong penulis

untuk merumuskan pertanyaan penelitian "bagaimana strategi keamanan siber Amerika Serikat di masa Pemerintahan Joe Biden terkait isu *state-sponsored cyber espionage*?"

Pembahasan

Amerika Serikat sejatinya sudah memiliki strategi keamanan siber yang cukup mumpuni. Pada masa pemerintahan Barack Obama misalnya, Obama memisahkan komando siber dari NSA menjadi sebuah unit militer independen dan penuh bernama US Cyber Command (US Cybercom). Meski begitu, komando siber masih belum memiliki keleluasaan untuk menjalankan operasi siber karena Obama memerintahkan segala bentuk operasi siber harus melalui persetujuannya (Lilli, 2020: 14-15). Langkah berbeda diambil oleh Presiden Trump yang memberikan kebebasan dan keleluasaan bagi US Cyber Command untuk mengambil langkah-langkah yang diperlukan untuk mempertahankan sekaligus mencapai kepentingan nasional AS dalam domain siber. Presiden Donald Trump juga mengadopsi doktrin *"Persistent engagement"* dan strategi *defend-forward* yang bertujuan untuk mencegah dan meminimalisir intensitas dan kecepatan dari para agresor (Devanny, 2021: 12).

Amerika Serikat juga memiliki sistem pertahanan siber bernama EINSTEIN 3 yang bertindak sebagai sistem pendeteksi aktivitas mencurigakan dalam sebuah sistem jaringan (Miller, 2021). Namun, insiden serangan *supply-chain* terhadap SolarWinds yang menjadi awal mula operasi spionase siber masif terhadap Pemerintah Federal AS menjadi sebuah alarm bagi administrasi Joe Biden untuk mulai merevisi strategi keamanan siber nasionalnya (Boyd, 2021). Langkah ini diperlukan, mengingat serangan *supply-chain* ini adalah sebuah kerentanan yang sangat memungkinkan dieksploitasi untuk tujuan-tujuan yang lebih destruktif seperti sabotase sistem keamanan di infrastruktur kritikal seperti sistem jaringan listrik hingga energi nuklir.

Keamanan siber Dalam Hubungan Internasional

Domain siber telah membawa perubahan signifikan dalam paradigma HI. Mattioli (2014: 24) berpendapat setidaknya ada tiga perubahan paradigma yang terjadi. Pertama, domain siber meningkatkan peran aktor non-negara dalam HI, termasuk individual. Kedua, domain siber merupakan sebuah "teritori" yang dapat memengaruhi apa yang terjadi dalam realitas utama (domain fisik). Ketiga, karena tidak ada aktor dominan dalam domain siber, sehingga tidak adanya kesepakatan bersama terkait definisi keamanan dalam domain siber. Karena setiap aktor memanfaatkan domain siber sesuai dengan kepentingan strategisnya, maka dari itu terdapat perbedaan mendasar bagaimana para aktor menafsirkan konsep keamanan siber itu sendiri.

Perubahan paradigma HI sebagaimana pendapat Mattioli tersebut juga didukung oleh pendapat Radu yang melihat bahwa domain siber telah memicu rangkaian perubahan dalam ekonomi, sosial dan politik serta keamanan dari level lokal hingga internasional (Radu, 2014: 1). Perubahan ekonomi ditandai dengan berkembangnya ekonomi digital dan menjamurnya e-commerce. Perubahan sosial-politik dengan berkembangnya diplomasi dan pemerintahan digital, serta perubahan serta gerakan sosial yang diamplifikasi melalui media sosial. Serta perubahan militer keamanan dengan memanfaatkan domain siber untuk mencapai tujuan strategis suatu negara.

Keamanan siber sendiri menurut penulis adalah sebuah tindakan, aksi maupun upaya untuk menciptakan rasa aman dari berbagai sumber dan bentuk ancaman siber yang dapat mengganggu fungsi-fungsi operasional negara, perusahaan serta individual dalam domain siber. Deskripsi keamanan siber lainnya berasal dari Bayuk, dkk. dan International Telecommunication Union (ITU). Bayuk, dkk. berpendapat bahwa keamanan siber

mengacu pada seperangkat kemampuan untuk mengontrol akses ke sistem jaringan serta informasi yang berada dalam jaringan tersebut (Bayuk, dkk., 2012: 1). Sedangkan ITU mendeskripsikan keamanan siber sebagai sebuah kumpulan alat, kebijakan, dan tindakan yang ditujukan untuk melindungi dimensi virtual *(digital realms)* dan dimensi non-virtual dalam domain siber (ITU, 2009).

