BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Hubungan Internasional merupakan segala hubungan yang melampaui lintas batas negara. Hubungan Internasional berjalan dengan sangat dinamis, yaitu berjalan sesuai perkembangan kehidupan sosial manusia, dipengaruhi perubahan kondisi lingkungan antar negara, hingga sangat dipengaruhi oleh perkembangan teknologi yang tidak ada habisnya, selalu ada pembaharuan di setiap waktunya.

Perkembangan ilmu pengetahuan dan teknologi yang sangat pesat dan semakin canggih ini khususnya baik dalam bidang transportasi, media, komunikasi internasional, maupun informasi juga dibarengi dengan semakin meningkatnya arus globalisasi yang telah menyebabkan wilayah negara satu dengan wilayah negara yang lain seakan-akan tidak ada lagi batas sehingga perpindahan informasi atau berita dari satu negara ke negara lain dilakukan dengan mudah dan sangat cepat. Semua individu dapat mengetahui segala informasi dalam waktu yang sama di berbagai tempat di dunia.

Dalam konteks hubungan internasional maka hubungan satu negara dengan negara lain pasti akan sangat terbantu dalam menjalin kerja sama, perdagangan, komunikasi dan masih banyak lagi keuntungan lainnya. Namun pertumbuhan pengguna web atau pertumbuhan teknologi canggih di seluruh dunia menjadi lebih cepat dari sebelumnya juga membawa risiko yang besar. Salah satu akibat dari perkembangan teknologi ini juga memunculkan adanya *cybercrime*, dimana dilakukan kejahatan dalam "ruang maya" melalui jaringan komputer dengan media internet yang merugikan orang/pihak lain.

Berbicara dalam lingkup internasional kini keamanan dan ketahanan suatu negara terancam, karena rahasia negara pun dapat diretas atau dikuasai. Hal tersebut akan sangat merugikan bagi negara "korban". Kini kedaulatan dan kekuatan suatu negara tidak lagi hanya dinilai dari ekonomi, budaya, atau militernya melainkan kecanggihan dan pemanfaatan Teknologi Informasi Komunikasi (TIK) juga sangat diperhitungkan.

Interaksi yang dilakukan oleh para aktor hubungan internasional sudah tidak lagi hanya melalui darat atau laut. Namun juga bisa melewati ruang maya atau kita bisa kenal dengan *cyber space*. Dengan adanya pembaruan cara menjalin hubungan antar negara maka muncul juga masalah-masalah yang terjadi karena adanya kebebasan ruang maya. Salah satunya adalah *cyber attacks* atau penyerangan siber. *Cyber attacks* dapat mengganggu aktivitas jaringan informasi berupa digital yang gunakan oleh individu, perusahaan, atau bahkan sekelas pemerintahan pun dapat terserang.

Misalnya, permasalahan database ekonomi, database politik, database militer, dan lainnya telah beralih menjadi operasi berbasis dunia maya demi efisiensi hingga keamanan. Karena itu, secara realistis dibutuhkan kemampuan praktek siber untuk menembus pertahanan suatu bangsa, lalu dilumpuhkannya. Karena kemampuan ofensif dan defensif yang kuat dari dunia maya, menjadikan banyak negara di dunia internasional mulai meningkatkan kemampuan pertahanan *cyberspace* mereka.

Dalam hal tertentu, banyak aspek kompetitif dalam mengembangkan metode yang paling tepat untuk berusaha masuk ke dalam dunia teknologi. Baik itu atas pengembangan kemampuan 5G, campur tangan dalam pemilihan politik negara, atau melakukan tindakan spionase dunia maya untuk merusak lingkungan di suatu negara, semua pelaku yang terlibat akan sangat khawatir dengan konsekuensi negatif yang sangat besar yang mungkin ditimbulkan oleh konfrontasi dunia maya.

