Paradigma
POLISTAAT
JURNAL ILMU SOSIAL DAN ILMU POLITIK
P-ISSN: 2579-3861 & E-ISSN: 2579-3888

Vol. 7. No. 1 (2024)

KEBIJAKAN AMERIKA SERIKAT PADA CYBERATTACK RUSIA PERIODE (2017-2020)

Deana Rahda Mahalsya
Universitas Katolik Parahyangan

Email: deanamahalsya00@gmail.com

Abstract

Cyberattacks are a sensitive issue, especially when it is related to the security of a country, this kind of thing becomes a threat to a big country like the United States whose daily life cannot be separated from the use of technology. Important information owned by the United States turned out to be the target of attacks by Russia through cyberattacks, this incident had a major impact on the condition of the United States' national security.The Cyberattack strategy carried out by Russia certainly received a swift response from the United States as the country that was the loser. Therefore, this research was conducted to review United States policies through cybersecurity against random cyberattacks carried out by Russia. This research will be carried out using the literature study research method and also a review of official state documents. As a country that has experienced cyberattacks, the United States has provided an illustration regarding the importance of a more modern national security focus, this has been realized by the United States government by issuing cybersecurity policies.

Keywords: cyberattack, cybersecurity, security, strategy

Abstrak

Cyberattack merupakan isu sensitif terutama jika dikaitkan dengan keamanan sebuah negara, hal semacam ini menjadi suatu ancaman bagi negara besar seperti Amerika Serikat yang kehidupan sehari-harinya tidak terlepas dari penggunaan teknologi. Informasi penting yang dimiliki oleh Amerika Serikat ternyata dijadikan target serangan oleh Rusia melalui *cyberattack*, kejadian ini berdampak besar pada kondisi keamanan nasional Amerika Serikat. Strategi *Cyberattack* yang di lakukan oleh Rusia ini tentu mendapat respons sigap dari Amerika Serikat sebagai negara yang di rugikan. Maka daripada itu penelitian ini dilakukan untuk meninjau kebijakan Amerika Serikat melalui *cybersecurity* terhadap *cyberattack* yang dilakukan oleh Rusia. Penelitian ini akan dilakukan menggunakan metode penelitian studi pustaka dan juga peninjauan terhadap dokumen resmi kenegaraan. Sebagai negara yang mengalami *cyberattack* Amerika Serikat telah memberikan gambaran terkait pentingnya fokus keamanan nasional yang lebih modern, hal ini diwujudkan oleh pemerintah Amerika Serikat dengan diterbitkannya kebijakan-kebijakan *cybersecurity.*

Kata kunci: cyberattack, cybersecurity, keamanan, strategi

1. Latar Belakang

Keberadaan *cyberattack* dalam era modern saat ini telah banyak memberikan pengaruh bagi kehidupan bernegara, banyak kegiatan kenegaraan yang dilakukan dengan menggunakan teknologi, tentunya hal ini memberikan dampak baru bagi kondisi negara dan keamanan nasional. Serangkaian *cyberattack* bahkan telah mempengaruhi kondisi negara maju seperti Amerika Serikat, hal ini dapat dilihat dari berbagai kejadian yang menimpa Amerika Serikat yang terindikasi dilakukan oleh Rusia. Aktor yang terlibat dalam permasalahan ini pun bukan hanya terbatas pada negara,

tapi berkembang pada kelompok masyarakat hingga individu, sehingga permasalahannya semakin kompleks (Nakashima & Timberg, 2020).

Contoh kasus serangan *cyberattack* yang merugikan Amerika Serikat dalam bidang keuangan adalah kasus Maksim Viktorovich, bahkan pencariannya langsung diumumkan oleh Pemerintahan Amerika Serikat melalui website FBI bahwasanya seorang warga kebangsaan Rusia terindikasi bekerja sama dengan pemerintah Rusia dalam *cyberattack* (Mallin, 2019). Maksim yang lebih jelas terindikasi dalam keterlibatannya bersama *Evil Corpi* yang berbasis di Moskow, selain itu Maksim juga bekerja bagi intelijen Rusia, sehingga sangat merugikan bagi Amerika Serikat. Asisten jaksa agung Brian Benczkowski juga memberikan komentar dari aksi kejahatan Maksim "*The worst computer hacking and bank fraud schemes of the past decade*" (BBC, 2019).