Spionase Siber Sebagai Ancaman Terhadap Keamanan dan Kepentingan Nasional Amerika Serikat

Presiden Joe Biden menjelaskan bahwa terdapat tiga kepentingan nasional utama Amerika Serikat di masa kepemimpinannya (White House, 2021). Adapun ketiganya adalah sebagai berikut:

a. Melindungi keamanan rakyat Amerika;
b. Memperluas kemakmuran dan peluang ekonomi; dan
c. Mewujudkan nilai-nilai demokrasi sebagai *American way of life.*

Dari ketiga kepentingan tersebut, keseluruhannya merupakan manifestasi dari idealisme liberal sebagai sebuah budaya strategis Amerika Serikat. Budaya strategis sendiri merupakan salah satu faktor penting bagi suatu pemimpin untuk mempersepsikan suatu fenomena sebagai sebuah ancaman terhadap keamanan nasionalnya (Ripsman dkk., 2016).

Spionase siber sebagaimana sifat alaminya adalah sebuah bentuk aktivitas intelijen yang umum dilakukan oleh tiap aktor dalam hubungan internasional. Tetapi, Spionase siber dapat menjadi masalah ketika informasi intelijen tersebut digunakan sebagai bahan untuk propaganda. Berkaca pada interferensi asing dalam pemilu Amerika Serikat, aktivitas spionase merupakan hal yang wajar dilakukan suatu negara dan merupakan tindakan rasional bagi suatu negara untuk mengumpulkan informasi terkait siapa yang akan menjadi pemimpin selanjutnya dari negara tersebut. Hal ini cukup penting mengingat pemimpin negara memiliki kapabilitas untuk menentukan arah kebijakan luar negeri negaranya. Dalam kasus ini, spionase siber yang dilakukan Fancy Bear dipersepsikan sebagai ancaman terhadap kepentingan nasional Amerika Serikat karena mencederai nilai-nilai demokrasi. Selain itu, propaganda dan peperangan informasi yang dilakukan oleh Rusia juga menyebabkan ketidakstabilan di masyarakat Amerika karena meningkatnya angka ketidakpercayaan terhadap pemerintah serta sistem pemilu demokratis (Jensen, 2019).

Amerika Serikat mempersepsikan empat negara sebagai musuh utama dalam domain siber. Rusia, Tiongkok, Korea Utara dan Iran dianggap sebagai negara yang mensponsori kelompok peretas untuk menjalankan berbagai operasi siber untuk mendukung tujuan atau kepentingan nasional masing-masing negaranya. Rusia sendiri melalui kelompok APT 28 atau Fancy Bear yang terafiliasi dengan GRU military unit 26165 yang juga dikenal sebagai unit 85th Main Special Service Center menjalankan berbagai operasi spionase siber yang targetnya berfokus pada sektor politik, pengembangan teknologi dan militer di negara asing (Strokan & Taylor, 2018: 158). Pemilihan target ini merefleksikan fokus operasional GRU sehingga industri pertahanan, tokoh atau elit politik, badan pemerintahan, institusi penelitian hingga universitas menjadi target "favorit" dari operasi spionase siber yang dilakukan oleh Fancy Bear. Meski begitu, Fancy Bear juga kerap menjalankan operasi siber ofensif dengan objektif tindakan pembalasan atau *retaliatory* terhadap pihak yang dianggap mengganggu atau mengusik kepentingan Rusia dan tidak jarang melakukannya dengan terang-terangan *(covert action)*.