Salah satu kasus *cyber warfare* yang menjadi sorotan dunia internasional, salah satunya adalah *cyber warfare* antara Tiongkok dan Amerika Serikat. Hubungan dan segala sesuatu yang terjadi antara Tiongkok dan Amerika Serikat menjadi sebuah perhatian dunia. Kedua negara ini saling bersaing secara militer, politik, ekonomi, hingga siber. Hubungan tersebut selalu berkembang dan berubah selama bertahun-tahun. Keduanya terlihat dari paradigma pemerintahan sebelumnya di Amerika Serikat, ada banyak kejahatan dunia maya yang terjadi di antara kedua negara. Terlepas dari itu, perlu dicatat bahwa semua pemerintah waspada akan kejahatan, baik itu di secara fisik atau dunia maya, dan karena itu semua negara harus berupaya memerangi serangan dunia maya bersama-sama di masa depan. Dalam konteks *cyber attacks* negara yang mendapatkan tuduhan sebagai penyerang ataupun terserang, sama-sama akan menimbulkan citra buruk sekaligus ketegangan bagi negara yang bersangkutan dan bahkan menjadi kewaspadaan terhadap dunia.

Di awal tahun 2000, teknologi komputer menjadi lebih maju dan orang-orang mulai menggunakan program sederhana atau yang sekarang kita kenal dengan aplikasi. Sementara orang-orang sudah mulai bergantung pada internet sebagai alat komunikasi, perkembangan tersebut juga berdampak pada hubungan antara Amerika Serikat dan Tiongkok menjadi lebih tegang. Hal tersebut merupakan hasil dari meningkatnya jumlah masalah spionase dunia maya dari kedua negara. Yang pada akhirnya mengakibatkan kedua negara tersebut menjadi dua pelaku terbesar serangan spionase dunia maya. Perbedaan antara negara terletak pada fakta bahwa Tiongkok sering melakukan serangan dunia maya untuk mengganggu kepentingan bisnis dan berbagai urusan komersial seperti mencuri rahasia dagang, kekayaan intelektual untuk teknologi baru, dan informasi lain untuk menguntungkan diri mereka sendiri secara komersial. Sebaliknya, Amerika Serikat sering dituduh oleh Tiongkok mendominasi internet dengan pengaruhnya dan menggunakan posisi mereka di dunia maya untuk mencari situasi yang menguntungkan dan pengumpulan intelijen mereka sendiri. (Brown, Yung, 2017, *"Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace",* melalui https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/)

Ketika berbicara tentang dua negara besar tersebut, pertanyaan besar adalah apakah ada ruang untuk kolaborasi antara Amerika Serikat dan Tiongkok dalam dunia *cyber*. Lalu pola yang dibuat oleh sejarah, akan menjadi hasil dimasa yang akan datang. Apakah akan ada kolaborasi menuju dunia maya yang lebih baik di masa mendatang, atau sebaliknya terjadi konfrontasi yang dapat menimbulkan dampak negatif yang sangat besar.

Berangkat dari berbagai konflik mengenai dunia *cyberspace* antara kedua negara "*power*" ini, akhirnya menimbulkan rasa ketidakpercayaan dan kewaspaadaan yang serius tentang bagaimana masing-masing negara mempersiapkan bagaimana pertahanan negara sendiri untuk memenuhi kepentingan nasionalnya.

Namun, kedua negara tersebut mengakui bahwa ada penyalahgunaan sistem teknologi secara terang-terangan yang diakui bersama antara kedua negara. Sebagai tanggapan atas berbagai tuduhan yang diajukan oleh kedua negara, Amerika Serikat dan Republik Rakyat tiongkok membentuk perjanjian pada tahun 2015 yang dikenal sebagai *"U.S.-China Cyber Agreement 2015",* pada saat pemerintahan Presiden Barack Obama. Presiden Obama dan Presiden Xi telah membuat perjanjian tersebut dengan harapan dapat mencegah serangan siber yang bermotivasi ekonomi antara kedua negara secara bilateral, serta meredakan ketegangan dalam prosesnya. Perjanjian tersebut datang pada saat ketegangan tinggi, khususnya setelah kebocoran tahun 2013 yang menunjukkan Amerika Serikat meretas organisasi infrastruktur pemerintah Tiongkok dan Hong Kong. Beberapa dari organisasi ini termasuk universitas, bisnis, dan bahkan populasi sipil. (Louie, 2017, *"U.S.-China Cybersecurity Cooperation, Melalui"* https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/)