Selain serangan yang dilakukan oleh individu terhadap sistem keuangan, terdapat serangan lain yang menyerang Amerika Serikat, *cyberattack* yang paling menyita perhatian pemerintah Amerika Serikat adalah saat sistem keamanan Gedung putih yang berhasil diretas oleh hacker Rusia, bahkan hal ini dikonfirmasi langsung oleh pihak istana dengan pernyataan John Ulyot selaku juru bicara dewan keamanan nasional (Nakashima, 2020). Buruknya hubungan antara Amerika Serikat dengan Rusia juga semakin jelas dengan beberapa video pidato Donald Trump dihadapkan publik, yang memberikan komentar terkait hubungan buruk antara Amerika Serikat dengan Rusia. Bahkan dari halaman media MIR Tv Vladimir Putin juga sempat memberikan statement yang menggambarkan hubungan memburuk di antara keduanya "*they (our relations) are going downhill, thye are getting worse and worse*" (Osborn & Tsvetkova, 2019).

Bocornya data perusahaan Facebook dalam pilpres Amerika Serikat pada 2016 juga bukan sekedar lelucon belaka, terutama dengan ketegasan untuk membubarkan *Cambridge Analytic* sebagai Lembaga konsultan politik tentu memiliki dasar keputusan yang kuat, terutama jika berkaitan dengan pencurian data banyak orang. pencurian data Facebook yang dijadikan sebagai analisis kemenangan politik pemilihan presiden Amerika Serikat oleh *Cambridge Analytic*, merupakan pembuktian serius terkait kepentingan keamanan *cyber*. kasus lain yang menjadi acuan bagi Amerika Serikat dalam meningkatkan *cybersecurity* adalah serangan terhadap sistem keamanan komputer gedung putih yang terindikasi dilakukan oleh Rusia, kejadian ini dikonfirmasi langsung oleh Jhon Ulyot selaku juru bicara dewan keamanan Amerika Serikat (Sanger, 2020).

Dari berbagai permasalahan yang disebabkan oleh *cyberattack* yang telah banyak dialami oleh Amerika Serikat, maka kondisi ini dirasa menjadi suatu momentum penting untuk melihat bagaimana respons yang diberikan oleh Amerika Serikat melalui instrumen kebijakan nasionalnya. Kepentingan negara untuk menjaga keamanan dalam bidang *cyber* bukan tanpa alasan untuk dilakukan, tetapi ini juga merupakan ancaman bagi *human security* Amerika Serikat, dan sudah seharusnya mendapatkan penanganan serius. Kondisi ini menjadi mengkhawatirkan karena bagaimanapun telah mengancam keamanan nasional sebuah negara, bahkan lebih dari itu *cyberattack* juga mengancam keamanan masyarakat hingga individu. Selain itu aksi kejahatan *cyberattack* ini adalah bentuk serangan langsung terhadap sistem negara yang berdampak langsung pada berbagai aspek nasional seperti pada bisnis kecil masyarakat sehingga mempengaruhi kondisi ekonomi, kejadian ini tentu telah

memberikan efek kerugian yang besar dan dirasakan langsung oleh masyarakat (Jimenez, 2022).

Kondisi keamanan nasional yang dapat disusupi oleh aktor asing tentu akan mempengaruhi kedaulatan negara, permasalahan pilpres Amerika Serikat pada tahun 2016 bukan hanya merugikan negara tetapi juga masyarakat. Data pribadi yang dicuri telah membuat masyarakat kehilangan privasi, selain itu aksi *cyberattack* juga dapat merugikan masyarakat pada sektor ekonomi seperti yang dilakukan oleh Maksim Viktorovich. Aksi *cyberattack* juga memberikan pengaruh besar pada masyarakat, kerugian materiel dan imateriel juga harus menjadi pertimbangan pemerintah untuk lebih banyak mengkaji mengenai kebijakan *cybersecurity*. Kebutuhan akan kebijakan *cybersecurity* bukan hanya sebuah isu belaka, melainkan kebutuhan dasar bagi negara dan masyarakat pada era modern yang tidak bisa lepas dari penggunaan teknologi.

