BAB I
PENDAHULUAN

1.1 Latar Belakang

Meningkatnya ketergantungan masyarakat pada teknologi informasi dan komunikasi (TIK) di semua tingkatan telah mengubah cara individu berinteraksi saat ini, baik secara pribadi maupun profesional. Internet telah berkembang pesat sejak komersialisasi pada pertengahan 1990-an. Pada awal abad ke-21, sepertiga populasi dunia memiliki akses ke teknologi. Selain itu, "Internet of Things" akan menghasilkan jumlah perangkat yang terhubung ke jaringan secara eksponensial. Aktivitas sosial dari berbagai masyarakat di dunia dalam segala level yang tersambung dalam internet terdapat dalam yang domain disebut dunia siber, dengan terus berkembangnya teknologi tentunya penggunaan ini akan terus berkembang. Domain siber mencakup arsitektur pengorganisasian Internet, perangkat yang terhubung ke Internet, dan jaringan kabel dan nirkabel. Beberapa dari jaringan ini dikelola oleh entitas pemerintah dan sektor swasta, beberapa terhubung ke Internet yang lebih luas dan beberapa tidak. Skala Internet membuatnya sulit untuk dipahami. Hal ini menyebabkan ketergantungan yang berlebihan pada analogi yang tidak tepat. Sementara Internet secara teknis adalah domain pertama yang murni dibuat oleh manusia, strukturnya mungkin sulit untuk dikonseptualisasikan. Alih-alih eksis dalam batas yang terbatas, ia meniru sistem alami lainnya seperti koloni bakteri dan galaksi yang berkembang, di mana miliaran node berkembang ke segala arah. Akibatnya, domain siber, terutama jaringan komputer berjaringan, yang beroperasi pada protokol transfer data di mana-mana, menjadi kompleks secara interaktif dan struktural. (Chang, 2011)

Cyberspace yang merupakan struktur global, dengan sedikit alat untuk menentukan batas yurisdiksi. Cyberspace telah memicu serangkaian penyesuaian ekonomi, sosial dan politik dari arena lokal hingga internasional. Selain itu, keamanan telah dibawa kembali ke garis depan sebagai salah satu perhatian utama yang mempengaruhi cara negara-negara berinteraksi. Keamanan bukanlah bagian dari desain asli dunia siber. Domain siber dirancang untuk keterbukaan. Protokol standar untuk transmisi data membentuk perekat yang menyatukan Internet dan

layanan nama domain membantu mengarahkan data ke tempat yang dituju. Akibatnya dari meningkatnya teknologi bersamaan dengan makin beragamnya penggunaannya, hal seperti insentif ekonomi dan politik untuk mengeksploitasi jaringan dengan tujuan jahat juga meningkat, dan keamanan siber telah mencapai tingkat yang sangat diperhatikan negara (Todes, 2004). Keamanan siber berkaitan dengan membuat dunia siber aman dari ancaman siber. Gagasan "ancaman dunia maya" agak kabur dan menyiratkan penggunaan jahat teknologi informasi dan komunikasi (TIK) baik sebagai target atau sebagai alat oleh berbagai aktor jahat. Konsep ancaman keamanan siber sebagai tindakan jahat yang berupaya merusak, atau mencuri data, dan mengganggu kehidupan digital secara umum. Teknologi berbasis cyber sekarang ada di mana-mana di seluruh dunia. Dapat dipastikan bahwa para penjahat, teroris, dan mata-mata juga sangat bergantung pada teknologi berbasis siber untuk mendukung tujuan mereka. Penjahat ini dapat mengakses teknologi berbasis cyber untuk menolak layanan, mencuri atau memanipulasi data, atau menggunakan perangkat untuk meluncurkan serangan terhadap dirinya sendiri atau peralatan lain. Contoh ancaman siber yang umum adalah cyberterrorists, cyberspies, cyberthieves, cyberwarriors, dan cyberhacktivists. Cyberterrorism yang menjadi fokus dalam penelitian kali ini dapat didefinisikan sebagai penjahat yang menggunakan teknologi komputer dan internet, terutama untuk menimbulkan ketakutan dan gangguan. Pemberontak, jihadis dan organisasi teroris transnasional, telah menggunakan internet sebagai alat untuk merencanakan serangan, radikalisasi dan perekrutan, metode penyebaran propaganda, dan alat komunikasi. (Obotivere, 2020)

Terorisme sendiri telah menjadi salah satu isu populer di dunia internasional. Isu ini dianggap sebagai ancaman serius bagi negara-negara di dunia. Ancaman terorisme tidak terlepas dari konstruksi sosial masyarakat internasional. Fenomena terorisme sebenarnya tidak sepenuhnya baru. Namun, studi tentang terorisme baru menjadi populer setelah tahun 2000-an. Beberapa pemicunya adalah serangan teroris di World Trade Center dan gedung Pentagon pada tahun 2001. Peristiwa 911 menandai bahwa terorisme merupakan ancaman serius bagi masyarakat dunia. Bahkan dalam perkembangannya, seiring dengan perkembangan teknologi informasi yang semakin pesat, ancaman yang muncul bisa lebih dari yang

diperkirakan sebelumnya. Dalam beberapa hari setelah serangan fisik ini, sementara negara itu masih menyesuaikan diri dengan hilangnya nyawa dan harta benda yang tragis, serangan cyber cacing Internet, yang disebut Nimda, menyebar ke seluruh negeri dalam waktu kurang dari satu jam dan menyerang 86.000 komputer. Serangan ini meningkatkan kesadaran masyarakat tentang betapa rentannya sistem pada saat itu terhadap serangan dunia maya. Dengan ini, kedepannya ancaman terorisme diprediksi tidak hanya menggunakan senjata konvensional. Dengan penguasaan teknologi digital yang mumpuni atau 'cyber-terror', dapat melumpuhkan aktivitas di sektor vital yang menopang kehidupan seperti ekonomi. Bahkan bisa menimbulkan bencana besar jika kemampuan penguasaan teknologi yang mereka miliki digunakan untuk mengambil alih sumber daya strategis seperti tenaga nuklir. (Kemmerer, 2003)

Salah satu peristiwa *cyber-attack* yang paling besar terjadi di Estonia, Pada musim semi 2007 Estonia jatuh di bawah kampanye serangan dunia maya yang berlangsung selama 22 hari. Serangan itu merupakan bagian dari konflik politik yang lebih luas antara Estonia dan Rusia terkait relokasi monumen era Soviet di Tallinn. Pemicu serangan tersebut adalah keputusan pemerintah Estonia untuk merelokasi sebuah monumen untuk pasukan Soviet dari persimpangan sibuk di pusat Tallinn ke pemakaman militer terdekat. Monumen yang menggambarkan seorang tentara Soviet ini awalnya didirikan pada tahun 1947 di lokasi pemakaman tentara Soviet yang tewas saat merebut Tallinn dalam Perang Dunia II. Sejak saat itu monumen telah mengembangkan dua identitas yang sangat berbeda. Untuk minoritas Rusia lokal itu mewakili "pembebas" sedangkan untuk Estonia itu mewakili "penindas". 27 April menandai dimulainya serangan siber yang menargetkan sistem informasi yang terhubung ke internet Estonia. Serangan dari berbagai jenis berlanjut selama total 22 hari. Meskipun jenis serangannya terkenal, mereka tidak tertandingi dalam ukuran dan variasi dibandingkan dengan negara seukuran Estonia. Selain itu, Estonia sangat berjejaring, sehingga serangan skala luas terhadap ketersediaan layanan digital publik memiliki pengaruh yang signifikan terhadap cara hidup warga negara biasa dan bisnis. Oleh karena itu, serangan siber ini tidak dapat dianggap sebagai gangguan belaka, tetapi harus dianggap sebagai ancaman terhadap keamanan nasional. (Ottis, 2008)