Pada September 2015, Presiden Obama menjadi tuan rumah atas kunjungan kenegaraan untuk Presiden Tiongkok Xi Jinping. Dari perspektif Amerika Serikat, pokok besar utama serangan tersebut adalah spionase ekonomi siber. Presiden Obama menekankan keinginan Amerika Serikat untuk melindungi perusahaannya dari kekayaan intelektual dan pencurian rahasia dagang. Kesepakatan yang dicapai oleh Obama dan Xi itu menyatakan bahwa harus ada peningkatan komunikasi dan kerja sama antara kedua negara untuk menyelidiki dan mencegah kejahatan dunia maya yang berasal dari negara masing-masing, baik pemerintahan Amerika Serikat maupun Tiongkok harus tidak melakukan peretasan terhadap satu sama lain baik secara sadar ataupun tidak sadar. Kesepakatan siber tersebut yang dicapai oleh Obama dan Xi, seharusnya manjadi pemicu atau landasan untuk menahan diri dari spionase perusahaan antara kedua negara. Perjanjian tersebut seharusnya menjadi awal yang baik bagi hubungan bilateral kedua negara ataupun dunia siber internasional. Seharusnya perjanjian tersebut berperan dalam pembentukan norma internasional.

Isi perjanjian Siber Amerika Serikat Tiongkok tersebut mengandung kesepakatan bahwa Amerika Serikat dan Tiongkok setuju, antara lain, untuk memberikan tanggapan tepat waktu untuk permintaan informasi ataupun bantuan terkait aktivitas dunia maya yang berbahaya. Juga saling menahan diri untuk tidak melakukan atau secara sadar mendukung pencurian kekayaan intelektual yang didukung dunia maya, mengupayakan upaya untuk lebih mengidentifikasi dan menyebarkan norma perilaku negara yang sesuai di dunia maya di dalam komunitas internasional dan membangun mekanisme hubungan tingkat tinggi bersama untuk memerangi kejahatan dunia maya dan masalah terkait.

Namun kesepakatan tersebut tetap membuat Amerika Serikat skeptis tentang apakah Tiongkok akan mematuhi dengan baik perjanjian tersebut, kesediaan Tiongkok untuk berbicara tentang spionase ekonomi sebagai kategori spionase yang berbeda dengan sendirinya untuk mencapai suatu kemenangan.

Beberapa hari setelah kesepakatan, dugaan buruk Amerika terhadap Tiongkok terbukti benar. Fakta menunjukan bahwa kesepakatan tersebut tidak berhasil. Negeri tirai bambu tersebut kembali melakukan peretasan. FBI mengirim peringatan bahwa adanya peretasan berlokasi dari Tiongkok. Tiongkok melakukan kejahatan siber dalam kategori *Corporate Data Theft* yaitu dengan membobol sistem komputer dan mencuri informasi militer dari perusahaan yang dikontrak dengan Angkatan Laut dan Korps Marinir. Akibatnya data pribadi lebih dari 100.000 personil Angkatan Laut Amerika Serikat teretas. Bahkan di keesokan hari setelah kesepakatan Obama-Xi selesai, perusahaan keamanan siber yaitu CrowdStrike mendeteksi adanya tujuh serangan siber Tiongkok terhadap Amerika Serikat. Lima serangan ditujukan kepada perusahaan teknologi Amerika Serikat. dan dua serangan lainnya ditujukan kepada perusahaan farmasi Amerika Serikat. FireEye sebuah perusahaan keamanan siber publik yang berkantor pusat di Milpitas, California, mengatakan bahwa peretasan yang dilakukan oleh Tiongkok disponsori oleh negara. (Brown, Yung, 2017, *"Evaluating the US-China Cybersecurity Agreement, Part 3: The US Approach to Cyberspace",* melalui https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/)

Pejabat senior administrasi Trump dan kontraktor pertahanan menuduh pemerintah Tiongkok melanggar perjanjian Obama-Xi dan menuduh Tiongkok meretas perusahaan swasta Amerika. Peretasan tersebut diakini akan memicu lebih banyak lagi serangan-serangan dan tindakan hukum Amerika Serikat sebagai wujud respon pelanggaran Tiongkok atas "U.S.- China Cyber Agreement". Namun Kedutaan Besar China di Washington tidak memberikan tanggapan komentar. (Lynch, 2018, *"What happen when the US-China Cyber Agreement isn't working?"*, Melalui https://www.fifthdomain.com/international/2018/11/12/what-happens-when-the-us-china-cyber-agreement-isnt-working/)