Kelompok APT lainnya yang berasal dari Rusia adalah APT 29 atau Cozy Bear yang memiliki afiliasi antara SVR ataupun FSB. Berbeda dengan Fancy Bear, Cozy Bear berfokus

pada operasi spionase siber dengan tujuan untuk *intelligence gathering* (F-Secure, 2015: 6). Meskipun tidak se-agresif Fancy Bear, Cozy Bear juga menjadi salah satu kelompok APT yang cukup disegani dan mendapat sorotan dari pihak intelijen maupun pengamat keamanan siber. Cozy Bear sangat terkenal dengan kehandalannya untuk menghindari sistem deteksi keamanan jaringan. Cozy Bear dipersepsikan sebagai kelompok peretas yang sangat "percaya diri" dengan kemampuannya, sehingga meskipun mereka sudah terdeteksi, mereka tidak mundur melainkan mencari cara agar tetap berada dalam sistem jaringan tersebut dalam waktu yang lama *(persistent)* (Mandiant, 2022). Kepercayaan diri kelompok Cozy Bear bukan tanpa alasan. Mereka merupakan kelompok APT yang memiliki kemampuan adaptasi dan improvisasi yang sangat baik. Bahkan, mereka tidak ragu untuk mengubah metode sekalipun saat misi atau operasi siber sedang berlangsung.

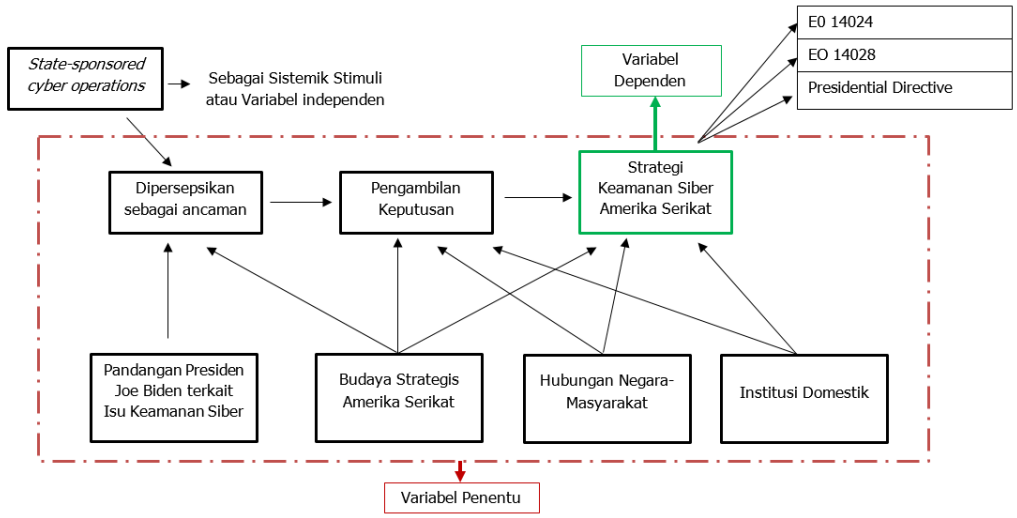
Kedua kelompok tersebut merupakan ujung tombak Rusia untuk operasi pengumpulan intelijen (Intelligence gathering) untuk mendukung tujuan-tujuan strategis Rusia. Aktor lainnya yang mensponsori spionase siber adalam Tiongkok. Berbeda dengan Rusia yang fokusnya pada kekuasaan dan pengaruh politik-militer. Tiongkok berfokus pada pengembangan teknologi dan ekonomi. Sehingga, operasi spionase siber yang dilakukan kebanyakan berfokus pada pencurian informasi intelektual dari target. Ada dua kelompok yang diduga disponsori oleh Beijing. Keduanya adalah APT 1 dan APT 41 (juga dikenal sebagai Wicked Panda atau Double Dragon. Fokus operasi kedua kelompok ini menargetkan industri atau sektor-sektor esensial bagi pengembangan teknologi Tiongkok. Adapun sektor-sektornya seperti IT, Aerospace, satelit dan telekomunikasi, energi hingga industri elektronik tingkat tinggi *(hi-tech).* Kedua kelompok ini merefleksikan kepentingan ekonomi Tiongkok yaitu rencana *"made in China 2025"* dan operasi spionase siber yang dilakukan nantinya akan menjadi bahan untuk *reverse-engineering* (Gilli & Gilli, 2019).

