BAB I
PENDAHULUAN

A. Latar Belakang Masalah

Studi mengenai keamanan telah menjadi perdebatan panjang bagi para ilmuan hubungan internasional. beberapa dari mereka menganggap wilayah cakupan dari "keamanan" hanya meliputi negara dan usahanya untuk bertahan dan menghadapi negara lain, pandangan ini disebut dengan "keamanan tradisional". Tetapi sebagian ilmuan yang lain memandang dunia telah berkembang sehingga konsep tentang keamanan tidak hanya meliputi aktor negara saja, melainkan berfokus kepada aktor non-negara beserta ancaman non-militer atau lebih dikenal sebagai "keamanan non-tradisional". Menurut Barry Buzan, Isu-isu dari keamanan non-tradisional ini tidak hanya mengancam keamanan serta kedaulatan suatu negara, lebih dari itu isu ini dapat mengancam masyarakat, kelompok, ataupun individu (Buzan, Wilde, & Wæver, 1997).

Perkembangan dan penggunaan teknologi di masa ini tidak hanya memberikan manfaat positif bagi masyarakat, tetapi menimbulkan beberapa ancaman baru yang lebih kompleks. Dimensi ancaman yang ditimbulkan dari kemajuan teknologi ini tidak hanya berada di dimensi nyata, tetapi menyerang pada dimensi virtual atau yang lebih dikenal sebagai ancaman siber. Ancaman siber ini berpotensi dapat mengancam keamanan dan pertahanan dari suatu negara. Motif yang dilakukan oleh pelaku kejahatan ini tidak hanya didasarkan pada motif ekonomi saja, pada beberapa kasus tindakan serangan siber ini bersifat politis dengan tujuan untuk menggangu pertahanan, keamanan maupun kepentingan nasional dari suatu negara. Ancaman serangan siber ini dianggap sangat berbahaya karena mampu mengakibakan kehancuran, gangguan, kerusakan jaringan infrastruktur militer maupun sipil yang tidak dapat diprediksi dampak dan ukuran yang ditimbulkannya. Hal tersebut semakin kompleks ketika

dunia saat ini sangat bergantung kepada teknologi komunikasi dan informasi sehingga akan berbanding lurus dengan resiko dan ancaman yang akan dihadapinya.

Mayoritas negara di seluruh dunia saat ini telah sadar akan pentingnya pertahanan siber, pertahanan siber adalah tindakan yang terkait dengan manajemen resiko keamanan yang dilakukan oleh organisasi dan negara dalam ruangan siber untuk melindungi kerahasiaan, integritas, dan ketersediaan data dan aset yang digunakan(Schatz et al., 2017). Meningkatnya pengguna internet dalam kurun waktu 10 terakhir ini membuat komunitas dunia digital atau cyber space menjadi lebih luas, tentu konsekuensi yang didapat adalah rentannya pemanfaatan ruang siber oleh pelaku yang tidak bertanggung jawab. Dampak dari ancaman siber dapat berupa penyalahgunaan informasi, pengendalian sistem secara jarak jauh, tindakan terorisme, pemicu konflik, spionase, gangguan fungsional ataupun kondisi merugikan lain nya, hingga dapat mengakibatkan kehancuran secara masif. Ancaman dari ruang siber berpotensi menjadi ancaman yang berbahaya karena sangat banyak celah yang dapat dimanfaatkan oleh para pelaku dan cakupan kejahatannya pun sangat luas pada suatu negara, kawasan, ataupun global.

Target penyerangan siber ini tidak memandang negara kuat ataupun negara lemah. Amerika Serikat sebagai salah satu negara dengan kemanan siber terbaik di dunia pun sering menjadi target operasi dari kelompok peretas yang menyerang beberapa titik vital Amerika Serikat. Menurut *Global Cybersecurity Index* tahun 2018 Amerika Serikat menempati posisi kedua dibawah Inggris sebagai negara yang memiliki keamanan siber terbaik karena memiliki pilar hukum dan memiliki berbagai regulasi hukum, baik substantif maupun prosedural yang mencakup kejahatan dunia maya (ITU, 2019).

