BAB I

PENDAHULUAN

1.1 Latar Belakang

Globalisasi memerlukan arus informasi dan proses informasi yang sedemikian besar dan cepat, hal tersebut sulit dicapai tanpa kehadiran teknologi informasi dan komunikasi. Tuntutan global yang kuat pada potensi transformasi dari teknologi baru ini menuntut komunikasi melalui internet tanpa terhalang oleh perbedaan waktu dan batas wilayah. Kini perkembangan teknologi informasi dan komunikasi telah menghadirkan tranformasi signifikan pada konsep keamanan (Rahmawati, 2017). Saat ini, negara-negara bebas untuk berinteraksi dan melakukan komunikasi lewat dunia maya/internet. Dengan begitu, negara memerlukan adaptasi baru sejalan dengan perkembangan ini. Maka konsep keamanan siber merupakan elemen penting dari sebuah negara dalam mengamankan stabilitas keamanan negaranya.

Era globalisasi mendorong interaksi dalam dunia nyata yang terjadi antar aktor-aktor hubungan internasional beralih pada teritori baru yaitu dunia maya/internet. Sebagai konsekuensinya, tren ancaman siber akan berkembang terus selaras dengan perkembangan teknologi informasi. Ancaman serangan siber tidak semata-mata hanya sebuah konsep, rentannya pertukaran informasi di ruang siber justru menuntut sebuah negara untuk mengembangkan sistem keamanan siber negaranya dalam menangani ancaman tersebut. Oleh sebab itu, perlu dilakukan penelitian agar negara mampu memperoleh teknik, taktik dan, strategi pertahanan siber yang akan terus berkembang. Bentuk evolusi peperangan baru di era globalisasi saat ini adalah *cyber war* dimana serangan siber tidak hanya terjadi pada institusi publik saja, namun juga menyerang institusi pemerintahan suatu negara.

Bersamaan dengan bertambahnya ruang interaksi antar aktor hubungan internasional saat ini justru telah merubah makna *power* menjadi lebih luas dalam hubungan antar negara. Dalam ruang darat, laut, dan udara tolak ukur *power* lebih

mudah dicari tolak ukurnya, namun dalam *cyberspace* standarisasi *power* justru menjadi kabur. Kini *cyberspace* menjadi ruang sekaligus sarana baru dalam mencapai kepentingan yang kemudian dikenal dengan *cyberpower* (D. dan T. A. Triwahyuni, 2016). Maka dari itu, dalam menanggapi ancaman *cyber* maka suatu negara membutuhkan pengelolaan keamanan *cyber* melalui regulasi kebijakan di bidang *cyber security* dan *cyber defense.*

Semenjak sains dan teknologi menjadi sebuah kebijakan yang mendominasi dalam modernisasi, perkembangan teknologi *cyber* di Tiongkok kini mengalami pertumbuhan yang pesat. Dengan berkembangnya kemajuan teknologi informasi tersebut, Tiongkok memiliki kemampuan untuk menggunakan ICT (*Information and Communication Technology)* dalam mendorong peningkatan negaranya dalam sektor ekonomi, pemerintahan dan modernisasi militer. Selain itu, adanya peningkatan kemampuan teknologi siber Tiongkok juga digunakan untuk melaksanakan *cyber attack* pada jaringan informasi global. Kegiatan *cyber attack* Tiongkok ini dikategorikan sebagai pelaksanaan *cyber operation* pada jaringan *cyberspace* global, dan salah satu sasaran Tiongkok ialah jaringan informasi Amerika Serikat (Shoimah, 2016).

Kemajuan teknologi dan informasi tidak hanya bisa menyerang instansi pemerintahan dan militer. Namun hal itu juga dapat mengancam seluruh aspek kehidupan manusia, seperti ekonomi, politik, budaya, dan keamanan suatu negara (Rahmawati, 2017). Misalnya di AS, hampir semua kantor negara dan administrasi publik di AS menggunakan internet. Bidang-bidang seperti industri, perbankan, transportasi, desinfeksi air, administrasi kesehatan hingga keamanan atau militer telah berbasis PC dan menggunakan jaringan internet. Tingginya ketergantungan AS pada TIK dan internet pada akhirnya menghadirkan kelemahan dan bahaya baru bagi kerangka perlindungan jaringan siber negara (Ardianto, 2017).

