BAB I

PENDAHULUAN

1.1. Latar Belakang Penelitian

Cyberspace atau dunia maya semakin mendominasi kehidupan masyarakat di era modern ini. *Cyberspace* diartikan sebagai wilayah global dalam lingkungan informasi yang terdiri dari jaringan infrastruktur teknologi informasi yang saling bergantung, termasuk internet, jaringan telekomunikasi, serta prosesor dan sistem kendali komputer yang tertanam (Chen et al., 2023). Berbeda dengan Internet itu sendiri, *cyberspace* adalah ruang yang dihasilkan dari hubungan-hubungan tersebut. Istilah cyberspace pertama kali diperkenalkan oleh penulis Amerika-Kanada, William Gibson, pada tahun 1982 dalam sebuah cerita yang diterbitkan di majalah Omni dan kemudian dalam bukunya, Neuromancer (Bussell, n.d.). Dalam novel fiksi ilmiah tersebut, Gibson menggambarkan *cyberspace* sebagai jaringan komputer yang dihuni oleh entitas dengan kecerdasan buatan. *Cyberspace* muncul setelah berdirinya pertama kali jaringan komputer, yaitu ARPANET *(Advanced Research Projects Agency Network)*, tahun 1969, sebagai proyek militer Amerika Serikat yang tujuannya adalah untuk berbagi informasi dalam jarak jauh tanpa memerlukan koneksi telepon khusus antara setiap jaringan(Featherly, 2023). Dari sinilah, teknologi internet terus berkembang dan infranstruktur jaringan global mulai dibangun yang telah memungkinkan akses mudah ke informasi dan komunikasi dengan siapa saja diseluruh dunia.

Menurut Dysson, *cyberspace* adalah sebuah ekosistem bioelektronik yang mencakup semua tempat dengan telepon, kabel coaxial, serat optik, atau gelombang elektromagnetik. *Cyberspace* memiliki beberapa karakteristik utama (Arifin, 2021a):

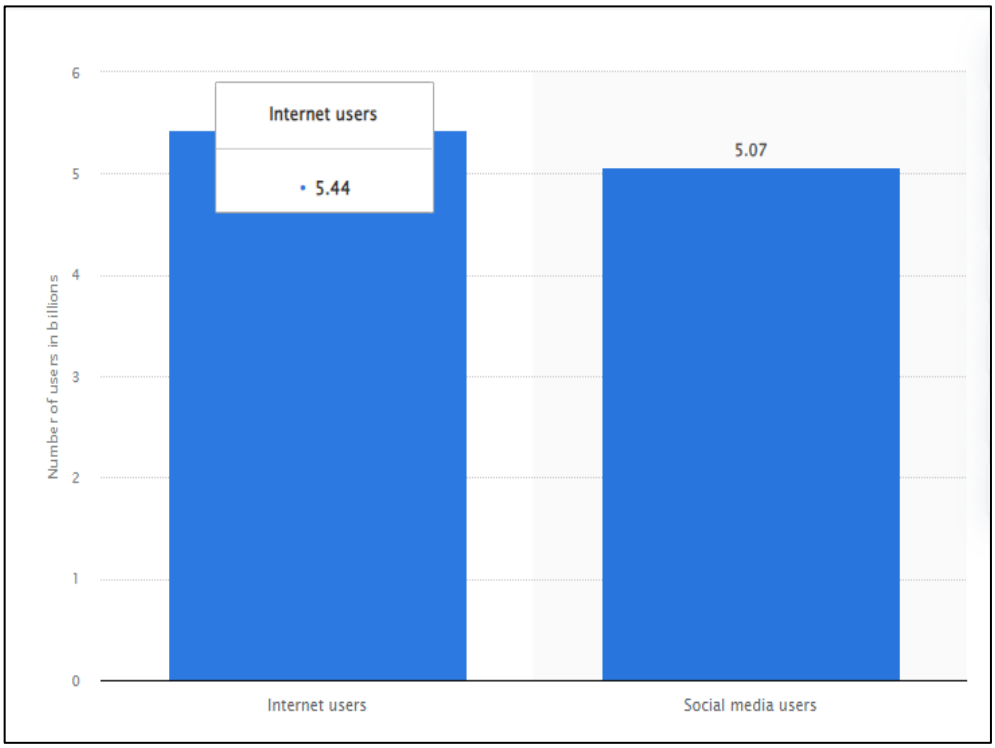
1. Beroperasi secara virtual. Cyberspace adalah dunia maya yang dihuni oleh orang-orang yang berinteraksi, berdiskusi, dan bertukar ide tanpa harus