Komputer ada di mana-mana. Hampir semua yang kita lakukan dalam kehidupan sehari-hari bergantung pada komputer dan jaringan komputer. Internet telah menjadi infrastruktur *critical* bagi pemerintah, perusahaan, dan lembaga keuangan. Komputer dan jaringan digunakan untuk mengendalikan dan mengelola proses manufaktur, pasokan air, jaringan tenaga listrik, sistem kontrol lalu lintas udara, dan sistem pasar saham, untuk menyebutkan beberapa. Akibatnya, serangan jaringan mulai berdampak pada aspek praktis kehidupan kita. Ketika masyarakat menjadi lebih bergantung pada komputer dan teknologi terkait untuk memfasilitasi kehidupan sehari-hari seperti sekarang ini, untuk mendukung infrastruktur nasional yang penting dan untuk meningkatkan komunikasi, risiko serangan siber merupakan masalah keamanan yang sangat signifikan dan relevan. (Willam K, 2012)

Isu-isu sosial, ekonomi, kebijakan publik, dan isu-isu manusia dalam kehidupan sehari-hari dari mana pun kita melihatnya, dan apapun kasus nya, media teknologi pasti tidak dapat terpisahkan. Keamanan siber menyentuh keamanan kekayaan digital dan budaya seseorang, organisasi, dan negara. Tantangan yang terlibat sangat kompleks, dan untuk mengatasinya memerlukan kemauan politik untuk merancang dan menerapkan strategi untuk pengembangan infrastruktur dan layanan digital yang mencakup strategi keamanan siber yang koheren, efektif, dapat diverifikasi, dan dapat dikelola. Memperoleh tingkat keamanan informasi yang cukup untuk memenuhi risiko teknologi dan informasi sangat penting untuk berfungsinya pemerintah dan organisasi. Meluasnya penggunaan teknologi digital berjalan seiring dengan meningkatnya ketergantungan pada teknologi tersebut dan saling ketergantungan infrastruktur penting. Hal ini menciptakan kerentanan yang tidak dapat diabaikan dalam berfungsinya institusi, yang berpotensi membahayakan mereka dan bahkan merusak kedaulatan negara. Tujuan dari keamanan siber adalah untuk membantu melindungi aset dan sumber daya organisasi dalam hal organisasi, manusia, keuangan, teknis, dan informasi, yang memungkinkan mereka untuk mengejar misi mereka. Tujuan utamanya adalah untuk memastikan bahwa tidak ada kerusakan abadi yang terjadi pada mereka. Ini terdiri dari mengurangi kemungkinan munculnya ancaman seperti membatasi kerusakan atau malfungsi yang diakibatkannya dan memastikan bahwa, setelah insiden keamanan, operasi normal

dapat dipulihkan dalam kerangka waktu yang dapat diterima dan dengan biaya yang dapat diterima. (ITU, 2007)

Untuk menyiapkan proses keamanan siber, penting untuk mengidentifikasi dengan benar aset dan sumber daya yang perlu dilindungi, sehingga dapat secara akurat menentukan ruang lingkup keamanan yang diperlukan untuk perlindungan yang efektif. Ini membutuhkan pendekatan keamanan global, yang multidisiplin dan komprehensif. Menyadari hal ini, kedua negara yaitu Indonesia dan Amerika Serikat masing-masing telah melakukan usaha mereka dalam mewujudkan keamanan dalam ruang siber. Tentunya kedua negara memiliki tantangan yang berbeda, tetapi kedua negara tersebut telah merasakan secara langsung bahaya dari serangan siber. Indonesia telah mengalami jutaan serangan dunia maya, bahkan Indonesia menjadi salah satu target utama serangan cyber di Asia. Pada tahun 2009 Indonesia juga menjadi salah satu sasaran serangan virus Stuxnet yang oleh banyak pakar cyber dianggap sebagai senjata cyber tercanggih saat ini karena mampu menyerang sasaran tertentu. Serangan siber jika diarahkan pada infrastruktur vital Indonesia, tidak hanya akan menyebabkan kerusakan program, malfungsi, tetapi juga berpotensi menimbulkan korban jiwa. Begitu pula dengan Amerika, negara ini menjadi sasaran serangan siber berganda dibandingkan dengan jumlah serangan siber di Indonesia, sebagai negara maju, Amerika memiliki tingkat penggunaan dan ketergantungan yang tinggi terhadap teknologi komunikasi dan informasi. Bahkan Amerika memiliki kebijakan dalam mengamankan domain ini dan membentuk unit khusus terkait pertahanan dan keamanan domain siber. Indonesia pada tahun 2013 baru memulai tahap penyusunan kebijakan di bidang keamanan dan pertahanan siber, sehingga sangat penting untuk mengambil pelajaran bagaimana Amerika menilai potensi, mengambil manfaat sekaligus mewaspadai ancaman terhadap domain ini secara serius. (Setiyawan, 2019)

Teknologi digital yang melibatkan dunia maya seperti internet memberikan keleluasaan bagi semua pihak, termasuk aktor non-negara seperti individu, kelompok, atau organisasi teroris. Internet sering digunakan oleh organisasi atau organisasi teroris untuk melakukan kegiatan teroris *(cyber terrorism)* untuk mendapatkan dukungan, seperti propaganda dan indoktrinasi. *Cyberspace* menjadi media yang digunakan karena pelaku aktivitas teroris tidak akan segera

teridentifikasi. *Cyberterrorism* memberikan tantangan bagi pemerintah Indonesia untuk berperan signifikan dalam melawan teroris yang melakukan manuever nya di ruang siber. Terorisme siber dapat menjadi metode atau cara yang lebih halus daripada metode tradisional yang umum digunakan. Individu atau organisasi teroris dapat menggunakan nama pengguna atau kode identitas palsu saat masuk ke situs web tertentu. Hal ini dapat memanipulasi aparat keamanan atau polisi untuk menemukan identitas teroris yang sebenarnya. Melalui dunia maya, aksi teroris tidak dibatasi. (Issn & Bagi, 2009)