2. Kerangka Pemikiran

2.1 Keamanan

Keberadaan keamanan bagi negara adalah identitas, untuk menjamin kelangsungan hidup masyarakatnya melalui kemerdekaan. menurut Berkowitz keamanan didefinisikan sebagai kemampuan dari suatu bangsa dalam melindungi nilai-nilai internalnya dari berbagai ancaman yang dilakukan oleh pihak luar (Berkowitz, 1965). Pengertian lain dari keamanan juga dijelaskan sebagai kepentingan negara yang berkaitan dengan kekuatan retoris dan politik, lebih jauh daripada itu keamanan merupakan tindakan untuk memberikan rasa aman terhadap bangsa, negara, individu, kelompok, lingkungan, planet hingga individu. Bentuk dari keamanan itu sendiri bisa berbentuk keamanan nasional hingga keamanan internasional (Barry Buzan, Ole Waever, 1998).

keamanan adalah aspek inti bagi negara dalam upaya untuk terus menjaga kedaulatan nasionalnya, dalam perspektif keamanan tradisional keamanan akan sangat erat kaitannya dengan militer isasi dan negara sebagai aktor, sehingga ada suatu pandangan bahwa kondisi keamanan suatu negara adalah ketika negara memiliki kemampuan untuk mempertahankan kepentingan nasionalnya, ketika mampu menghindari peperangan dan jika terlibat perang adalah dalam kondisi terpaksa mampu memenangkan peperangan itu (Kusnanto, 2003). Cakupan dalam pandangan keamanan tradisional juga terpaku pada ancaman yang selalu dianggap berasal dari luar, sehingga konteks keamanan tradisional memang sangat terpaku pada negara dan kegiatan militer sebagai acuannya.

2.2 Keamanan Non-Tradisional

Perkembangan permasalahan keamanan terus berkembang, bukan hanya terbatas pada permasalahan negara, tetapi menyentuh pada kondisi masyarakat dan individu. Perkembangan ini merujuk pada pengertian sekuritisasi, di mana aspek pengamanan lebih berkembang dan menyentuh berbagai hal yang bersifat emansipatoris, perkembangan ini membuat jawaban yang lebih spesifik mengenai keberadaan keamanan yang ditujukan untuk siapa. Mely Caballero menjelaskan bahwa perkembangan teori mengenai keamanan pasca perang dingin mengalami perubahan yang membuat pengertian dari keamanan tersebut lebih meluas (Caballero-Anthony, 2016), keamanan bukan lagi topik mengenai gerakan militer isasi dalam pengamanan negara, tetapi menjadi meluas dalam fokus keamanan masyarakat di mana akhirnya terdapat gagasan baru yaitu mengenai sekuritisasi yang mengartikan bahwa ancaman adalah segala sesuatu yang mengancam bagi

kehidupan masyarakat, yang tadinya tidak disadari namun setelah disadari menjadi suatu hal yang meluas. Konsep non-tradisional secara singkat (Caballero-Anthony, 2016):

- Meskipun tidak menolak negara sebagai rujukan keamanan, ia berpendapat untuk dimasukkannya rujukan lain, terutama individu dan komunitas.
- Diakui bahwa ancaman seperti perubahan iklim, pandemi dan krisis keuangan bersifat transnasional dan memerlukan tanggapan non-militer.
- Mengingat bahwa ancaman memiliki implikasi lintas batas, kerja sama multilateral internasional sangat penting.
- Aktor non-negara dan lembaga internasional dipandang memiliki peran penting dalam tata kelola global dari ancaman yang muncul.

Cakupan keamanan tradisional yang berpusat hanya pada negara tidak cukup memadai untuk bisa mencakup keselamatan dan kesejahteraan masyarakat, sehingga jika keselamatan masyarakat dan kelompok masih rapuh tentu hal tersebut juga akan mempengaruhi keamanan negara itu sendiri. Perkembangan mengenai ancaman dalam masalah keamanan juga tidak bisa di atasi dengan solusi militer seperti penutupan perbatasan atau dengan meningkatkan penjagaan militer saja (Michael Renner, Hilary French, 2005). Sehingga teori keamanan non-tradisional adalah rujukan dengan konsep lebih baik bagi negara dalam mengahadapi perkembangan ancaman yang mulai mengusik kedaulatan nasional.