bertemu secara fisik. Selain manusia, penghuni dunia maya juga mencakup data, informasi, surat elektronik, ide-ide, dan ilmu pengetahuan. Dunia maya dipenuhi oleh lalu lintas data dan informasi.

2. Selalu berubah dengan cepat. Dunia cyber berubah cepat karena interaksi dari hampir semua orang di seluruh dunia, didukung oleh kemudahan memperbarui data.
3. Tidak mengenal batas teritorial. Penghuni cyberspace berasal dari berbagai negara dan berinteraksi tanpa mengenal batas-batas teritorial.
4. Anonimitas dalam aktivitas. Orang-orang di dunia maya dapat melakukan aktivitas tanpa menunjukkan identitas asli mereka karena interaksi di cyberspace tidak melibatkan pertemuan fisik.
5. Informasi bersifat publik. Informasi di dalam cyberspace, termasuk hasil pemikiran intelektual, bersifat publik, tidak dimiliki oleh siapapun, dan dapat digunakan oleh siapa saja tanpa perlu otorisasi.

Cyberspace telah mencakup aspek-aspek kehidupan yang membawa manfaat besar, baik dalam ekonomi, sosial, budaya, dan keamanan. E-commerce adalah salah satu bukti aspek ekonomi digital bagaimana *cyberspace* telah mengubah sistem perdagangan, dari tradisional menjadi lebih modern dengan transaksi jual beli melalui online atau media elektronik. Kemudian, platform media sosial juga telah mempermudah cara interaksi dalam aspek sosial budaya. Dari contoh-contoh aspek tersebut, hal ini menggambarkan bagaimana *cyberspace* bukan lagi sesuatu yang terpisah dari kehidupan manusia. Berdasarkan platform data Statista, per Januari 2024, terdapat 5,35 miliar pengguna internet di seluruh dunia, yang merupakan 66,2 persen dari populasi global. Dari jumlah tersebut, 5,04 miliar, atau 62,3 persen dari populasi dunia, adalah pengguna media sosial (Petrosyan, 2024). Meskipun perkembangan ini membawa manfaat besar, tetapi tantangan dalam *cyberspace* juga semakin luas, yaitu dengan munculnya kejahatan siber *(Cyber Crime).*

Gambar 1.1 Data Pengguna Internet dan Media Sosial per Januari 2024 di Seluruh Dunia



Sumber: Data Statista, 2024

Kejahatan siber mengacu pada aktivitas melanggar hukum yang terutama menggunakan komputer dalam pelaksanaannya. Departemen Kehakiman Amerika Serikat memperluas cakupan kejahatan siber untuk mencakup aktivitas ilegal apa pun yang melibatkan penggunaan komputer untuk menyimpan bukti (Amit Kumar, 2022). Secara sederhana, kejahatan siber dapat digambarkan sebagai tindakan kriminal yang dilakukan dengan menggunakan komputer dan internet, dengan tujuan untuk mencuri identitas seseorang, menjual barang ilegal, melecehkan korban, atau menyebabkan gangguan berbahaya. Diperkirakan sekitar 2.328 kejahatan siber dilakukan setiap hari selama 21 tahun terakhir, dari tahun 2001 hingga 2021, kejahatan siber diperkirakan telah menyebabkan setidaknya 6,5 juta korban dan kerugian sekitar USD 26 miliar pada periode yang sama (Palatty, 2023).