Kondisi keamanan siber Amerika Serikat masih memerlukan pengembangan yang cukup masif dikarenakan seluruh aspek kehidupan sudah berbasis internet dan

terkomputerisasi, maka timbul risiko ancaman siber yang masuk dari sistem keamanan siber AS yang rentan dan memiliki celah. Salah satu ancaman yang menyerang keamanan siber AS adalah masalah spionase melalui penyadapan oleh Tiongkok terhadap Amerika Serikat. Dalam kasus ini subjek dan objek spionase merupakan individu atau kelompok dalam satu negara dengan catatan bahwa kegiatan spionase atau kegiatan kejahatan siber lainnya merupakan suatu kejahatan siber dari negara bersangkutan. Sebagai contoh, Februari 2015 terjadi serangan DoS yang mengirimkan informasi palsu pada setiap komputer dalam jaringan yang ditargetkan, lalu mengambil keuntungan dari perangkat jaringan yang salah konfigurasi melalui situs hosting GreatFire dan CN-NYTimes. Pada Maret 2015 terjadi pencurian jaringannya diakses selama sekitar satu tahun oleh para peretas dengan kasus pencurian kata sandi di situs register.com (A. Walls, Perkins E, 2013).

Lalu adanya pelanggaran keamanan siber yang dilakukan Tiongkok terhadap Angkatan Laut Amerika Serikat pada Desember 2018 berupa pencurian data-data dan rencana rudal anti-kapal supersonik yang akan dibawa di kapal selam AS dari proyek Sea Dragon. Selain itu terjadi lonjakan spionase digital Tiongkok pada Maret 2020 yang berasal dari laporan oleh perusahaan keamanan siber FireEye, yang telah mengidentifikasi aktivitas dari grup berlabel 'APT41' yang telah menargetkan rahasia dagang dan kekayaan intelektual produsen. Kemudian badan Oktober 2020. National Security Agency (NSA) memperingatkan bahwa 25 Common Vulnerabilities and Exposures (CVEs) sedang digunakan atau ditargetkan oleh aktor siber yang disponsori negara Tiongkok telah melakukan operasi peretasan terhadap jaringan milik Sistem Keamanan Nasional, Pangkalan Industri Pertahanan AS, dan sistem Departemen Pertahanan. NSA juga menyatakan bahwa jaringan-jaringan itu secara konsisten dipindai, ditargetkan, dan dieksploitasi oleh aktor yang disponsori Tiongkok. (Gechev, 2021). Ancaman-ancaman dan kejahatan tersebut perlu diantisipasi, salah satunya melalui keamanan siber sebagai sebuah rangkaian aktifitas ataupun pengukuran yang dimaksudkan untuk melindungi dari disrupsi, serangan, atau ancaman yang lainnya

melalui elemen-elemen cyberspace baik software, hardware, computer network (Fischer, 2009).

1.2 Identifikasi Masalah

Dari beberapa uraian latar belakang yang disajikan, masalah-masalah berikut dapat ditemukan:

1. Bagaimana masalah siber yang terjadi antara Amerika Serikat dengan Tiongkok?
2. Bagaimana upaya dan strategi Amerika Serikat dalam meningkatkan keamanan siber negaranya?

1.3 Pembatasan Masalah

Dalam penelitian ini penulis akan membatasi pembahasanya, fokus penelitian lebih menekankan pada serangan siber terhadap Amerika Serikat tahun 2015-2020, dan bagaimana Amerika Serikat menyusun strategi untuk mengatasi ancaman tersebut. Batasan masalah ini diperlukan untuk lebih mengarahkan penulis agar tetap fokus dalam inti bahasan dari penelitian.

1.4 Perumusan Masalah

Masalah spionase siber yang dilakukan oleh Tiongkok terhadap Amerika Serikat telah berlangsung cukup lama, pihak Amerika Serikat pun telah melakukan tanggapan atas kejadian tersebut. Namun upaya yang ditempuh oleh pemerintah Amerika Serikat nampaknya belum efektif dalam mengatasi permasalahan *cyber attack* yang menyerang negaranya, kemudian dirumuskan suatu masalah yang diteliti yaitu sebagai berikut: "Bagaimana strategi yang dilakukan Amerika Serikat mengatasi ancaman siber dari Tiongkok pada tahun 2015-2020?"

1.5 Tujuan dan Manfaat Penelitian

1.5.1 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

1) Memahami masalah siber yang terjadi antara Amerika Serikat dengan Tiongkok

2) Menganalisis upaya dan strategi Amerika Serikat untuk mengatasi masalah ancaman siber Tiongkok

1.5.2 Manfaat Penelitian

Berdasarkan tujuan penelitian yang hendak dicapai, maka penelitian ini diharapkan mampu memberikan manfaat bagi perkembangan ilmu hubungan internasional. Adapun manfaat penelitian ini ialah sebagai berikut:

a. Manfaat Teoritis

1) Memberikan sumbangan ilmu pengetahuan terkait ruang siber.

2) Memberikan pemahaman tentang masalah keamanan di dalam bidang siber.

3) Memberikan informasi dan data bagi keilmuan hubungan internasional.

b. Manfaat Praktis

1) Hasil penelitian ini diharapkan dapat memberikan kontribusi informasi dan pemahaman tentang pengaruh *cyber attack* terhadap keamanan dan stabilitas nasional suatu negara.

2) Hasil penelitian ini dapat memberikan acuan lahirnya penelitian-penelitian lain terkait keamanan siber.