2.3 Human security

Dalam pembahasan human security negara bukan merupakan pusat kajian melainkan berpusat pada individu, Pengertian human security secara sederhana merupakan instrumen untuk melindungi setiap individu (Caballero-Anthony, 2018). Pada teori ini fokus security berada pada individu, karena adanya Perubahan dalam cara pandang mengenai ancaman adalah inti utama pembahasan ini, karena dalam security inti dari permasalahan adalah pada sektor ancaman. Perkembangan ancaman yang menjadi lebih multi dimensi adalah pendorong bagi redefining security karena perkembangan ancaman, sehingga keamanan dapat di artikan melalui ancaman yang berada di sekitarnya (Richard H Ullman, 1983).

Dalam pembahasan mengenai human security terdapat banyak hal yang menjadi bagian di dalamnya, yang di jelaskan juga oleh UNDP yaitu (Acharya, 2001):

- Economic Security
- Food Security
- Health Security
- Environmental Security
- Personal Security
- Community Security
- Political Security

2.4 Cybersecurity

Teori mengenai *cybersecurity* ini juga akhirnya menjadi hal yang penting bagi Amerika Serikat sebagai negara adidaya (Wang, 2009), dari setiap periode kepemimpinan presiden dan dari tahun ke tahun Amerika Serikat selalu melakukan riset aktif terkait ancaman dalam bidang *cyberspace*, hal ini disadari karena kebutuhan masyarakat Amerika Serikat yang banyak melakukan kegiatan di dalam *cyber space* seperti kegiatan jual beli saham online, perdagangan

internasional seperti amazon dan banyak lagi kegiatan ekonomi besar yang dilakukan masyarakat Amerika Serikat yang melibatkan penggunaan teknologi di dalam *cyber space.*

Penggunaan teknologi dalam kegiatan *cyber space* juga menjadi keuntungan bagi negara dalam melakukan baik kegiatan positif maupun negatif seperti contohnya melakukan serangan *cyber warfare* menjadi lebih mudah dan menguntungkan untuk dilakukan, karena tidak perlu mengorbankan banyak nyawa dan mengeluarkan banyak dana untuk melakukan peperangan tetapi efek dari serangannya akan jauh lebih terasa bagi kehidupan negara yang menjadi sasaran serangan *cyber warfare*. Maka penggunaan teori *cybersecurity* saat ini menjadi sangat penting karena bagaimanapun kehidupan masyarakat dan kenegaraan tidak bisa lagi terlepas dari penggunaan teknologi di dalam *cyber space* sehingga demi mengamankan kepentingan nasional dan masyarakat maka penerapan teori *cybersecurity* sangat penting untuk diterapkan.

Pilar penting dalam pembahasan mengenai teori *cybersecurity* dijelaskan oleh lembaga kenegaraan Amerika Serikat, yaitu DHS dalam 5 pilar yaitu (Brown, 2018):

Pilar I – Identifikasi Risiko

- Sasaran 1: Menilai Risiko Keamanan Siber yang Berkembang. Kami akan memahami postur risiko keamanan siber nasional yang berkembang untuk menginformasikan dan memprioritaskan aktivitas manajemen risiko.

Pilar II – Pengurangan Kerentanan

- Sasaran 2: Melindungi Sistem Informasi Pemerintah Federal. Kami akan mengurangi kerentanan lembaga federal untuk memastikan mereka mencapai tingkat keamanan siber yang memadai.
- Sasaran 3: Melindungi Infrastruktur Penting. Kami akan bermitra dengan pemangku kepentingan utama untuk memastikan bahwa risiko keamanan siber nasional dikelola secara memadai.

Pilar III – Pengurangan Ancaman

- Tujuan 4: Mencegah dan Menghentikan Penggunaan *cyber space* oleh Kriminal. Kami akan mengurangi ancaman dunia maya dengan melawan organisasi kriminal transnasional dan penjahat dunia maya yang canggih.