Jumlah target yang disebabkan oleh aktivitas *cyberterrorist* juga lebih besar. Teroris dunia maya dapat menargetkan jaringan komputer milik individu, pemerintah, komunitas, maskapai swasta, dll. Pilihan target atau kompleksitas target memungkinkan teroris menemukan kelemahan yang bisa mereka manfaatkan. Aktivitas teroris siber dapat dilakukan di perangkat seluler. Terorisme dunia maya tidak memerlukan pelatihan fisik dan psikologis. Kehadirannya dalam berpindah dari satu tempat ke tempat lain membuatnya lebih fleksibel untuk melakukan tindakan seperti merekrut atau mengumpulkan dukungan. Terorisme dunia maya selalu dianggap memiliki dampak yang lebih besar pada manusia. Oleh karena itu, metode ini memobilisasi media yang lebih besar untuk publisitas. (Issn & Bagi, 2009)

Pemerintah Indonesia saat ini sedang dalam tahap perumusan kebijakan, strategi ketahanan dan keamanan sistem informasi dalam rangka menghadapi ancaman siber. Berdasarkan analisis perkembangan lingkungan dan konteks strategis perkiraan ancaman, tantangan, dan risiko penyelenggaraan pertahanan negara, Kementerian Pertahanan menetapkan bahwa kebijakan pertahanan negara, baik pertahanan militer maupun pertahanan nirmiliter nantinya akan memiliki kemampuan pertahanan siber. Pemerintah melihat meskipun inovasi teknologi senjata konvensional masih berkembang, kemajuan ilmu pengetahuan dan teknologi saat ini juga sangat mempengaruhi bentuk dan pola perang di masa depan, salah satunya adalah dengan menciptakan jaringan perang berbasis teknologi informasi dan komunikasi. Pangkalan perang ini secara signifikan mengubah keamanan strategis, terutama dengan penggunaan jaringan komunikasi dan

informasi di seluruh sektor, terutama di sektor pertahanan. (Buku Putih Pertahanan Indonesia, 2014)

Upaya Indonesia dalam mewujudkan dan mengembangkan kemampuan di bidang ini akan menghadapi beberapa tantangan, seperti kebijakan dan pengaturan *cyber law* yang belum memadai, koordinasi dan kerjasama di sektor pemerintah dan swasta yang sangat lemah, tata kelola dan organisasi keamanan siber nasional yang belum bersinergi, belum ada mekanisme standar dan perlindungan infrastruktur vital, infrastruktur informasi vital yang belum terintegrasi dan keterbatasan kualitas dan kuantitas sumber daya manusia khususnya di bidang keamanan siber. Masalah hukum mendasar terkait serangan siber di Indonesia adalah penggunaan perspektif yang sama dalam melihat isu serangan siber. Serangan siber masih dianggap sebagai kejahatan siber yang penanganannya berada di bawah domain Kepolisian Negara Republik Indonesia. Hal ini terjadi karena terbatasnya pengaturan masalah hukum dalam hal pelanggaran, kejahatan dan keamanan siber di Indonesia. (Zainal A, 2013)

Pemerintah Indonesia membentuk Badan Siber dan Sandi Negara (BSSN) melalui Peraturan Presiden Nomor 53 Tahun 2017. Pembentukan badan ini merupakan upaya pemerintah untuk menjaga keamanan siber Indonesia sebagai salah satu bidang Pemerintah yang perlu didorong dan diperkuat untuk meningkatkan pertumbuhan ekonomi nasional dan mewujudkan ketahanan nasional. BSSN adalah lembaga pemerintah nonkementerian yang berada di bawah dan bertanggung jawab kepada presiden melalui menteri yang menyelenggarakan koordinasi, sinkronisasi, dan pengendalian penyelenggaraan pemerintahan di bidang politik, hukum, dan keamanan. Lembaga ini merupakan gabungan dari Lembaga Sandi Negara dan Direktorat Pengamanan Informasi Kementerian Komunikasi dan Informatika. Lembaga ini menyelenggarakan tugas dan fungsi di bidang persandian serta melaksanakan seluruh tugas dan fungsi di bidang pengamanan informasi, pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, dan pengamanan jaringan dan prasarana telekomunikasi. Badan ini menerapkan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengkonsolidasikan semua elemen yang terkait dengan keamanan siber Indonesia. (Setiyawan, 2019)

Menurut Amerika, Cyberspace adalah sektor vital ekonomi global yang dapat menggerakkan ekonomi dan inovasi. Pengembangan domain ini membawa tantangan baru bagi keamanan nasional, ekonomi, dan komunitas global. Isu keamanan nasional di dunia maya telah menarik perhatian negara ini sejak tahun 1992 dan telah menjadi ancaman bagi keamanan nasional sejak tahun 1996. Presiden Obama menyatakan bahwa ancaman dunia maya telah menjadi salah satu ancaman berat bagi perekonomian dan keamanan nasional yang oleh karena itu, Amerika harus siap menghadapinya (Schmitt, 1998). The Director of National Intelligence (DNI) menyatakan bahwa ancaman siber merupakan ancaman strategis nomor 1 di Amerika Serikat untuk menggantikan ancaman teroris yang pertama kali muncul dalam insiden 911. US National Intelligence Officer for Science and Technology menyatakan bahwa peningkatan ancaman cyber didorong oleh beberapa hal seperti peningkatan konektivitas antara jaringan yang aman dan tidak aman, menciptakan celah baru untuk gangguan ke dalam sistem di infrastruktur vital dan kompleksitas jaringan computer yang tumbuh lebih cepat daripada kemampuan untuk memahami dan melindunginya. Serangan dan operasi dunia maya terhadap Amerika sebagian besar dilakukan oleh aktor negara dan non-negara untuk menembus dan mengganggu jaringan dan sistem. Serangan siber digunakan karena kekuatan militer mereka tidak sebanding jika berhadapan langsung. Selain itu, operasi siber dan 8 serangan yang dilakukan terhadap Amerika sering kali mengandung motif ekonomi, industri, dan militer. (Charles G & Chang, 2004)

Pada Februari 2003, Presiden Bush mengeluarkan kebijakan berupa Strategi Nasional Pengamanan Dunia Maya yang menggarisbawahi tiga prioritas, yaitu mencegah serangan terhadap infrastruktur vital Amerika, mengurangi kerentanan nasional terhadap serangan dunia maya dan meminimalkan kerusakan dan waktu pemulihan dari serangan dunia maya. Kebijakan tersebut juga mengidentifikasi lima prioritas nasional yang kritis, yaitu antara lain menerapkan sistem respon keamanan siber, mengurangi ancaman dan kerentanan dunia siber, meningkatkan kesadaran pelatihan keamanan siber, mengamankan ranah pemerintahan siber dan meningkatkan kerjasama di bidang siber baik secara nasional maupun internasional. Kelima prioritas kebijakan tersebut bertujuan untuk meningkatkan sistem keamanan dunia maya pemerintah dan juga infrastruktur vital sektor swasta. Dari 5

prioritas tersebut, dijabarkan lebih lanjut melalui beberapa aksi & inisiatif, antara lain yaitu Mendorong kemitraan melalui kemitraan publik-swasta untuk menanggapi insiden siber, Meningkatkan berbagi informasi terkait serangan, ancaman dan kerentanan siber, Mengutamakan penelitian dan pengembangan keamanan siber, Mengembangkan program pelatihan dan pendidikan di bidang keamanan siber, Memperkuat kontra intelijen siber, Meningkatkan kemampuan melakukan serangan dan merespon serangan, membangun kemitraan internasional untuk melindungi infrastruktur informasi, membangun jaringan pemantauan nasional dan 9 internasional untuk mendeteksi dan mencegah serangan dunia maya. (Chen, 2013)