Kejahatan siber *(cybercrime)* sebagai bentuk kejahatan transnasional yang kompleks dan sering kali melibatkan kelompok kejahatan terorganisir. Berikut poin-poin utama dari kejahatan siber (Sviatun et al., 2021):

a. Kejahatan Transnasional: Kejahatan dunia maya melibatkan pelaku dan korban yang berada di wilayah yang berbeda, dengan dampaknya yang bisa dirasakan di seluruh dunia. Hal ini memerlukan respons yang mendesak, dinamis, dan terintegrasi.
b. Tidak Ada Tempat Kejadian Perkara Tradisional: Menurut Maillart dan Brenner, kejahatan dunia maya tidak memiliki tempat kejadian perkara dalam pengertian tradisional, seperti bukti fisik, sidik jari, atau saksi.
c. Dampak Positif dan Negatif Teknologi Komputer: Renu & Pawan menyatakan bahwa teknologi komputer yang murah, kuat, dan mudah digunakan memiliki dampak positif terhadap perekonomian. Namun, kejahatan dunia maya dapat menyebabkan bisnis, perusahaan, dan lembaga pemerintah berhenti berfungsi.
d. Peningkatan Penggunaan Teknologi dan Ancaman Data: Penggunaan perangkat dan teknologi oleh masyarakat telah meningkat, begitu juga dengan aset data. Hal ini menciptakan ancaman dan peluang untuk penyalahgunaan data, meningkatkan potensi aktivitas kriminal menggunakan informasi digital.
e. Kategori Kejahatan Dunia Maya: Kejahatan dunia maya dibagi menjadi dua kategori:
   Jenis pertama: Sebagian besar bersifat teknologi.
   Jenis kedua: Memiliki unsur manusia yang lebih terlihat.

Terdapat beberapa aspek dalam kejahatan siber, mulai dari faktor aktivitas, ruang lingkup, serta jenis-jenis kejahatan siber berdasarkan motif dan sasaran (Arifin, 2021b):

1) **Dalam faktor aktivitas**, dapat dilihat dari dua dari sisi, yaitu sisi geografi dan sosial-ekonomi. Dari sisi geografi, teknologi internet dapat menghapus batasan wilayah negara, keterhubungan antara jaringan yang berbeda

mempermudah pelaku kejahatan dalam melakukan tindakannya. Sedangkan, dari sisi sosial-ekonomi, keberadaan kejahatan siber menciptakan nilai ekonomi. Aktivitas kejahatan di dunia maya berkaitan erat dengan keamanan jaringan, sehingga banyak pengguna yang sangat membutuhkan perangkat keamanan jaringan. Hal ini menjadikan kejahatan sebagai bagian dari kegiatan ekonomi global.

2) **Dalam ruang lingkup**, kejahatan siber menggunakan komputer dan perangkat lainnya sebagai objek penyalahgunaan dengan cara merubah, memodifikasi, dan menghapus data secara tidak sah.
3) **Dalam jenis-jenis kejahatan siber berdasarkan motif**, kejahatan siber sebagai kejahatan murni, dengan menggunakan internet sebagai sarana kejahatan, misalnya, kejahatan pencurian identitas, yaitu mencuri nomor kartu kredit orang lain untuk digunakan dalam transaksi internet. Kemudian, kejahatan siber sebagai kejahatan 'abu-abu'. Sulit untuk menentukan apakah kegiatan ini dianggap sebagai tindak pidana. Hal ini dikarenakan motif dari aktivitas tersebut belum tentu untuk melakukan kejahatan, misalnya, pemindaian port yang merupakan kegiatan mengumpulkan informasi tentang status port pada sistem orang lain.
4) **Dalam jenis-jenis kejahatan siber berdasarkan sasaran,** kejahatan siber menyerang individu, yaitu, kejahatan yang dilakukan terhadap seseorang atau beberapa orang dengan motif balas dendam atau tidak disengaja dan bertujuan untuk mencemarkan nama baik, contoh: pornografi, penguntitan siber *(cyberstalking),* perundungan siber *(cyberbullying)*, pelanggaran siber *(cyber trespass)*. Kemudian, kejahatan siber yang menyerang hak cipta (hak milik), kejahatan yang bertujuan untuk mendapatkan keuntungan materi atau non-materi, misalnya menggandakan uang. Kejahatan siber yang menyerang pemerintah, bertujuan untuk merusak keamanan institusi pemerintah atau menodai citra institusi pemerintah yang dimotivasi oleh tindakan spionase, terorisme, pembajakan atau subversi keamanan terhadap aset milik pemerintah.