Iran dan Korea Utara juga dinilai sebagai aktor yang mensponsori spionase siber terhadap Amerika Serikat. Meskipun begitu, keduanya tidak se-*high profile* Rusia dan Tiongkok. Korea Utara sendiri menggunakan kapabilitas sibernya untuk mendukung tujuan-tujuan strategis Pyongyang, salah satunya melakukan pencurian mata uang Crypto untuk mendanai modernisasi dan pengembangan teknologi militer konvensional khususnya persenjataan nuklir yang mana perekonomian Korea Utara tidak mungkin melanjutkan modernisasi di tengah terpaan beragam sanksi internasional yang dijatuhkan terhadap Pyongyang (Lee, 2020). Di sisi lain, Iran merupakan negara yang cukup aktif menjalankan beragam misi operasi siber di Timur Tengah. Iran juga menunjukan kapabilitas yang sangat mumpuni untuk melakukan operasi siber ofensif sehingga Amerika Serikat melihat Iran sebagai aktor ancaman potensial bagi kepentingan nasional Amerika khususnya keamanan infrastruktur kritis (Director of National Intelligence, 2022: 15).

Masing-masing aktor ancaman siber diatas terus melakukan pengembangan kapabilitas sibernya. Peningkatan intensitas serta semakin seringnya insiden keamanan siber semakin menunjukan instabilitas dalam domain siber. Rangkaian beragam bentuk serangan siber yang melanda Amerika Serikat dalam rentang waktu 2020 – awal 2022 menunjukan bahwa Amerika Serikat semakin rentan terkena serangan siber, dan hanya menunggu waktu untuk terjadinya sebuah insiden keamanan siber yang destruktif seperti stuxnet, malware NotPetya, malware Industroyer, hingga malware Triton yang dapat menyabotase sistem keamanan operasional dari infrastruktur kritikal seperti listrik dan energi dan berpotensi menyebabkan *reactor meltdown* dapat terjadi di masa depan. Untuk itu, Amerika Serikat perlu sebuah strategi keamanan siber terbaru yang diharapkan dapat menjadi jawaban atas beragam potensi ancaman keamanan siber di masa depan.

Strategi Keamanan Siber Amerika Serikat Di Masa Pemerintahan Joe Biden Terkait Isu State-Sposored Cyber Espionage

Semakin meningkatnya intensitas dan insiden keamanan siber yang mengancam kepentingan nasional AS seperti upaya interferensi Pemilu Presiden Amerika, pembobolan dan pencurian data atau informasi dari pemerintah federal melalui insiden SolarWinds, hingga insiden serangan ransomware terhadap Colonial Pipeline menjadi sebuah faktor pemicu Presiden Joe Biden untuk memformulasikan sebuah strategi keamanan siber baru (Geller, 2020). Presiden Joe Biden menilai bahwa insiden keamanan siber ini mengganggu kepentingan nasional Amerika Serikat, dan mempersepsikan bahwa para aktor akan terus menjalankan aksinya sehingga Amerika perlu memberikan respon atas krisis dalam domain siber. Hal ini menunjukan bahwa terdapat sebuah proses yang dilakukan Presiden Joe Biden untuk mempersepsikan operasi spionase siber sebagai sebuah ancaman terhadap keamanan nasional Amerika. Setelah melalui proses persepsi ancaman, langkah lanjutannya adalah proses perumusan atau pengambilan keputusan yang melibatkan berbagai pemangku kepentingan untuk merumuskan strategi keamanan siber yang dapat bermanfaat bagi semua stakeholder, dan objektif utamanya adalah mengamankan kepentingan nasional Amerika Serikat. Proses tersebut kemudian menghasilkan kebijakan atau strategi keamanan siber baru. Proses tersebut merupakan manifestasi dari kerangka pemikiran yang penulis gunakan yaitu teori kebijakan luar negeri dengan pendekatan realisme neoklasik yang dikemukakan oleh Gidion Rose dan dielaborasi lebih lanjut oleh Ripsman dkk. Adapun hasil analisis penulis terkait strategi keamanan siber Amerika dapat dilihat pada gambar di bawah.