Pilar IV – Mitigasi Konsekuensi

- Sasaran 5: Menanggapi Insiden Dunia Maya Secara Efektif. Kami akan meminimalkan konsekuensi dari insiden dunia maya yang berpotensi signifikan melalui upaya tanggapan seluruh komunitas yang terkoordinasi.

Pilar V – Mengaktifkan Hasil Keamanan Siber

- Sasaran 6: Memperkuat Keamanan dan Keandalan Ekosistem Cyber. Kami akan mendukung kebijakan dan aktivitas yang memungkinkan peningkatan manajemen risiko keamanan siber global.
- Sasaran 7: Meningkatkan Manajemen Kegiatan Keamanan Siber DHS. Kami akan melaksanakan upaya keamanan siber departemen kami secara terintegrasi dan diprioritaskan.

Dari 5 poin dan beberapa hal yang dijelaskan di dalamnya, maka poin-poin ini memang diperuntukkan untuk menjadi penjelasan sekaligus bagian penting dalam kebijakan mengenai *cybersecurity* terutama untuk menanggapi berbagai kejadian yang mengancam kondisi negara.

3. Hasil dan Pembahasan

Penyerangan terhadap keamanan negara telah mengalami perkembangan seiring berjalannya waktu, bahkan apa yang dilakukan oleh Rusia kepada Amerika Serikat merupakan bentuk serangan baru yang memiliki dampak lebih besar daripada serangan militer. Serangan seperti ini bukan lagi hanya dihadapi oleh negara, bahkan juga oleh perusahaan swasta nasional hingga masyarakat. Rusia memadukan kegiatan *cyberattack* dengan kegiatan intelijen yang disponsori negara dan perusahaan kriminal dalam satu operasi. Hal lain yang menjadi penting dihadapi perusahaan swasta adalah pencurian kekayaan intelektual, yang telah merugikan Amerika Serikat sebesar $180 miliar per tahun (Simon, 2017). Dalam upaya menangani permasalahan ini pemerintah Amerika Serikat bahkan mengajukan suatu konsep mengenai *cybersecurity* pada forum G7 dan G20, kegiatan hubungan bilateral hingga multilateral bahkan banyak dikampanyekan oleh Amerika Serikat untuk terus meminimalisir kejahatan *cyberattack.*

Berbagai kebijakan yang dipilih oleh pemerintah Amerika Serikat dalam menegakkan *cybersecurity,* merupakan bentuk dari upaya mengamankan keamanan nasional Amerika Serikat sendiri. “Tindakan, Baik dari aktor negara atau non-negara, upaya untuk menghancurkan informasi digital atau perangkat keras fisik termasuk dalam ranah operasi siber militer dan dapat diperlakukan sebagai masalah keamanan nasional” (Herr & Friedman, 2015). Hal ini menjadi salah satu latar belakang Amerika Serikat untuk bertindak tegas pada kondisi *cybersecurity* nasionalnya, terutama dengan beberapa latar belakang masalah penyerangan infrastruktur vital seperti bank. Upaya langsung yang dilakukan oleh pemerintah Amerika Serikat saat itu adalah melakukan perbincangan, melalui pemimpinnya Donald Trump yang melakukan dialog langsung dengan pemimpin Rusia yaitu Vladimir Putin, mengenai konflik pada bidang *cyber* yang terjadi di antara keduanya, hal itu dilakukan di sela-sela acara pertemuan G20 Juli 2017 di Hamburg-Jerman, (Geller, 2018).

Selain itu juga lembaga negara seperti *Departement of Homeland Security* (DHS), *Cybersecurity and Infrastructure Security Agency* (CISA), *National Security Agency* (NSA), *Central Intelligence Agency* (CIA), hingga *The White House* turut berperan dalam memerangi *cyberattack* melalui kebijakan *cybersecurity*, keberadaan lembaga-lembaga kenegaraan menjadi sangat penting terutama setalah penyerangan terhadap sistem gedung putih. Dalam kebijakannya Donald Trump sangat menjunjung “*American First*” dalam sistem keamanan, lalu pada Desember 2017 *The White House* mengeluarkan dokumen *National Cyber Security Strategy* yang berisi poin-poin mengenai keamanan Amerika Serikat, yang salah satunya berbunyi “*Dete and disrupt malicious cyber actors. The united states will prioritize the precautionary principle before important infrastructure is attacked. The united states will also invite allies and friendly countries to jointly fight cybercrime*.” (States, 2017).