Berdasarkan sasaran diatas, kejahatan siber diklasifikasikan menjadi serangan siber *(cyberattack)*, berikut beberapa jenis serangan siber yang umum (Jaikaran, 2023).

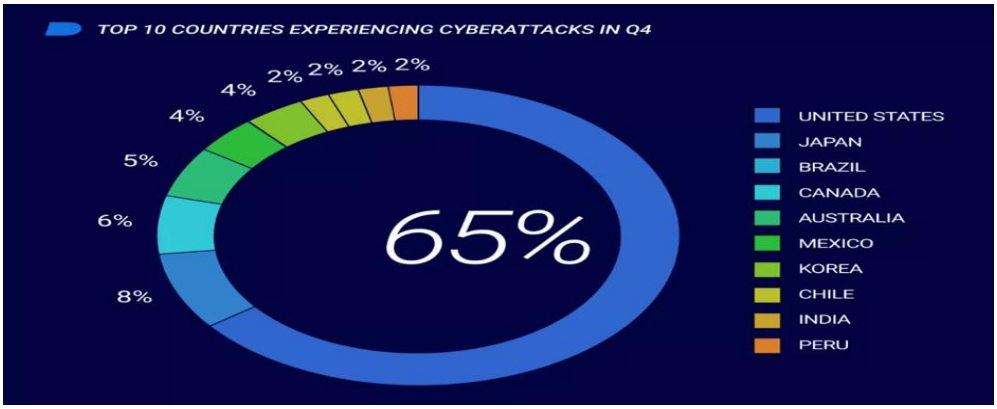
1) *Botnet*: Jaringan komputer yang dikendalikan oleh pihak yang tidak berwenang untuk melakukan aktivitas penipuan, seperti mendistribusikan *malware* atau menambang mata uang kripto.
2) Pelanggaran email bisnis: Pelaku penipuan yang sering membuat alamat email palsu yang menyamar sebagai pejabat tinggi untuk mengelabui organisasi agar mentransfer dana. Penipuan ini dapat mencakup faktur palsu dan menyebabkan kerugian finansial.
3) *Man-in-the-Middle (MitM)*: Seorang yang penyadapan antara dua komputer untuk mencegat dan mengakses komunikasi.
4) *Ransomware*: Penyerang mengenkripsi file dan sistem untuk mencegah pengguna mengakses data atau sistem IT. Penyerang biasanya meminta pembayaran, dalam mata uang kripto, untuk mengenkripsi sistem. Dalam beberapa kasus, penyerang mencuri data dan mengancam akan melepaskannya kecuali uang tebusan dibayarkan.
5) Serangan rantai pasokan: Memasukkan komponen jahat ke dalam produk untuk mengakses data atau memanipulasi sistem. Serangan ini dapat terjadi pada setiap tahap siklus hidup produk, seperti pengembangan atau pembaruan.
6) *Denial of Service (DOS)* atau *Distributed Denial of Service (DDOS)*: Serangan DOS atau serangan kegagalan layanan, membanjiri permintaan tidak sah ke sumber daya seperti situs web, membuatnya tidak dapat diakses oleh pengguna yang berwenang. Serangan DDOS melibatkan banyak host yang menyerang satu sumber daya.
7) Peretasan dan kebocoran: Pihak yang tidak berwenang dapat memperoleh akses ke data sensitif, mengekspos atau mempermalukan korban, atau meminta uang tebusan untuk mencegah kebocoran tersebut.
8) *Phishing*: Penyerang sering mengelabui pemerintah atau perusahaan agar terlibat dengan kode berbahaya melalui email penipuan yang berisi tautan

web dan lampiran berbahaya. Mengklik tautan ini atau membuka lampiran dapat menyebabkan infeksi malware.