Gambar 1. Analisis Strategi Keamanan Siber Amerika Serikat Menggunakan Kerangka Pemikiran Teori Kebijakan Luar Negeri Realisme Neoklasik
Sumber: Hasil analisis yang diolah oleh tim penulis, (2022).

Secara garis besar, Presiden Joe Biden merumuskan dan mengeluarkan tiga kebijakan untuk meningkatkan keamanan siber Amerika Serikat. Adapun ketiga kebijakan tersebut dapat dilihat pada tabel di bawah:

Tabel 1. Kebijakan Keamanan Siber Presiden Joe Biden

Kebijakan	Isi	Keterangan
Perintah Eksekutif (EO) 14024	• Penjatuhan sanksi ekonomi dan pengambilan langkah-langkah diplomatik kepada pemerintah Rusia dan pihak-pihak yang terlibat sebagai respon atas aktivitas siber yang mengganggu dan mengancam kepentingan nasional Amerika Serikat. • Mendukung upaya pendekatan keamanan siber global (Global cybersecurity approach) dengan memperkuat upaya AS untuk mempromosikan kerangka *responsible state behavior* dalam domain siber. • Memperkuat komitmen keamanan domain siber kolektif AS dengan melakukan latihan pertahanan siber gabungan dengan negara-negara sekutunya.	Alasan penjatuhan sanksi ini karena Presiden Joe Biden menilai bahwa: • Rusia telah berupaya melemahkan pelaksanaan pemilu demokratis yang bebas dan adil. • Pihak-pihak yang terlibat secara langsung maupun tidak dalam upaya tersebut. • Pelanggaran terhadap prinsip-prinsip hukum internasional khususnya penghormatan terhadap integritas teritori negara.
Perintah Eksekutif (EO) 14028	Beragam upaya untuk meningkatkan keamanan siber nasional, khususnya berfokus pada jaringan Pemerintah Federal. • Meningkatkan transparansi antara Pemerintah Federal dengan sektor swasta dengan menghilangkan *contractual barrier* yang membatasi pembagian informasi antara pemerintah dan swasta, serta memperkuat kerangka kerjasama antara pemerintah-swasta untuk investigasi insiden keamanan siber secara bersama-sama. • Modernisasi keamanan siber pemerintah federal dengan mendorong pengimplementasian arsitektur *zero-trust*, mendorong penggunaan enkripsi, serta monitoring jaringan secara ketat terkait aktivitas yang berkaitan	Perintah Eksekutif ini merupakan inisiatif awal dari Presiden Joe Biden untuk meningkatkan keamanan siber nasional. Presiden Joe Biden kemudian mengambil langkah lanjutan yang dituangkan dalam Presidential Memorandum dan arahan presiden untuk meningkatkan keamanan siber dalam sektor-sektor yang lebih spesifik.

	dengan data sensitif pemerintah federal, serta mendorong aparatur sipil untuk mengikuti dan memahami standar keamanan siber yang berlaku. • Meningkatkan keamanan dalam perangkat *supply-chain* dengan mendorong para pengembang perangkat lunak untuk lebih transparan, salah satunya mencantumkan Software Bill of Materials (SBOM) atau komposisi yang membentuk perangkat lunak tersebut, serta menginstruksikan CISA dan NIST untuk membentuk standar keamanan siber dasar seperti pengunaan enkripsi data, adopsi otentikasi multi-faktor serta monitoring aktivitas secara berkala. • Membentuk Cybersecurity Safety Board yang bertugas untuk meninjau, memberi rekomendasi serta mendorong perbaikan di sektor publik maupun swasta terkait insiden keamanan siber yang terjadi. • Membuat SOP tentang respon insiden yang harus diikuti oleh semua agensi eksekutif pemerintah federal. • Meningkatkan deteksi kerentanan dalam jaringan pemerintah federal dengan mewajibkan agensi sipil untuk mengadopsi Endpoint Threat Detection and Response (ETDR atau EDR) dan mendukung operasi *active cyber hunting* untuk mendeteksi insiden serta memberi respon atas insiden tersebut • Meningkatkan kemampuan investigasi dan remediasi pemerintah federal dengan tujuan untuk mendeteksi dan menetralisir ancaman siber sebelum memberi dampak yang jauh lebih besar.	