Di Amerika, tanggung jawab keamanan siber dilakukan oleh the Department of Homeland Security (DHS), the Department of Defense (DoD) dan the Federal Bureau of Investigation (FBI). DHS bertanggung jawab atas keamanan internal. DHS memiliki Divisi Keamanan Siber Nasional yang bertugas bekerja sama dengan lembaga publik, swasta, dan internasional untuk mengamankan dunia maya dan kepentingan Amerika di dunia maya. Divisi ini memiliki National Cyber Response Coordination Group, yang terdiri dari 13 badan federal dan bertanggung jawab untuk mengoordinasikan tanggapan federal terhadap insiden cyber yang berdampak nasional. DHS memiliki National Cybersecurity & Communications Integration Center (NCCIC) dan United States Computer Emergency Readiness Team (US-CERT) yang bertugas mengawasi keamanan siber selama 24 jam. NCCIC berupaya menciptakan infrastruktur dan komunikasi siber yang aman dan tangguh yang mendukung negara, ekonomi, keselamatan dan kesehatan dengan mengurangi kemungkinan dan keparahan dampak insiden siber yang dapat mengganggu keamanan dan keamanan vital jaringan teknologi informasi dan komunikasi. Organ ini bertanggung jawab atas operasi dan komunikasi dunia maya di federal, negara bagian, intelijen, sektor swasta, dan penegakan hukum. (DHS, 2021)

US-CERT memimpin upaya untuk meningkatkan postur keamanan siber, mengoordinasikan berbagi informasi, dan secara proaktif mengelola risiko siber sambil melindungi hak konstitusional rakyat Amerika. Organ ini bertanggung jawab untuk menganalisis dan mengurangi ancaman dunia maya, kerentanan dunia

maya, menyebarluaskan informasi tentang ancaman dunia maya, dan mengoordinasikan tindakan tanggapan atas insiden dunia maya. US-CERT membuat program yang mendorong dan memfasilitasi berbagi informasi dan kolaborasi terkait keamanan siber pada pemerintah, industri, akademisi, dan entitas internasional, seperti US-CERT Portal, Government Forum of Incident Response Security 13 Teams (GFIRST), US-CERT Einstein Program (US-CERT, 2021). Tanggung jawab kedua untuk keamanan siber di Amerika dilakukan oleh the Federal Bureau of Investigation (FBI). FBI adalah badan federal yang bertindak sebagai badan intelijen domestik serta petugas penegak hukum federal. Badan ini bertanggung jawab untuk membela negara dari segala bentuk kejahatan, tindakan terorisme, intelijen asing, penegakan hukum, dan melindungi hak-hak sipil. FBI berfokus pada penanganan ancaman terhadap fondasi rakyat Amerika atau melibatkan ancaman besar dan kompleks terhadap pemerintah negara bagian yang sulit diatasi sendiri. Untuk menghadapi ancaman serta serangan berbasis siber dan kejahatan teknologi tinggi, FBI membentuk Divisi Siber FBI yang memimpin upaya nasional untuk menyelidiki dan menuntut kejahatan di dunia siber termasuk terorisme siber, spionase, intrusi komputer, dan penipuan di dunia maya. Misi ini dilakukan melalui National Cyber Investigative Joint Task Force (NCIJTF) yang diamanatkan oleh Presiden AS untuk menjadi titik sentral bagi semua instansi pemerintah untuk mengkoordinasikan, mengintegrasikan, dan berbagi semua informasi terkait investigasi ancaman cyber. FBI bertanggung jawab untuk mengembangkan dan mendukung gugus tugas gabungan ini yang terdiri dari 19 badan intelijen dan penegak hukum untuk bekerja sama mengidentifikasi aktor-aktor utama 15 dan polanya. Tujuannya adalah untuk memprediksi, mencegah dan mengejar penyerang cyber (FBI, 2021).

Pada intinya, Keamanan siber adalah praktik melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari serangan berbahaya. Ini juga dikenal sebagai keamanan teknologi informasi atau keamanan informasi elektronik. Istilah ini berlaku dalam berbagai konteks, dari bisnis hingga komputasi seluler, dan dapat dibagi menjadi beberapa kategori umum. Dalam hal ini, kedua negara sudah cukup paham bahwa keamanan siber merupakan suatu hal yang perlu diperhatikan yang dapat dilihat dengan perkembangan dalam penanganan serangan

siber yang dilakukan kedua negara. Tetapi tidak dapat dipungkiri bahwa setelah semua penjabaran diatas kita dapat melihat bahwa penanganan siber di Indonesia sangatlah jauh jika dibandingkan dengan apa yang dilakukan Amerika seperti mulai dari lembaga penanganan, mekanisme kerja dan sampai kepada payung hukum yang ada. Jelas Amerika sebagai negara maju dan juga yang lebih dulu memahami pentingnya keamanan siber memiliki sistem yang lebih muktahir dibandingkan Indonesia sebagai negara berkembang, jadi penting bagi Indonesia untuk terus berkaca dan mencoba mempelajari apa yang diimplementasikan di Amerika. Misi Indonesia dalam meningkatkan kualitas keamanan dalam ruang siber akhirnya dapat dilakukan dengan ditandatanganinya LoI yang berisi kerjasama dengan Amerika Serikat dalam peningkatan keamanan ruang siber yang ditandatangani di tahun 2018. Tentunya Kerjasama dalam ruang siber bukan lah hal baru bagi dunia internasional, seperti contohnya pembentukan European Network and Information Security Agency (ENISA) pada tahun 2004, Council Framework Decision on Attacks against Information Systems pada 2005, European Cybercrime Centre pada tahun 2013, dan Tahun 2017 ASEAN mendukung international voluntary cyber norms.