Alasan Tiongkok melakukan serangan siber tersebut diduga karena motif ekonomi. Begitu perang perdagangan dimulai antara Tiongkok dan Amerika Serikat, Beijing memiliki insentif finansial untuk meretas bisnis Amerika dan meningkatkan pencurian kekayaan intelektualnya. Ross Rustici, seorang direktur senior intelijen ancaman di Cybereason, sebuah perusahaan keamanan siber dalam Lynch "*What happen when the US-China Cyber Agreement isn't working?"* mengatakan bahwa orang Tiongkok didorong ke perjanjian 2015 karena takut mereka akan menghadapi sanksi atau tarif pada produk mereka. Tetapi setelah Presiden Donald Trump memulai perang dagang dengan Tiongkok, Tiongkok menyadari bahwa perusahaannya tetap dihukum dan meningkatkan peretasan sektor swasta mereka. Pemerintahan Amerika Serikat telah menanggapi peretasan Tiongkok dengan mengambil langkah-langkah hukum dan ekonomi. Sejak 2017, pemerintah federal telah mendakwa tiga orang sebagai mata-mata untuk Tiongkok, dan menuntut lima kasus pencurian atau percobaan pencurian lainnya, menurut Departemen Kehakiman.· (Lynch, 2018, *"What happen when the US-China Cyber Agreement isn't working?",* Melalui https://www.fifthdomain.com/international/2018/11/12/what-happens-when-the-us-china-cyber-agreement-isnt-working/)

Pada bulan Juni 2016 FireEye sebuah perusahaan keamanan siber publik yang berkantor pusat di Milpitas, California melaporkaan dan mengklaim jumlah jaringan yang disusupi oleh kelompok peretasan yang berbasis di Tiongkok yang dilacaknya turun dari 60 pada Februari 2013 menjadi kurang dari 10 pada Mei 2016. Fakta tersebut memperlihatkan bahwa adanya penurunan drastis jumlah peretasan. Penurunan julmah serangan tersebut adalah sebuah tanda bahwa Tiongkok melakukan peningkatan kecanggihan serangan. Lalu ada juga laporan lain dari Kaspersky Labs adalah perusahaan yang membuat produk atau perangkat lunak antivirus, anti spyware, anti spam, dan produk keamanan lainnya melaporkan adanya peretasan Tiongkok atas industri pertahanan, nuklir, dan penerbangan Rusia naik hampir tiga kali lipat dalam tujuh bulan pertama tahun 2016. (Segal, 2018, *"The U.S.-China Cyber Espionage Deal One Year Later",* Melalui https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later)

Peneliti memilih judul ini untuk mengetahui dan menganalisa Serangan Siber apa saja yang dilakukan oleh Tiongkok terhadap Amerika Serikat setelah perjanjian Siber 2015. Mengapa Tiongkok melanggar sebuah perjanjian resmi tentang siber untuk tidak saling melakukan peretasan kembali. Dan pemaparan diatas menjadi pendorong untuk peneliti supaya mengkaji lebih dalam dan mengembangkan pengetahuan studi Hubungan Internasional.

Dari penelitian yang dibuat oleh Dewi Purwani dari Universitas Andalas tahun 2019 tentang *"Analisis Motivasi Amerika Serikat Melakukan Kerja Sama Keamanan Siber dengan Tiongkok".* Peneliti menemukan kesamaan dalam meneliti yaitu analisa Kerja Sama Keamanan Siber Amerika Serikat dengan Tiongkok, Kesamaan lain yang ditemukan adalah mengenai konflik siber apa saja yang terjadi antara Tiongkok dengan Amerika Serikat. Perbedaannya peneliti meneliti serangan apa yang terjadi setelah adanya perjanjian siber tahun 2015. Sedangkan peneliti diatas meneliti serangan siber apa saja yang terjadi sebelum adanya perjanjian siber sehingga Amerika Serikat dan Tiongkok melakukan kembali Perjanjian Siber tersebut di 2015.