Arahan lanjutan Presiden Joe Biden untuk meningkatkan keamanan siber nasional.	1) *National Security Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.* • Memorandum tersebut berisikan pengimplementasian EO 14028 untuk National Security Systems (NSS) dan mendorong penggunaan solusi lintas domain dengan mendorong pertukaran informasi yang dikomandoi oleh NSA sebagai *National Manager*. 2) *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems.* • Memerintahkan CISA dan NIST membuat sasaran kinerja keamanan siber untuk sektor infrastruktur kritikal. • Secara formal membentuk *the President's Industrial Control System Cybersecurity* (ICS) *Initiative.* Sebuah inisiatif sukarela untuk memfasilitasi penyebaran teknologi dan sistem deteksi ancaman siber. • Menginstruksikan secara khusus bagi pemilik dan operatos sistem perpipaan minyak bumi atau cairan berbahaya untuk membuat langkah mitigasi khusus untuk melindungi dari serangan ransomware serta membuat rencana kontijensi pemulihan dari insiden keamanan siber khususnya insiden ransomware. 3) *Fact Sheet: Act Now to Protect Against Potential Cyber Attack.* • Memandatkan pengimplementasian otentikasi multifaktor. • Menerapkan alat keamanan siber modern untuk memitigasi ancaman siber.	Keempat kebijakan ini merupakan langkah lanjutan Presiden Joe Biden untuk meningkatkan sistem keamanan siber Amerika secara keseluruhan.

	• Memastikan sistem telah mendapat *patch* secara berkala berdasarkan katalog kerentanan yang dipublikasikan oleh CISA. • Membuat data cadangan yang disimpan secara luring. 4) *Protecting Against Malicious Cyber Activity before the Holidays.* • Menginstruksikan pengawasan logs, penggunaan otentikasi multifaktor, serta melakukan *update patch* secara berkala. • Memberikan edukasi kepada karyawan terkait menghindari kampanye *spear-phising*.	

Sumber: The White House (2021-2022), diolah oleh Tim Penulis.

Kesimpulan

Strategi Keamanan siber Amerika Serikat yang dibuat oleh Presiden Joe Biden sejatinya merupakan bentuk dari Kebijakan Luar Negeri sebagai bentuk respon atas stimuli sistemik yang mengganggu kepentingan nasional Amerika Serikat. Penulis menggunakan pendekatan realisme neoklasik yang mana merupakan pendekatan yang menggabungkan dua pendekatan realisme yaitu realisme tradisional (atau yang disebut innenpolitik) dan realisme struktural atau neorealisme. Neoklasik berperan sebagai jalan tengah dalam perdebatan tentang mengapa atau faktor apa yang membuat negara berperilaku sedemikian rupa. Neoklasik melihat bahwa baik faktor eksternal (sistemik stimuli) maupun faktor internal (domestik) memainkan peran yang sama besar dalam menjelaskan mengapa suatu negara mengambil kebijakan tertentu.

Presiden Joe Biden dihadapi oleh masalah yang datang dari eksternal, yaitu spionase siber yang disponsori negara. Operasi spionase merupakan praktik umum yang diterima (baik secara formal maupun informal) oleh seluruh negara. Namun, Presiden Joe Biden mempersepsikan insiden spionase siber yang menargetkan Amerika Serikat sebagai sebuah ancaman. Faktor yang mendorong Presiden Joe Biden untuk mempersepsikan spionase siber sebagai sebuah ancaman terhadap kepentingan dan keamanan nasional AS adalah mengacu pada budaya strategis Amerika Serikat yang bersandar pada idealisme liberal.

Nilai-nilai liberal juga tercermin dari kepentingan nasional Amerika Serikat yang mengedepankan perlindungan pada rakyat, ekonomi serta nilai-nilai demokrasi yang semuanya merupakan manifestasi dari idealisme liberal. Budaya Strategis yang tergambar dalam kepentingan nasional menjadi faktor pendorong bagi Presiden Joe Biden untuk mempersepsikan spionase siber sebagai ancaman terhadap keamanan dan kepentingan nasional.