Pemerintah Amerika Serikat juga mengirimkan tim komando *cyber* ke Eropa untuk melakukan kerja sama memerangi *cyberattack* yang dilakukan oleh Rusia, kegiatan tersebut juga ditujukan untuk mencegah penyebaran disinformasi dan mencegah Rusia ikut campur pemilihan 2020 (Barnes, 2018). Selain upaya yang di lakukan oleh pemerintah melalui lembaga negara, upaya Amerika Serikat dalam menangani kondisi keamanan nasionalnya juga di dukung oleh perusahaan swasta, hal ini tidak terlepas juga dari peran CISA yang memiliki misi untuk berkolaborasi dengan

perusahaan swasta dalam meningkatkan keamanan (CISA, n.d.). Salah satu perusahaan yang banyak berperan dalam upaya maksimal penerapan *cybersecurity* adalah Facebook, hal ini didasarkan pada kasus *Cambridge Analytic* yang melakukan pencurian data Facebook untuk disalah gunakan oleh Rusia dalam persentase kemenangan calon presiden. Perusahaan teknologi Twitter juga melakukan upaya untuk pelarangan iklan bertema politis untuk menghindari pengiringan opini publik dalam hal sosial politik (Conger, 2019).

Pemanfaatan dari badan-badan kenegaraan yang dilakukan oleh Amerika Serikat menjadi penggerak bagi kebijakan *cybersecurity* nasional, integrasi antar badan untuk melakukan berbagai kegiatan terkait permasalahan *cyberattack* juga cukup menjelaskan keseriusan Amerika Serikat dalam merespons ancaman terhadap kedaulatan nasionalnya. Namun sebagai negara yang memiliki banyak perusahaan teknologi nasional, tentu keberadaan perusahaan teknologi nasional juga memiliki peran dalam *cybersecurity* Amerika Serikat, beberapa perusahaan teknologi besar seperti Google, Facebook dan Twitter adalah salah satu penggerak kebijakan *cybersecurity* karena perusahaan-perusahaan tersebut adalah platform yang paling banyak digunakan masyarakat untuk interaksi sosial media. Lalu dengan maraknya aksi *cyberattack* Google, Facebook dan Twitter melakukan kegiatan untuk menghapus berbagai akun palsu dan mempertimbangkan kembali kegiatan iklan ataupun dialog terkait kampanye politis (Maryoto, 2021), hal ini bertujuan untuk meminimalisir kejadian seperti *Cambridge Analytic* terulang terutama pada waktu tertentu. Platform media teknologi yang saat ini marak digunakan oleh masyarakat memang cenderung menjadi sasaran aksi kejahatan *cyberattack* sehingga peran perusahaan teknologi nasional menjadi penting untuk terlibat. Masyarakat juga diharapkan lebih mampu untuk menjaga data pribadi dan privasinya sehingga keamanan nasional akan terdorong menjadi lebih kondusif.

Perkembangan kebijakan mengenai *cybersecurity* yang dilakukan oleh pemerintah Amerika Serikat dan berbagai lembaga lainnya, seiring waktu telah banyak menunjukkan perkembangan. Pemblokiran jaringan terhadap badan riset internet di St.Petersburg yaitu perusahaan yang memiliki kedekatan dengan Vladimir Putin, juga menjadi tolak ukur keberanian pemerintah Amerika Serikat dalam menindak berbagai ancaman yang menintai keamanan nasional Amerika Serikat. Efektivitas kebijakan *cyberattack* Amerika Serikat juga semakin didukung dengan adanya pemberian otoritas baru oleh Presiden Donald Trump kepada komando *Cyber* Amerika Serikat dengan intelijen dari badan keamanan nasional semakin memperkuat efektivitas kinerja pemerintah Amerika Serikat dalam melakukan tindak kepada para pelaku tindak kejahatan *cyberattack* (Nakashima, 2019). Kemajuan dari efektivitas kebijakan Amerika Serikat dalam permasalahan *cyberattack* juga di rasakan dari peningkatan kesadaran masyarakat pasca terjadinya serangan *cyberattack* dalam pemilihan presiden pada 2016 yang melibatkan perusahaan swasta sebagai korbannya.