Keberadaan kerjasama ini tentunya diharapkan akan menjadi jawaban dalam penanganan keamanan siber atau setidaknya terdapat peningkatan dalam hal tersebut dikarenakan aspek ini sangatlah penting untuk keamanan nasional didalam perkembangan zaman yang semakin membuat ancaman cyber attack terus meningkat baik dalam intensitas atau kompleksitas. Amerika Serikat yang dapat dinilai sebagai ahli dalam bidang ini diharapkan dapat meningkatkan segala aspek keamanan siber yang terdapat di Indonesia dan dengan ini seharusnya kerjasama ini merupakan Langkah yang sangat tepat. Kendati sudah melakukan kerjasama yang membahas keamanan ruang siber dengan negara besar seperti Amerika Serikat, Indonesia masih belum terlihat mendapatkan peningkatan yang signifikan dalam aspek keamanan siber dikarenakan banyaknya masalah cyber attack yang dialami dan terkesan cukup diremehkan dalam aspek keamanan siber. Salah satu yang paling baru adalah peristiwa dimana situs dari Badan Siber dan Sandi Negara (BSSN) berhasil diretas oleh seorang hacker dari Brazil, dan yang cukup memalukan dari peristiwa ini adalah dimana hacker tersebut menulis bahwa ia

dengan mudah meretas situs lembaga yang seharusnya menjadi garda terdepan Indonesia dalam aspek keamanan siber nasional. Serangan cyber telah meningkat dan perang cyber menghantui keamanan global. Namun, tidak ada kerangka atau otoritas yang mengatur dunia maya yang sekarang dianggap sebagai yurisdiksi negara. Ketiadaan instrumen mendesak tersebut telah menyebabkan kebingungan dan ketidakefektifan untuk memerangi gangguan teknologi tersebut, khususnya dalam hubungan internasional

Untuk meneliti tentang topik Kerjasama Ruang Siber antara Amerika Serikat dan Indonesia, Peneliti akan menggunakan tiga jurnal. Dalam mengidentifikasi usaha-usaha yang dilakukan kedua negara bersangkutan yaitu Indonesia dan Amerika serikat dalam penanganan ancaman yang muncul dari keberadaan ruang siber khususnya dalam konteks kebijakan apa saja yang dikeluarkan oleh kedua negara dalam penanganan ini, penulis menggunakan jurnal karya Anang Setiyawan. Dalam jurnal ini penulis menemukan bahwa kedua negara telah secara mandi membuat berbagai perangkat hukum mengenai cybersecurity, tapi tidak dapat dipungkiri jika dibandingkan lewat aspek hukum dan badan penanganan bahwa level dari Indonesia dan Amerika sangatlah jauh. Amerika memiliki perangkat hukum yang jauh lebih dalam dan kompleks, begitu pula dengan badan penanganannya yang sudah tertata rapi jika dilihat dari *chain of command* yang ada. Ditemukan pula bahwa Amerika sudah jauh terlebih dulu sadar akan pentingnya cybersecurity yang tentunya membuat mereka lebih berpengalaman. Indonesia sendiri sudah memiliki beberapa perangkat hukum tapi belum bisa dikatakan cukup, karena masih banyak lingkup yang belum digapai. Dari sisi badan penanganan, Indonesia juga sudah memiliki BSSN tapi tentunya kinerjanya sendiripun belum bisa dikatakan berhasil. Penguatan kebijakan berupa undang-undang diperlukan untuk memperjelas, memperkuat domain siber sebagai bagian dari domain kedaulatan Indonesia dan memberikan landasan hukum yang dapat menjangkau tingkat ancaman siber yang kompleks, dinamis, dan multidomain. Hukum harus mampu mengkolaborasikan kewenangan, kekuatan dan seluruh pemangku kepentingan terkait mengingat penanganan sifat ancaman siber yang sangat kompleks, dinamis dan multidomain terhadap keamanan, pertahanan, dan kepentingan nasional Indonesia. Dengan ini, kerjasama antara Indonesia dan

Amerika Serikat sebagai negara yang lebih superior dalam aspek cybersecurity diharapkan dapat membantu peningkatan kapasitas penanganan yang ada di Indonesia karena keadaannya masih rentan sekarang. (Setiyawan, 2019)

Dengan tujuan untuk lebih memahami urgensi kerjasama diplomasi dalam peningkatan kapasitas penanganan dalam ancaman siber antara Indonesia dan Amerika Serikat, dapat terlihat dari sisi historis kedua negara dalam penanganan ruang siber. Penulis akan menggunakan jurnal dari Arindha Nityasari. Dengan meneliti jurnal ini penulis menemukan pentingnya *cyber diplomation* dalam usaha penanganan ancaman siber. Sejarah diplomasi siber telah dimulai sejak 2009 ketika Workshop Keamanan Siber diadakan di Wina menyusul kepemimpinan Estonia dalam Forum Organisasi untuk Keamanan dan Kerjasama di Eropa (OSCE) untuk Kerjasama Keamanan. Pada tahun 2010, AS mendorong konferensi untuk merumuskan Confidence-Building Measure (CBM) tentang keamanan siber. Peningkatan kapasitas siber dalam konteks ini dibatasi untuk menyamakan kapasitas semua negara untuk keamanan siber mereka. Yang sering diketahui adalah negara berkembang cenderung kurang siap dibandingkan negara maju. Oleh karena itu, salah satu strategi untuk mengurangi ketimpangan tersebut adalah dengan membentuk Computer Emergency Response Team (CERT) nasional yang memungkinkan negara-negara berkembang untuk meningkatkan kapasitas siber mereka yang terdiri dari pelatihan, transfer teknologi, dan berbagi praktik terbaik dengan jaringan CERT. Terlibat dalam forum-forum diplomasi siber tentunya akan menguntungkan Indonesia dalam arti Indonesia akan memperoleh alih teknologi alat yang digunakan untuk meningkatkan keamanan siber. Forum tersebut juga akan menguntungkan Indonesia dalam hal pertukaran informasi yang akan meningkatkan kapabilitas pemangku kepentingan keamanan siber di Indonesia sebagai individu (misalnya keterampilan manajerial Internet, informasi terkini tentang keamanan siber). Untuk kasus Indonesia, diplomasi cyber telah dilakukan dengan pembentukan CERT pada tahun 1998. Sebagaimana dijelaskan di atas, CERT adalah komunitas yang telah terhubung dengan CERT di setiap negara lain. Indonesia mendirikan CERT dianggap awal di Asia, karena pengembangan CERT di Asia dimulai sekitar waktu itu juga. Tidak seperti CERT di Korea Selatan,

Jepang, dan Australia, CERT Indonesia dibangun oleh komunitas dan bukan didukung oleh pemerintah. (Nityasari, 2021)

Struktur badan penanganan adalah faktor yang sangat penting dalam usaha untuk melawan *cyber attack*, untuk memahami hal tersebut sebuah negara bisa melakukan pengkajian tentang apa yang dilakukan negara lain dalam menghadapi hal yang sama. Kerjasama Indonesia dan Amerika berada di level dimana salah satu pihak lebih superior dan dengan ini pihak lainnya harus belajar dan mencoba mengaplikasikan. Untuk ini penulis memakai jurnal dari Handrini Ardiyanti. Dengan ini penulis dapat melakukan kajian atas hal apa saja yang patut dicontoh oleh Indonesia terhadap rekan kerjasama nya yaitu Amerika. Terkait dengan organisasi pemrosesan keamanan siber. Salah satu strategi menarik yang patut dicermati dalam menghadapi perang siber adalah bahwa pemerintah AS melakukan upaya serius untuk mengembangkan *National Cyber Security Department* (NCSD) atau departemen khusus yang bertanggung jawab menangani keamanan siber nasional, dengan dukungan dari sektor swasta dan di Indonesia juga memiliki bagan yang serupa yaitu BSSN. Departemen dan masyarakat bertanggung jawab untuk membangun dan memelihara sistem keamanan siber nasional atau dunia maya yang efektif, membuat dan menerapkan rencana manajemen risiko dunia siber untuk melindungi telekomunikasi dan infrastruktur siber dari situasi kritis yang dikenal sebagai *National Cyberspace Response System*. Organisasi yang terkait dengan keamanan jaringan harus konsisten dengan organisasi yang menggunakan sistem teknologi informasi, dengan fokus pada empat aspek utama, yaitu: satu adalah sistem informasi, yang lain adalah persaingan organisasi, ketiga, sistem informasi dan keputusan organisasi (sistem informasi dan pengambilan keputusan dalam organisasi), lalu yang keempat, penggunaan sistem informasi organisasi. Dari jurnal ini juga ditemukan bahwa Indonesia memerlukan pengembangan strategi nasional dengan memenuhi empat pondasi yang mendukung perkembangan teknologi informasi termasuk didalamnya pengembangan *cybersecurity* yaitu: perkembangan perangkat lunak *(software)* seperti sistem dan aplikasi dan perkembangan alat keras *(hardware)* perkembangan sarana dan prasarana teknologi informasi, manajemen isi *(content management)*, *telecommunication and networking*, perkembangan internet serta perdagangan online atau melalui internet. (Ardiyanti, 2014)