Dari penelitian yang dibuat oleh Guntomo Raharjo dari Universiras Islam Negeri Syarif Hidayatullah Jakarta tahun 2016 tentang *"Strategi Amerika Serikat dalam Menghadapi Eskalasi Cyber Power Tiongkok 2011-2015".* Peneliti menemukan kesamaan dalam meneliti yaitu bagaimana Tiongkok melakukan *cyber attacks* terhadap Amerika Serikat. Kesamaan lain yang ditemukan adanya respon dan reaksi dari Amerika terhadap serangan siber yang dilakukan oleh Tiongkok. Perbedaannya terjadi pada kurun waktu penelitian kasus tersebut. Peneliti meneliti 2015 hingga 2021 dimana itu adalah setelah *"U.S.-China Cyber Agreement 2015".* Sedangkan peneliti diatas meneliti pada jangka waktu 2011 hingga 2015 yaitu setelah perjanjian pertama ke perjanjian siber kedua negara adidaya tersebut.

Dari penelitian yang dibuat oleh Ryan Fajar Prasetyo dari Universitas Komputer Airlangga tahun 2018 tentang “Kebijakan *Cyber Security* Korea Selatan Pasca terjadinya *Cyber Attack* oleh Korea Utara (2009-2014)”. Peneliti menemukan kesamaan dalam meneliti yaitu tentang adanya penyerangan siber antara dua negara. Persamaan lain yang ditemukan adalah, konsep-konsep yang digunakan. Seperti *cyber attack* dan *cyber security*. Perbedaannya adalah peneliti meneliti penyerangan siber yang dilakukan oleh negara Tiongkok terhadap Amerika Serikat, sedangkan peneliti diatas meneliti penyerangan yang dilakukan oleh Korea Utara kepada Korea Selatan.

Dari penelitian yang dibuat oleh Rahmadi Pratama Aritonang dari Universitas Airlangga tahun 2019 tentang ”Operasi Siber Ofensif Iran terhadap Amerika Serikat, Israel, dan Arab Saudi: Kepentingan dan Strategi Ofensif Iran”. Peneliti menemukan kesamaan dalam meneliti yaitu tentang adanya penyerangan siber terhadap negara Amerika Serikat. Perbedaannya adalah peneliti meneliti penyerangan siber yang dilakukan oleh negara Tiongkok, sedangkan peneliti diatas meneliti penyerangan yang dilakukan oleh negara Iran.

Dari penelitian yang dibuat oleh Mega Ramadhanty dari Universitas Jenderal Achmad Yani 2018 tentang “Faktor-faktor Penyebab Amerika Serikat menjadikan Tiongkok sebagai Ancaman utama Keamanan *Cyber* Periode 2007-2014”. Peneliti menemukan kesamaan dalam meneliti yaitu adanya kekhawatian dari Amerika Serikat merasa terancam dengan serangan *cyber* yang dilakukan oleh Tiongkok. Perbedaannya adalah peneliti tidak hanya meneliti faktor-faktor penyebab Amerika Serikat menjadikan Tiongkok ancaman keamanan siber, namun juga meneliti serangan apa yang dilakukan.

Maka dengan adanya kekosongan-kekosongan diatas dan latar belakang penelitian inilah yang mendorong peneliti mencoba memberikan pembaharuan dengan mengajukan penelitian yang berjudul:

“Serangan Siber Tiongkok kepada Amerika Serikat Pasca Kesepakatan Keamanan Siber 2015”

Penelitian ini berdasarkan pada beberapa mata kuliah dalam kurikulum Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Komputer Indonesia yaitu:

1. Hubungan Internasional di Amerika Utara, Mata kuliah ini mempelajari tentang hubungan antar negara di Amerika Utara. Amerika Serikat terletak di benua Amerika tepatnya di Amerika Utara. Mata kuliah ini membantu peneliti untuk mengetahui arah kebijakan luar negeri Amerika Serikat pada masa lampau dan sekarang.
2. Hubungan Internasional di Asia Timur, Mata kuliah ini mempelajari tentang hubungan antar negara di Asia Timur. Tiongkok berada di benua Asia yang tepatnya terletak di Asia Timur. Mata kuliah ini membantu peneliti untuk mengetahui arah kebijakan luar negeri Tiongkok pada masa lampau dan masa sekarang.
3. Politik Luar Negeri, Mata kuliah ini membantu peneliti untuk menganalisa arah politik luar negeri yang dilakukan Tiongkok, bagaimana Tiongkok melakukan

kebijakan untuk menyerang Amerika Serikat setelah melakukan perjanjian siber.