4. Kesimpulan dan Rekomendasi

Pada dasarnya permasalahan keamanan pada negara saat ini telah berkembang menjadi lebih luas, terutama pasca perang dingin. Pemahaman mengenai keamanan negara yang dulu dilambangkan dengan persenjataan dan ketahanan militer, saat ini digambarkan mengalami perubahan menuju aspek yang lebih modern yaitu teknologi. Maka dari itu keberadaan *cybersecurity* menjadi penting untuk keamanan negara saat ini, terutama sebagai kebijakan sekaligus aturan yang mengatur kondisi keamanan

dalam lingkup *cyber*. kondisi negara yang mulai merasakan adanya efek nyata ancaman *cyberattack* harus lebih mendorong bagaimana kebijakan terkait *cybersecurity* ditetapkan sebagai peraturan hukum yang dilandaskan pada kesepakatan dan rekomendasi dari tata kelola yang ada, hal ini ditujukan untuk lebih membentuk kondisi yang kondusif dari keberlangsungan *cybersecurity*.

Tindakan Amerika Serikat untuk terus berinovasi dalam kebijakan *cybersecurity* juga dapat didasarkan pada perkembangan ancaman yang menjadi lebih multi dimensi, sehingga menjadi pendorong bagi *redefining security*, sehingga keamanan dapat diartikan melalui ancaman yang berada di sekitarnya (Richard H Ullman, 1983). Tujuan Amerika Serikat dalam mengampanyekan *cybersecurity* tidak terlepas dari *national interest* yang ditujukan untuk mengamankan aset nasionalnya yang banyak tersimpan dalam *cyberspace*, terutama dengan maraknya penyerangan pada aset dan sistem nasional yang berpotensi besar mengancam kondisi keamanan nasional Amerika Serikat. pengaruh dari *cybersecurity* diharapkan dapat mengatasi permasalahan *cyber* secara efektif, terutama dalam menanggulangi ancaman terhadap *human security* yang dihadapi oleh Amerika Serikat, perkembangan ancaman yang meluas pada aspek *cyber* adalah ancaman nyata yang telah dijelaskan dalam keamanan non-tradisional bahwa sektor ancaman tidak lagi hanya terbatas pada ancaman militer dan negara, melainkan meluas pada ancaman bersama yang dapat dirasakan dan berdampak langsung pada masyarakat.

Aspek *human security* juga telah banyak menjadi sorotan karena menjadi aspek yang paling terdampak oleh ancaman dari keberadaan *cyberattack*, selain itu aksi *cyberattack* seperti yang sudah dijelaskan pada latar belakang bahwa berbagai aksi kejahatan melalui tindak *cyberattack* telah merugikan kehidupan nasional dan masyarakat Amerika Serikat, dan yang terjadi pada keamanan *cyber* Amerika Serikat telah memberikan gambaran bahwa keamanan nasional memiliki dimensi lebih luas dari hanya tentang negara, melainkan kejahatan *cyberattack* menjadi pembuktian bahwa keamanan bukan hanya terbatas pada kemampuan militer negara, melainkan juga ditentukan pada kondisi masyarakat hingga individu. Konsep mengenai *cybersecurity* adalah bentuk resolusi konflik yang diharapkan mampu menekan eskalasi konflik *cyberattack*, sehingga *cybersecurity* juga diharapkan menjadi sebuah pedoman untuk menghadapi kejahatan *cyber* baik dalam skala nasional maupun internasional dengan dilandaskan pada rekomendasi, kesepakatan hingga hukum internasional.