Dengan mengetahui banyaknya prospek kerjasama antara Indonesia dan Amerika serikat dalam bidang teknologi dan informasi, penulis menyadari bahwa dalam ruang lingkup yang umum kerjasama Indonesia dan Amerika memiliki prospek yang sangat besar dan tinggi. Karena ini, penulis akan meneliti tiga jurnal mengenai kerjasama Amerika Serikat dengan Indonesia. Sama dengan pemikiran penulis, Joshua Kurlantzick lewat karya jurnalnya menyatakan bahwa Indonesia dan Amerika memiliki potensial kerja sama yang sangat besar tetapi realita nya masih fakta yang ada mengindikasikan bahwa kinerja kerjasama yang ada masih belum mendekati potensi besar yang sebenarya dapat dicapai. Indonesia tampaknya akan menjadi mitra alami bagi Amerika Serikat. Sebagai negara terpadat di Asia Tenggara, demokrasi yang dinamis, pemimpin Perhimpunan Bangsa-Bangsa Asia Tenggara (ASEAN), dan anggota G20. Semua hal tersebut menunjukan bahwa Indonesia sering berada dalam kolam yang sama atau setidaknya sejenis dengan Amerika serikat dan seharusnya dapat menimbulkan kerjasama erat yang saling menguntungkan seperti khususnya dalam aspek keamanan. Kurlantzick berpendapat bahwa Indonesia dapat lebih menjadi mitra keamanan bagi Amerika Serikat dan mengusulkan untuk meningkatkan ruang lingkup kerja sama di tiga bidang di mana negara-negara tersebut memiliki kepentingan bersama. Pertama, Amerika Serikat dan Indonesia harus bekerja sama untuk memeriksa ketegasan China yang tumbuh di Laut China Selatan. Kedua, kedua negara harus bersama-sama memerangi ekspansi militan ke Asia Tenggara yang terkait dengan Negara Islam yang memproklamirkan diri. Dan akhirnya, kedua negara harus bekerja sama untuk melawan pembajakan dan kejahatan transnasional lainnya di Asia Tenggara. Semua unsur kerjasama keamanan yang disebutkan oleh Kurlantzick jika dapat terealisasi, penulis percaya bahwa akan dapat berefek dengan peningkatan penanganan ruang siber di Indonesia yaitu khususnya dalam aspek *cyberterrorism.* Seperti kita tahu bahwa teknologi dan informasi seperti khusunya Internet telah terintegrasi dalam segala aspek kehidupan. Dengan diadakannya kerjasama keamanan yang disebutkan diatas, secara natural peningkatan kerjasama ruang siber pun akan terjadi. (Kurlantzick, 2018)

Membahas tentang keamanan, Jurnal karya Frega Wenas Inkiriwang menjelaskan tentang dinamisme serta sejarah kerja sama keamanan yang telah terjadi antara Indonesia dan Amerika. Indonesia memiliki kepentingan strategis bagi AS. Oleh karena itu, AS terus berkontribusi membantu negara mengembangkan militernya setelah Indonesia merdeka. Banyak program, termasuk Pendidikan dan Pelatihan Militer Internasional (IMET), telah memberikan akses bagi personel militer Indonesia ke doktrin dan taktik AS. Kedua negara memandang IMET sebagai indikator hubungan pertahanan mereka. Namun demikian, karena dinamika dan perubahan dalam prioritas kepentingan antara kedua negara, program IMET telah mengalami banyak tantangan. Selama lebih dari satu dekade, Kongres AS memberlakukan larangan program IMET untuk militer Indonesia, dari tahun 1992 hingga 2005. Ketika AS dan Indonesia memiliki kepentingan bersama dan saling melengkapi, hubungan pertahanan antara keduanya positif yang memfasilitasi akses ke program IMET bagi personel militer Indonesia. Ketika terjadi konflik prioritas kepentingan antara kedua negara, hubungan baik sulit dipertahankan. Di akhir periode "Perang Dingin" ketika Tembok Berlin runtuh dan AS tidak lagi memiliki pesaing terdekat, AS mengalihkan prioritas kepentingannya dari membendung komunisme ke mendukung hak asasi manusia sebagai bagian dari demokrasi. Sementara itu, pemerintah Indonesia fokus pada keutuhan dan kesatuan wilayahnya meskipun merugikan hak asasi manusia. Kedua militer memiliki interaksi yang sangat baik. Karena banyak personel militer Indonesia menerima beberapa pendidikan militer profesional mereka di AS, mereka mengadopsi doktrin AS dalam organisasi mereka. Selain itu, Indonesia juga menggunakan sejumlah besar peralatan militer AS, termasuk pesawat dan senjata. Meskipun Kongres AS telah memberlakukan larangan IMET pada militer Indonesia setelah pembantaian Timor Timur, militer AS masih berusaha untuk mempertahankan hubungan dengan rekan-rekan mereka dari Indonesia. (Inkiriwang, 2020)

Dari beberapa jurnal yang telah diteliti penulis dapat dipahami bahwa hubungan kerjasama Indonesia dan Amerika Serikat sudah dapat diprediksi atau sebuah kejadian yang memang seharusnya terjadi, alasan dari pernyataan ini adalah sesuatu yang dibahas di hampir setiap jurnal yang telah diteliti diatas yaitu kedua