Tahun 2017 terjadi serangan siber terbesar yang menyerang berbagai negara di dunia, salah satunya adalah Amerika Serikat. motif serangan ini adalah pelaku menyerang

dan mengunci data dari targetnya dan meminta tebusan sesuai dengan nominal yang sudah ditentukan oleh pelaku dalam waktu yang terbatas. Jika dalam waktu yang telah ditentukan korban membayar tebusannya maka data-data tersebut akan aman, tetapi jika tidak data pengguna tersebut akan hilang secara permanen. Nominal tebusan yang diminta oleh pelaku beragam, tetapi mereka hanya menerima pembayaran melalui bitcoin. Bitcoin ini beroperasi pada sistem blockchain yang dikenal dengan sifat anonimitasnya sehingga para peretas lebih memilih menggunakan bitcoin sebagai alat transaksi mereka.

Pada tanggal 7 Mei 2021, *Colonial Pipeline*, sebuah sistem pipa minyak Amerika yang berasal dari Houston, Texas, mengalami serangan siber ransomware yang berdampak pada peralatan komputerisasi yang mengelola pipa tersebut. Serangan ini dikatakan merupakan serangan paling "mengganggu" yang pernah dilaporkan sepanjang tahun 2021 dan menarik perhatian dari berbagai kalangan mengenai rentannya keamanan siber infrastruktur Amerika Serikat terhadap serangan siber (Bing & Kell, 2021). Akibat serangan ini, *Colonial Pipeline* terpaksa menutup jalur pipa mereka selama hampir satu minggu dan menyebakan lonjakan harga bahan bakar dan tindakan *panic buying* bagi konsumen, kejadian ini memberikan dampak yang cukup signifikan bagi perekonomian Amerika Serikat. *Colonial Pipeline* akhirnya memulai pemeriksaan secara menyeluruh terhadap pipa-pipa mereka untuk mencari kerusakan yang terlihat. Pada akhirnya pihak Colonial Pipeline memberikan pernyataan bahwa tidak ada pipa yang rusak, hanya komputerisasi dan sistem yang mengelola pipanya saja yang mengalami masalah (Turton & Mehrotra, 2021). Pihak pemerintah AS melalui FBI pun akhirnya menginvestigasi kejadian tersebut, mereka akhirnya mengkonfirmasi "DarkSide" kelompok peretas asal Rusia yang bertanggung jawab atas insiden tersebut. Kejadian diretasnya infrastruktur penting nasional merupakan kejadian langka di Amerika Serikat, tetapi dari kejadian ini juga mengindikasikan kejahatan siber telah berkembang dan

pemerintah didorong untuk lebih serius dalam menangani serangan siber sekaligus meningkatkan keamanan siber mereka karena jika layanan publik yang diserang oleh peretas maka kemungkinan pelaku untuk meminta tebusan semakin besar (Tidy, 2021).

Hubungan rumit antara Amerika Serikat dan Rusia telah berlangsung sejak mulainya perang dingin. Hubungan antar kedua negara ini seringkali bersitegang bahkan menimbulkan beberapa konflik. Walaupun jarang sekali antar kedua negara ini terjadi konflik bersenjata tetapi ketegangan kedua negara masih tetap berlangsung. Salah satu pemicu ketegangan yang terjadi antar kedua belah negara ini melalui *cyberspace* atau dunia siber. Salah satu kejadian besar yang tercatat dalam sejarah adalah keterlibataan Rusia dalam pemilihan umum Amerika Serikat pada tahun 2016. Serangan siber ini menargetkan calon presiden Hillary Clinton termasuk dalam proses pengkampanyean mereka. Selain itu tujuan lain dari penyerangan ini untuk mencuri data para pemilih (Abrahams, 2019).

Semenjak kejadian tersebut, ketegangan siber kedua negara semakin bertambah. Ketegangan ini semakin menguat akibat perasaan sentimental masyarakatnya dalam membela negara mereka masing masing. Sehingga, walaupun tidak ada keterlibatan pemerintah secara langsung serangan masih tetap bisa terjadi. Hal ini juga yang menciptakan kecenderungan Amerika Serikat lebih rentan diserang oleh pelaku siber dari Rusia dibandingkan dengan negara lain. Di sisi lain juga, akibat ketegangan antara Amerika Serikat dan Rusia membuat peretas dari Rusia cenderung menyerang Amerika Serikat dibandingkan negara besar lainnya seperti Inggris atau China. Hal ini juga yang melatarbelakangi motif “Darkside” sebagai pelaku utama dari penyerangan Colonial Pipeline. Walaupun motivasi utama mereka menyerang Colonial Pipeline hanya demi uang, tetapi terdapat hal lain yang melatarbelakangi pihak tersebut akhirnya memilih Amerika Serikat sebagai targetnya.