Perjalanan Amerika Serikat dalam membangun kebijakan *cybersecurity* untuk melindungi kondisi keamanan nasionalnya adalah pelajaran penting mengenai proses pembangunan *cybersecurity* yang lebih kondusif. Posisi *cybersecurity* sebagai kebijakan suatu negara juga harus didasarkan pada rekomendasi, kesepakatan ataupun hukum internasional karena permasalahan *cyber* tidak hanya terbatas pada satu negara atau satu aktor, sehingga dibutuhkan standarisasi dan kebijakan yang telah dikaji pada lingkup internasional dan disepakati bersama oleh berbagai pihak seperti kelompok, organisasi nasional/internasional, masyarakat dan juga negara. hal tersebut diperlukan untuk membangun konsistensi dari penerapan *cybersecurity* pada setiap aspek yang beragam, karena ranah *cyber* memang telah menyebar luas dan berpengaruh pada banyak hal seperti keamanan, ekonomi, kesehatan, hingga pendidikan, oleh karena itu standarisasi menjadi penting untuk menjamin kegiatan

dalam *cyberspace* dapat berjalan dengan aman dan kondusif sehingga tidak menimbulkan kerugian bagi masyarakat.

Daftar Pustaka

Barnes, J. E. (2018). *U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections*. https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html

Barry Buzan, Ole Waever, J. D. W. (1998). *Security A New Framework For Analysis*.

BBC. (2019). *Evil Corp: US charges Russians over hacking attacks*. BBC News. https://www.bbc.com/news/world-us-canada-50677512

Brown, M. L. (2018). *DHS Releases Its Cybersecurity Strategy −*. 1–5.

Caballero-Anthony, M. (2016). An Introduction to Non-Traditional Security Studies: A Transnational Approach. *An Introduction to Non-Traditional Security Studies: A Transnational Approach, Energy Security*. https://doi.org/10.4135/9781473972308

CISA. (n.d.). *Capability Delivery*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/about/divisions-offices/cybersecurity-division/capability-delivery

Conger, K. (2019). *Twitter Will Ban All Political Ads, C.E.O. Jack Dorsey Says*. https://www.nytimes.com/2019/10/30/technology/twitter-political-ads-ban.html

Geller, E. (2018). *Trump-Putin meeting rekindles ridiculed cyber plan*. https://www.politico.com/story/2018/07/16/trump-putin-russia-cybersecurity-689470

Herr, T., & Friedman, A. (2015). *The American Foreign Policy Council Defense Technology Program Brief. January*.

Jimenez, N. (2022). *Cyber-attacks on small firms: The US economy's "Achilles heel"?* BBC News.

Kusnanto, A. (2003). KEAMANAN NASIONAL, PERTAHANAN NEGARA, DAN KETERTIBAN UMUM Oleh: Dr. Kusnanto Anggoro. *Keamanan Nasional, Pertahanan Negara, Dan Ketertiban Umum*, 1–10.

Mallin, A. (2019). *Russian nationals indicted by DOJ in alleged massive hacking and bank fraud scheme*. https://abcnews.go.com/Politics/russian-nationals-indicted-doj-alleged-massive-hacking-bank/story?id=67518005

Maryoto, A. (2021). *Kontroversi Obrolan Politik di Perusahaan Teknologi*. Kompas. https://www.kompas.id/baca/opini/2021/05/06/kontroversi-obrolan-politik-di-perusahaan-teknologi/

Nakashima, E. (2020). *Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce*. The Washington Post. https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html

Nakashima, E., & Timberg, C. (2020). *Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce*. https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-

agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html

Osborn, A., & Tsvetkova, M. (2019). *Putin says U.S.-Russia relations are getting "worse and worse."* https://www.reuters.com/article/us-usa-russia-putin-idUSKCN1TE0L7

Sanger, D. E. (2020). *Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect*. https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html

Simon, D. A. (2017). *Raising the Consequences of Hacking American Companies*. *October*, 1–16.

States, U. (2017). National Security Strategy of the United States of America, 2006, 2015. *Foundations of Homeland Security: Law and Policy: Second Edition*, 175–180. https://doi.org/10.1002/9781119289142.ch9

Wang, J. P. (2009). *Computer Network Security Theory and Practice*.