negara sebagai demokrasi terbesar di dunia. Seperti yang dibahas dalam jurnal karya Agussalim Burhanuddin, Demokrasi bukan hanya ide yang cair dan terbuka, tetapi juga konsep yang pada dasarnya diperebutkan. Sejak ditemukan sebagai bentuk politik dan pemerintahan, konseptualisasi dan penerapan demokrasi tidak pernah mencapai kesepakatan universal. Amerika Serikat yang sering disebut sebagai negara demokrasi yang mapan dan mengklaim demokrasi sebagai salah satu prinsip politik luar negerinya, kerap menjadi sasaran kritik atas unilateralismenya. Di belahan dunia lain, Indonesia sering dikagumi karena demokratisasi jalur cepatnya yang berubah dari sistem otoriter menjadi demokrasi penuh dalam waktu yang relatif singkat. Namun, setelah hampir dua dekade transformasi di bawah semangat apa yang disebut reformasi, negara ini masih berjuang dengan demokratisasinya. Sebelum abad kedelapan belas, istilah 'demokrasi' umumnya dianggap sebagai 'pemerintah partisipatif langsung'. berdasarkan pengalaman negara-kota Yunani. Ketika sistem politik Amerika berkembang dan mengilhami banyak pemerintah yang baru dibentuk untuk mengadopsinya, 'demokrasi' telah digunakan sebagai label untuk 'pemerintah perwakilan yang dipilih' dan perwakilan telah menjadi mekanisme fundamental demokrasi modern yang dipelopori oleh sistem Amerika. Pada dasarnya sebagai kedua negara demokrasi terbesar, kedua negara diharapkan memiliki kepentingan dan misi negara yang sama sebagai pelopor demokrasi. Tentunya dengan ini diharapkan kedua negara dapat dengan mudah melakukan kerjasama dan dapat mengkapitalisasi hal tersebut. (Burhanuddin, 2017)

Dalam memahami ancaman yang dapat diberikan oleh cyberterrorism, penulis melakukan penelitian tentang Isu Cyberterrorism. Penulis meneliti jurnal karya Gabriel Weimann sebagai permulaan. Dalam jurnal tersebut dinyatakan bahwa potensi ancaman yang ditimbulkan oleh terorisme siber telah memicu kekhawatiran yang cukup besar. Banyak pakar keamanan, politisi, dan lainnya telah mempublikasikan bahaya peretasan cyberterrorist ke dalam sistem komputer pemerintah dan swasta dan melumpuhkan sektor militer, keuangan, dan layanan di negara maju. Kekuatan psikologis, politik, dan ekonomi telah bergabung untuk mempromosikan ketakutan akan terorisme siber. Dari perspektif psikologis, dua ketakutan terbesar zaman modern digabungkan dalam istilah “cyberterrorism”.

Ketakutan akan viktimisasi yang acak dan kejam berpadu dengan baik dengan ketidakpercayaan dan ketakutan langsung terhadap teknologi computer. Bahkan sebelum 9/11, sejumlah latihan mengidentifikasi kerentanan yang tampak di jaringan komputer sektor militer dan energi AS. Setelah 9/11, wacana keamanan dan terorisme segera menonjolkan terorisme siber, yang dipromosikan oleh aktor-aktor yang berkepentingan dari kalangan politik, bisnis, dan keamanan. Terorisme siber, tentu saja, merupakan pilihan yang menarik bagi teroris modern, yang menghargai anonimitasnya, potensinya untuk menimbulkan kerusakan besar, dampak psikologisnya, dan daya tarik medianya. Memerangi terorisme siber tidak hanya menjadi masalah yang sangat dipolitisasi, tetapi juga menjadi masalah yang menguntungkan secara ekonomi. Seluruh industri telah muncul untuk bergulat dengan ancaman terorisme siber: lembaga think tank telah meluncurkan proyek yang rumit dan mengeluarkan kertas putih yang mengkhawatirkan tentang masalah ini, para ahli telah bersaksi tentang bahaya terorisme siber di hadapan Kongres, dan perusahaan swasta dengan tergesa-gesa mengerahkan konsultan keamanan dan perangkat lunak yang dirancang untuk melindungi sasaran publik dan swasta. (Weimann, 2004)

Setelah memahami ancaman riil yang diberikan oleh cyberterrorism yang telah berdampak dalam segala level sosial dan telah menjadi ancaman yang sangat mengkhawatirkan masyarakat. Lewat jurnal karya Stein Schjolberg, Potensi ancaman serangan teroris di dunia maya akan terfokus pada sistem dan jaringan yang berisi infrastruktur informasi penting. Ini dapat mencakup tindakan terhadap kerahasiaan, integritas dan ketersediaan sistem dan jaringan tersebut melalui kejahatan dunia maya: akses ilegal, intersepsi ilegal, gangguan data, gangguan sistem, dan penyalahgunaan perangkat. Penghambatan serius terhadap fungsi sistem komputer dan jaringan infrastruktur informasi penting dari suatu Negara atau pemerintah akan menjadi target yang paling mungkin. Ketergantungan teknologi informasi dan komunikasi sekaligus menciptakan kerentanan yang menjadi tantangan bagi keamanan siber. Serangan terhadap infrastruktur informasi penting dapat menyebabkan gangguan menyeluruh dan merupakan ancaman signifikan yang mungkin memiliki konsekuensi paling serius bagi masyarakat. Target potensial dapat berupa sistem dan jaringan pemerintahan, jaringan telekomunikasi,

sistem navigasi untuk pelayaran dan lalu lintas udara, sistem kontrol air, sistem energi, dan sistem keuangan, atau fungsi lain yang sangat penting bagi masyarakat. Ini harus merupakan tindak pidana ketika teroris dapat menghalangi atau mengganggu berfungsinya dengan benar, atau mempengaruhi aktivitas sistem komputer, atau membuat sistem tidak beroperasi, mis. merusak sistem. Dengan demikian sistem komputer dapat ditutup untuk waktu yang singkat atau lama, atau sistem juga dapat memproses data komputer pada kecepatan yang lebih lambat, atau kehabisan memori, atau memproses secara tidak benar, atau menghilangkan pemrosesan yang benar. Tidak masalah apakah penghalang itu bersifat sementara atau permanen, atau sebagian atau seluruhnya. (Schjolberg, 2006)

Cyberterrorism merupakan suatu ancaman yang sangat beragam dan berkembang seiring zaman yang makin dibantu dengan perkembangan teknologi yang sangat massif. Wajib bagi sebuah negara untuk dapat menangani fenomena yang ada. Menurut Nadiah Khaeriah Kadir, Judhariksawan, dan Maskun, melalui jurnal yang mereka buat, Salah satu permasalahan cybercrime adalah kerusakan yang ditimbulkannya dan mendapat perhatian dari berbagai kalangan yang eskalasi menjadi cyber-terrorism. Keberadaan dunia maya yang mudah diakses melawan radikalisme mendorong cepatnya kinerja dari tujuan buruk tersebut dengan membuat platform. Penggunaan dunia maya oleh organisasi radikal seperti teroris menciptakan ancaman baru bagi forum internasional. Cyber-terrorism dapat dipahami sebagai konvergensi terorisme dan dunia maya. Dalam hal ini, ancaman atau serangan terhadap komputer di mana jaringan dan informasi yang tersimpan di dalamnya bertujuan untuk mengintimidasi pemerintah dan/atau masyarakat untuk tujuan politik atau sosial. Selain itu, untuk memenuhi syarat sebagai cyberterrorism, serangan harus menyebabkan kekerasan terhadap orang atau properti, atau setidaknya cukup berbahaya untuk menimbulkan ketakutan, seperti serangan yang menyebabkan kematian atau cedera tubuh, ledakan, atau kerugian ekonomi yang signifikan. Beberapa jaringan kelompok teroris secara tidak langsung diuntungkan dengan hadirnya produk teknologi berbasis internet yang dapat mencakup banyak aspek, mulai dari kepentingan propaganda, rekrutmen, hingga jejaring. Internet tidak hanya memudahkan teroris untuk berkomunikasi, mengatur sel teroris, berbagi informasi, merencanakan serangan, dan merekrut orang lain, tetapi juga

semakin sering digunakan sebagai alat untuk melakukan tindakan terorisme. Anggota organisasi teroris berbagi pengetahuan mereka melalui apa yang disebut percakapan online di mana teroris mendiskusikan berbagai masalah dan rencana untuk masa depan. Namun, situs-situs ini dilindungi oleh kata sandi, dan karenanya analis anti-terorisme seringkali tidak dapat mengakses dan memantau informasi. (Kadir, Judhariksawan, dan Maskun, 2019)