B. Rumusan Masalah

Dengan latar belakang di atas kemudian penulis menarik rumusan masalah yaitu:

Bagaimana Pemerintah Amerika Serikat mendorong isu keamanan siber Ransomware pada Kasus Colonial Pipeline di tahun 2021 sebagai isu yang mengancam?

C. Kerangka Teori

Teori Sekuritisasi

Teori Sekuritisasi adalah teori yang berkembang bersamaan dengan berkembangnya konsep keamanan non-tradisional. Teori ini menunjukan jika suatu isu keamanan tidak muncul secara alami tetapi muncul karena dibuat oleh para pembuat keputusan. Teori ini menyatakan sebuah isu dapat dikatakan sebagai isu keamanan yang ekstrim ketika aktor sekuritisasi yang memiliki kekuatan dalam kelembagaan maupun kekuatan sosial melabeli isu tersebut sebagai isu yang berbahaya, mengancam, dan mengkhawatirkan (McGlinchey et al., 2017). Aktor sekuritisasi memerlukan sebuah langkah politis dalam mengubah suatu isu menjadi sebuah isu yang di sekuritisasi melalui pengadaan sumber daya yang berasal dari aktor-aktor penting dalam proses sekuritisasi(Trihartono et al., 2020). Menurut buzan, inti dari teori sekuritisasi adalah *speech act*, yaitu bagaimana seorang aktor sekuritisasi dapat membingkai suatu isu sebagai masalah sekuritisasi kepada para penonton agar secara kolektif mengangkat masalah tersebut sebagai masalah yang "mengancam" (Buzan et al., 1998). Tetapi jika penonton secara kolektif tidak menganggap masalah tersebut sebagai suatu ancaman, maka *speech act* yang dilakukan aktor sekuritisasi gagal dan masalah tersebut tidak dapat tersekuritisasi.

Menurut Barry Buzan, Ole Wæver, dan Jaap de Wilde, dalam melakukan analisa terhadap studi keamanan tertadapat tiga tipe unit:

1. *Referent Objects*, sesuatu yang dilihat sebagai objek yang terancam dan mendapatkan klaim yang sah untuk mendapatkan perlindungan.
2. *Securitizing Actors*, merupakan aktor yang melakukan tindakan sekuritisasi terhadap suatu isu yang terancam keamanannya.
3. *Functional Actors*, aktor pendukung yang tidak harus bertindak seperti *Referent Objects* dan *Securitizing Actors* tetapi dapat mempengaruhi dinamika suatu sektor keamanan. (Buzan et al., 1998)

Dalam penelitian ini, kelompok dan individu menjadi *referent objects* atau objek yang terancam, kemudian pemerintah Amerika Serikat sebagai *securitizing actors* atau aktor yang melakukan tindakan sekuritisasi, terakhir *functional actors* yaitu para pakar teknologi dan keamanan siber yang turut memberikan pengaruh terhadap sektor keamanan.

Pada penelitian ini, peneliti akan berfokus kepada Amerika Serikat sebagai *securitizing actors* yang melakukan tindakan sekuritisasi terhadap kasus kejahatan siber ini. Pemerintah Amerika Serikat melihat kejahatan siber harus menjadi prioritas karena subjek yang diserang tidak menentu, dapat menyerang instansi, individu, atau bahkan perusahaan seperti yang terjadi pada Perusahaan *Colonial Pipeline*. Amerika Serikat menjadi securitizing actor karena beberapa hal, diantaranya karena Pemerintah Amerika Serikat sebagai aktor politis dapat dengan mudah membingkai suatu isu menjadi isu yang "mengancam" sehingga proses sekuritisasi akan semakin mudah dilakukan. Argumen yang dibangun oleh aktor sekuritiasi dalam melakukan "speech act" juga

biasanya seputar perlunya meningkatkan pertahanan dan keamanan negara, bangsa ataupun sebuah sistem yang lebih besar (Buzan et al., 1998).

D. Hipotesis

Berdasarkan data di atas penulis menyimpulkan jawaban sementara penulis dapat menyimpulkan:

> Pemerintah Amerika Serikat Membingkai Isu Ransomware Sebagai Isu Keamanan Negara yang Mengancam Melalui *Speech Act*. Pemerintah Amerika Serikat melakukan respon terkait isu tersebut dengan membuat kebijakan terkait keamanan siber serta memperkuat memperkuat standar keamanan digital dan standar perangkat lunak sebagai alat pertahanan digital di seluruh sektor swasta.