Spionase siber sebagai sebuah ancaman, Presiden Joe Biden tentu mengambil langkah-langkah tegas untuk mempertahankan negara dan bangsanya. Melalui proses pengambilan keputusan yang melibatkan sektor swasta, Presiden Joe Biden mengeluarkan rangkaian kebijakan keamanan siber yang keseluruhannya bertujuan untuk melindungi Amerika Serikat dari ancaman siber. Proses yang dilalui mulai dari terjadinya insiden spionase siber sebagai variabel independen (sistemik stimuli), lalu dipersepsikan oleh

Presiden Joe Biden yang setelahnya memasuki proses pengambilan keputusan (variabel penentu) untuk membuat kebijakan keamanan siber nasional (variabel dependen) merupakan bentuk manifestasi dari teori kebijakan luar negeri realisme neoklasik.

Referensi

Baker, Kurt. (2022, 1 Juni). "What is cyber espionage." diakses melalui https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

Bayuk, J.L., dkk. (2012). "Cyber security policy guidebook." *WILEY.*

Biden Jr, Joseph R. (2021). "Interim National Strategic Guidance." *Executive Office of the President.* Washington DC. Diunduh melalui https://apps.dtic.mil/sti/citations/AD1124337

Boyd, Rylle. (2021, 16 Maret). "The SolarWinds hack highlights the need to revise U.S. Cyber Strategy." https://www.americansecurityproject.org/the-solarwinds-hack-highlights-the-need-to-revise-u-s-cyber-strategy/

Burgess, Matt. (2017, 18 April). "Hacking the hackers: everything you need to know about Shadow Brokers' attack on the NSA." Diakses melalui https://www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers

CISA. (2021, 15 April). "NSA-CISA-FBI Joint advisory on Russian SVR targeting U.S. and Allied networks." Diakses melalui https://www.cisa.gov/uscert/ncas/current-activity/2021/04/15/nsa-cisa-fbi-joint-advisory-russian-svr-targeting-us-and-allied

Devanny, Joe. (2021). "'Madman Theory' or 'persistent engagement'? The coherence og US Cyber Strategy under Trump." *Journal of Applied Security Research.* Doi: https://doi.org/10.1080/19361610.2021.1872359

Director of National Intelligence. (2022). "Annual Threat Assessment of the U.S. Intelligence Agency." Diunduh melalui https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

Duchon, Richie. (2016, 15 September). "Russian hackers publish more health data of Rio 2016 olympians. *NBC News.* Diakses melalui https://www.nbcnews.com/storyline/2016-rio-summer-olympics/russian-hackers-publish-more-health-data-rio-2016-olympians-n648656

Geller, Eric. (2020, 17 Desember), "Biden pledges robust response to cyber crisis 'from the moment we take office.' *Politico*. https://www.politico.com/news/2020/12/17/biden-cyber-crisis-response-447858

Ghernaouti, Solange. (2013), "Cyber Power: Crime, conflict and security in cyberspace," *Lausanne*: EPFL Press, hal. 14

IISS, (2022), "Military Cyber Capabilities." Dalam *the Military Balance 2022. London:* Routledge. ISBN: 9781003294566, hal. 510

International Telecommunication Union. (2009). "Overview of cybersecurity: recommendation ITU-T X.1205. diakses melalui https://www.itu.int/rec/T-REC-X.1205-200804-I/en

Jensen, Benjamin. Dkk. (2019). "Fancy Bears and digital trolls: cyber strategy with a Russian twist." *Journal of Strategic Studies.* Doi: https://doi.org/10.1080/01402390.2018.1559152

Kaspersky. (2015, 17 Februari). "Equation Group: The Crown Creator of Cyber-Espionage". *Kaspersky.* https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage

Kolbe, Paul R. (2020, 23 Desember). "With hacking, the United States needs to stop playing the victim." *The New York Times,* https://www.nytimes.com/2020/12/23/opinion/russia-united-states-hack.html