Setelah melakukan penelitian terhadap sembilan jurnal yang dinilai relavan dalam tujuan penelitian penulis kali ini, kesembilan jurnal sangat membantu penulis dalam merumuskan penelitian yang ingin dilakukan. Topik kerjasama Indonesia dan Amerika Serikat sudah banyak diteliti oleh berbagai penulis, sedangkan secara khususnya dalam masalah siber juga cukup banyak diteliti seperti beberapa jurnal yang telah dikutip diatas. Tetapi setalah melakukan kajian literatur terhadap kesembilan jurnal yang dinilai relevan, penulis menemukan celah dalam penelitian tersebut yaitu belum adanya penelitian mengenai **Implementasi Kerjasama Ruang Siber Antara Indonesia dan Amerika Serikat Dalam Meningkatan Kapasitas Penanganan Ancaman *Cyberterrorism* di Indonesia.**

1.2 Rumusan Masalah

Indonesia dan Amerika Serikat merupakan kedua negara yang mempunyai hubungan yang sarat dengan sejarah dan keberagaman kerjasama. Kedua negara telah melakukan kerjasama yang jika dilacak dalam sejarah bahkan terjadi disaat perang dingin. Dalam aspek keamaanan atau Terorisme, kedua negara telah melakukan kerja sama semenjak kemerdekaan Indonesia dengan program Pendidikan dan Pelatihan Militer Internasional (IMET). Walaupun mengalami banyak dinamika perubahan kebijakan dikarenakan kepentingan nasional yang berbeda, kerjasama kedua negara tetap diberlakukan hingga saat ini. Berbicara tentang isu keamanan atau lebih khususnya terorisme, kedua negara telah melakukan berbagai cara dalam melawan dan yang terbaru munculnya ancaman baru yang dipicu dari keberadaan ruang siber yaitu ancaman *Cyberterrorism*. Ancaman ini jika dilihat dari sejarah pertama menghebohkan dunia tidak lama setelah peristiwa 9/11 yang mengguncang seluruh negara.

Menyadari ancaman besar yang diberikan *Cyberterrorism*, Kedua negara melakukan berbagai hal untuk dapat melindungi diri mereka. Dengan terus berkembangnya teknologi dan pemakaian Internet, ancaman *Cyberterrorism* pun semakin beragam dan kompleks. Dalam hal penanganan tidak dapat dipungkiri Amerika jauh lebih sukses daripada Indonesia dan hal tersebut bukanlah suatu kejutan dikarenakan hal tersebut sudah selayaknya terjadi. Amerika Serikat dilihat dari sudut apapun merupakan negara yang lebih superior, termasuk dalam ruang siber. Memahami ini, keberadaan inisiasi kerjasama ruang siber antara Amerika Serikat dan Indonesia merupakan hal yang seharusnya menjadi jawaban dari permasalah keamanan siber yang dialami. Namun setelah penandatanganan kerjasama tersebut yaitu pada tahun 2018 sampai sekarang yaitu 2022 yang berarti kerjasama sudah terjalin selama 4 tahun. Melihat fakta yang terjadi selama 4 tahun tersebut, tidak ada perkembangan besar yang signifikan terjadi terhadap keamanan siber Indonesia yang seharusnya menjadi tujuan kerjasama. Kasus terbaru yang terjadi justru sangatlah memalukan dimana seorang *hacker* Brazil berhasil meretas website BSSN yaitu sebuah organisasi Indonesia yang seharusnya menjadi garda terdepan dalam pengamanan isu siber. Dengan ini berbagai hal yang telah disampaikan diatas penulis mengangkat pertanyaan yaitu **"Bagaimana Implementasi Kerjasama Ruang Siber Antara Indonesia dan Amerika Serikat Dalam Meningkatan Kapasitas Penanganan Ancaman *Cyberterrorism* di Indonesia?".**

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas dapat disimpulkan bahwa tujuan penelitian ini adalah untuk menganalisa apa yang telah diimplementasikan dalam Kerjasama Ruang Siber Antara Indonesia dan Amerika Serikat Dalam Peningkatan Kapasitas Penanganan Ancaman *Cyberterrorism*

1.4 Manfaat Penelitian

Manfaat-manfaat yang dapat diperoleh dari penelitian ini adalah :

1. Manfaat praktis penelitian ini diharapkan dapat digunakan untuk penelitian lebih lanjut terkait hubungan internasional dalam bidang keamanan atau terlebih khususnya lagi pada bidang *Cyberterrorism*

2. Secara akademis manfaat penelitian ini adalah untuk mengembangkan penelitian yang telah dilakukan sebelumnya serta untuk mencari perbedaan pada penelitian yang telah dilakukan sebelumnya. Dan hasil dari penelitian ini diharapkan dapat memberikan serta menambah wawasan dan berkontribusi bagi ilmu Hubungan Internasional bidang keamanan atau khususnya *Cyberterrorism*

1.5 Sistematika Penulisan

Untuk memahami alur pemikiran penelitian ini, maka tulisan ini dibagi dalam bagian-bagian yang terdiri dari bab dan sub-bab. Sistematika penulisan tersebut membagi hasil penelitian ke dalam V bab, yaitu

BAB I PENDAHULUAN

Pada bab ini akan menjelaskan latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian danpenelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini akan menjelaskan mengenai tinjauan pustaka, membandingkan penelitian ini dengan penelitian-penelitian serupa yang telah dilakukan sebelumnya, kerangka pemikiran, alur pemikiran dan hipotesis.

BAB III METODOLOGI PENELITIAN

Pada bab ini berisikan tentang metode penelitian yang penulis gunakan, bagaimana penulis meakukan penelitian beserta sumber data yang penulis gunakan untuk penelitian ini didapatkan.

BAB IV ANALISA KERJASAMA RUANG SIBER ANTARA INDONESIA DAN AMERIKA SERIKAT DALAM PENANGANAN CYBERTERRORISM

Pada bab ini penulis akan melakukan penelitian mengenai kerjasama ruang siber antara Indonesia dan Amerika yang sudah berlangsung sejak 2018 dalam penanganan Cyberterrorism.

BAB V PENUTUP

Pada bab ini akan berisikan mengenai kesimpulan dan saran dari penelitian yang penulis lakukan.