4. *Cyber Security*, Mata kuliah ini mempelajari tentang teknik pengamanan dan proteksi bagi industri atau pun pemerintah dari serangan di dunia siber. Mata kuliah ini membantu peneliti menganalisi strategi pertahanan negara Tiongkok dan Amerika Serikat dalam menghadapi serangan siber.
5. *Cyber Law*, Mata kuliah ini mempelajari tentang ruang lingkup yang meliputi aspek hukum dan menggunakan pemanfaaatan teknologi internet. Mata kuliah ini membantu peneliti untuk menganalisa fenomena penyerangan siber Tiongkok terhadap Amerika serikat dalam perspektif hukum siber.

1.2 Rumusan Masalah

1.2.1 Rumusan Masalah Mayor

Berdasarkan latar belakang diatas, peneliti merumuskan masalah utama dari penelitian ini adalah sebagai berikut “Bagaimana Serangan Siber Tiongkok pada Amerika Serikat Pasca Perjanjian Siber dengan Amerika Serikat 2015”

1.2.2 Rumusan Masalah Minor

1. Apa saja Serangan Siber yang dilakukan Tiongkok kepada Amerika Serikat Pasca Perjanjian Siber 2015?
1. Apa Kepentingan Tiongkok dengan tindakan mengabaikan Perjanjian Siber 2015 dengan Amerika Serikat?

2. Bagaimana Amerika Serikat merespon Serangan Siber Tiongkok Pasca Perjanjian Siber 2015?

1.2.3 Pembatasan Masalah

Berdasarkan yang penulis telah uraikan dalam latar belakang dan rumusan masalah, maka penulis membatasi masalah dengan kurun waktu 2015 hingga bulan Maret 2021 untuk meneliti serangan siber yang dilakukan oleh Tiongkok setelah adanya perjanjian siber antara Tiongkok dengan Amerika Serikat pada tahun 2015. Pembatasan masalah diteliti hanya 6 tahun mengingat pada tahun 2015 adalah dimulainya kesepakatan "U.S.-China Cyber Agreement". Lalu Tiongkok melakukan pelanggaran dan akhirnya muncul kembali serangan antara Tiongkok dengan Amerika Serikat hingga saat ini.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Maksud dari penelitian ini untuk mengetahui serangan siber apa saja yang dilakukan Tiongkok kepada Amerika Serikat setelah adanya perjanjian Siber 2015.

1.3.2 Tujuan Penelitian

Adapun tujuan dari dilakukannya penelitian ini adalah sebagai berikut:

1. Untuk mengetahui dan menganalisa serangan siber apa saja yang dilakukan Tiongkok terhadap Amerika Serikat setelah adanya perjanjian siber di tahun 2015.

2. Untuk mengetahui dan menganalisa kepentingan Tiongkok dengan tindakan mengabaikan perjanjian siber dengan Amerika Serikat.
3. Untuk menggambarkan respon Ameika Serikat atas serangan siber Tiongkok setelah adanya perjanjian siber 2015.

1.4 Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Penelitian ini diharapkan dapat berguna untuk memperkaya pengetahuan keilmuan dan pemahaman perihal Cyber Attacks sebuah negara terhadap negara lain, dan dampak apa yang terjadi akibat dari adanya penyerangan tersebut.

1.4.2 Kegunaan Praktis

Melalui penelitian ini, kegunaan bagi peneliti untuk memperoleh gelar Sarjana S-1 (Strata Satu) pada Progam Studi Hubungan Internasional Universitas Komputer Indonesia. Kepada penstudi Hubungan Internasional yang tertarik terhadap Serangan Siber juga diharapkan dapat membantu menambah wawasan.