Lee, Christy. (2020, 21 Februari). "Cybertheft help North Korea offset revenue lost to sanctions." *VOA*. https://www.voanews.com/a/east-asia-pacific_cyberthefts-help-north-korea-offset-revenue-lost-sanctions/6184667.html

Lilli, Eugenio. (2020). "President Obama and US Cybersecurity Policy." *Journal of Cyber Policy.* Doi: https://doi.org/10.1080/23738871.2020.1778759

MacKenzie, Donald. (1998), "Technology and the Arms Race." *International security vol. 14(1),* DOI: http://www.jstor.org/stable/2538768, hal. 161

Mandiant. (2022, 27 April). "Assembling the Russian Nesting Doll: UNC2452 Merged into APT29." https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29

Marks, Joseph, dan Schaffer, Aaron. (2022, 6 Juni), The U.S. isn't getting ahead of the cyber threat, experts say, *The Washington Post*. https://www.washingtonpost.com/politics/2022/06/06/us-isnt-getting-ahead-cyber-threat-experts-say/

Mattioli, Rossella. (2014). "The 'state(s)' of Cybersecurity." Dalam G. Giacomello (ed.), *Security in Cyberspace: targeting nations, infrastructures, individuals. New York:* Bloomsbury.

Miller, Jason. (2021, 18 Mei). "CISA's EINSTEIN had a chance to be great, but it's more than good enough. https://federalnewsnetwork.com/reporters-notebook-jason-miller/2021/05/cisas-einstein-had-a-chance-to-be-great-but-its-more-than-good-enough/

Radu, Roxana. (2014). "Power Technology and Powerful Technologies: Global governmentality and security in the cyberspace." Dalam Jan-Frederik Kremer & Benedikt Muller (Ed.). *Cyberspace and international relations.* Springer.

Rid, Thomas. (2016, 20 Oktober). "How Russia pulled off the biggest election hack in U.S. history." Diakses melalui https://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/

Ripsman, Norrin M., dkk. (2016). "Neoclassical Realist Theory of International Politics." *Oxford.*

Ryan, Missy. (2021, 1 April). "The U.S. system created the world's most advanced military. Can it maintain an edge?" *The Washinton Post.* https://www.washingtonpost.com/national-security/china-us-military-technology/2021/03/31/acc2d9f4-866c-11eb-8a67-f314e5fcf88d_story.html

Smith, Jane. (2021), "Iron Rain: Understanding nation-state motives and APT Group." *VMWare Global Threat Report,* diunduh melalui https://www.vmware.com/learn/security/iron-rain-understanding-nation-state-motives-and-apt-groups.html

Strokan, Mikhail A., dan Taylor, Brian D. (2018). "Intelligence." Dalam Tsygankov (ed.) Routledge Handbook of Russian Foreign Policy.

Temple-Raston, Dina. (2021, 16 April), "A 'worst nightmare' cyberattack: the untold story of the solarwinds hack." *NPR*. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

The White House, (2021, 12 Mei), Executive Order on Improving the Nation's Cybersecurity, diakses melalui https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/?utm_source=lin

The White House, (2021, 28 Juli), National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, diakses melalui https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

The White House, (2022, 19 Januari), Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, diakses melalui https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

The White House, (2022, 21 Maret), FACT SHEET: Act Now to Protect Against Potential Cyberattack, diakses melalui https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/

The White House. (2021, 16 Desember). "Protecting Against Malicious Cyber Activity before the Holidays." diakses melalui https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/16/protecting-against-malicious-cyber-activity-before-the-holidays

Trehan, Robin. (2020, 9 Mei). "Technology sector's impact on USA Economy." *Deltec Bank,* https://www.deltecbank.com/2020/05/09/technology-sectors-impact-on-usa-economy/

Westby, Jody. (2020, 20 Desember). "Russia has carried out 20 years of cyberattack that call for international response." Forbes. Diakses melalui https://www.forbes.com/sites/jodywestby/2020/12/20/russia-has-carried-out-20-years-of-cyber-attacks-that-call-for-international-response/?sh=5b311d366605

Williams, Jane. (2018). "Cybercrime in the digital age." https://www.global-engage.com/life-science/cyber-crime-in-the-digital-age/