E. Metode Penelitian

a) Jenis Penelitian

Metode penelitian yang digunakan penulis adalah metode kualitatif dengan menggunakan susunan analisis deskriptif. Penelitian ini mengolah data-data yang berbagai literatur ilmiah yang diolah melalui kata-kata yang memiliki makna sehingga akan menciptakan hasil yang relevan dan dapat dipahami. Tujuan dari penelitian kalitatif adalah memahami suatu konteks dari permasalahan tertentu melalui pendeskripsian secara rinci dan mendalam yang sebenarnya terjadi di lapangan studi (Nugrahani, 2014).

b) Teknik Pengumpulan Data

Teknik pengumpulan data yang penulis gunakan berasal dari lakukan berasal dari studi literatur dan *online research*. Penelitian ini dilakukan dengan cara menganalisa dan menjelaskan fakta secara sistematik

dengan tujuan agar penulis lebih mudah dalam menarik kesimpulan berdasarkan teori – teori yang relevan. Jenis data yang digunakan penulis berupa data sekunder yang diperoleh dari literatur berupa buku, jurnal, artikel dan media baik cetak maupun elektronik. Pengambilan data dari sumber internet didapatkan melalui proses selektif dan berasal dari sumber yang terpercaya.

c) Teknik Analisis Data

Penulis menggunakan teknik analisis data interaktif dari milles dan huberman. Analisis data ini menggunakan tiga komponen utama yaitu reduksi data, sajian data, dan penarikan kesimpulan. Ketiga komponen data tersebut harus ada karena ketiga komponen tersebut memiliki keterkaitan dan dapat menentukan simpulan di akhir penelitian (Nugrahani, 2014). Pengumpulan data dilakukan secara terus menerus oleh penulis hingga dapat menemukan simpulan di akhir.

F. Batasan Penelitian

Pembatasan penelitian digunakan untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah agar penelitian lebih terfokus dan memudahkan dalam pembahasan sehingga tujuan penelitian akan tercapai. Pada penelitian ini penulis akan berfokus pada kasus peretasan Colonial Pipeline di tahun 2021 dan luas lingkup pembahasan hanya seputar keamanan siber di Amerika Serikat. Peneliti juga membatasi penelitian mengenai keamanan siber di Amerika Serikat pada lima tahun terakhir (2017-2021).

G. Tujuan Penelitian

1. Mengetahui pentingnya melakukan keamanan siber sebagai bagian dari prioritas negara dalam mengamankan

kepentingan di ruang maya yang memiliki dampak pada dunia nyata.

2. Mengetahui tindakan sekuritisasi pemerintah Amerika Serikat pada saat kejadian penyerangan Ransomware dan mengetahui kebijakan perlindungan keamanan siber yang dimiliki oleh Amerika Serikat.
3. Mengetahui dampak penyerangan siber Ransomware bagi *Colonial Pipeline* sebagai salah satu produsen minyak terbesar di Amerika yang mempengaruhi keamanan dan perekonomian negara dan masyarakat.

H. Sisetematika Penulisan

Dalam sistematika penulisan skripsi ini, penulis membagi penulisan kedalam tiga bab, diantaranya adalah sebagai berikut:

BAB I Bab pendahuluan mendeskripsikan mengenai latar belakang masalah, rumusan masalah, kerangka teori, hipotesis, metode penelitian, batasan penelitian, tujuan penulisan, dan sistematika penulisan.

BAB II Menjelaskan mengenai respon pemerintah Amerika Serikat dalam penanganan keamanan siber dan mengetahui perkembangan keamanan pemerintah siber Amerika Serikat setelah kejadian peretasan sistem komputer pada peruisahaan *Collonial Pipeline*. Pada bab ini juga penulis menjelaskan langkah sekuritisasi pemerintah Amerika Serikat dalam penanganan kejahatan siber melalui teori sekuritisasi oleh Barry Buzan, Ole Wæver, dan Jaap de Wilde.

BAB III Berisi kesimpulan singkat, rinci, dan jelas dari penelitan yang telah dilakukan oleh penulis pada bab-bab sebelumnya.