9) *Malware*: Perangkat lunak berbahaya yang sengaja ditambahkan ke produk TI untuk menyebabkan kerusakan, seperti membahayakan kerahasiaan, integritas, atau ketersediaan data. Malware dapat mengganggu dengan berbagai cara, seperti mengunduh dari drive USB atau dari Internet.

Jenis serangan siber yang umum ini menyoroti beragam metode yang digunakan oleh pelaku kejahatan untuk mengeksploitasi kerentanan teknologi informasi dan komunikasi. Berdasarkan laporan intelijen ancaman dari Global BlackBerry per 1 September hingga 30 November 2022, tercatat sepuluh negara yang paling banyak menjadi korban serangan siber, Amerika Serika menempati posisi pertama sebagai negara yang paling banyak menjadi korban serangan siber (Sussman & Mok, 2023).

Gambar 1.2 The Top 10 Countries Most Targeted by Cyberattacks



Sumber: Laporan Intelijen Ancaman dari Global BlackBerry (2022)

Perkembangan teknologi yang begitu pesat, tidak sepenuhnya dimanfaatkan dengan baik oleh sebagian orang, serangan siber merupakan bukti bagaimana penyalahgunaan teknologi sangat berbahaya dan merugikan individu, masyarakat, perusahaan, bahkan mengancam keamanan nasional dan internasional, contoh kasus Ransomware WannaCry tahun 2017, yang menyebar secara global dengan cepat, WannaCry menginfeksi setidaknya 230.000 perangkat di 150 negara, dengan kerugian mencapai sekitar US$ 4 miliar Global (Diapoldo et al., 2022). Peristiwa

serangan siber telah menunjukkan bahwa kerentanan terhadap infrastruktur teknologi informasi dapat memiliki dampak besar tidak hanya pada tingkat nasional tetapi juga secara global.

Jenis kejahatan siber yang berbahaya juga adalah spionase siber yang disponsori oleh aktor negara yang memiliki tujuan untuk mengancam keamanan nasional suatu negara atau mencuri informasi rahasia suatu negara untuk mencari keuntungan. Persaingan global dapat mendorong negara-negara untuk bersaing dengan cara yang tidak sehat dan melakukan berbagai upaya untuk memperkuat diri mereka sendiri dengan melumpuhkan negara saingannya. Salah satu upaya yang dilakukan adalah melalui kegiatan spionase, yaitu memata-matai negara target untuk ditaklukkan (Dwi Hastri, 2021). Informasi dan data rahasia yang diperoleh dari spionase digunakan untuk mengetahui kelemahan negara tersebut sehingga mereka dapat dengan mudah merancang dan memperkuat strategi serangan. Untuk mendapatkan informasi rahasia dari negara yang menjadi target spionase, agen spionase harus memasuki wilayah terlarang dari negara tersebut. Di wilayah terlarang ini, agen mata-mata bertugas mengambil data dan informasi rahasia yang mencakup kelemahan dan kekuatan negara target. Namun, metode konvensional ini sudah tidak relevan lagi karena memakan waktu lama, informasi yang didapat terbatas, dan keberadaan agen spionase lebih mudah terdeteksi. Dengan memanfaatkan teknologi canggih dan percepatan digital, agen spionase kini dapat melakukan sabotase dan penyadapan dengan berbagai cara, yang melahirkan berbagai jenis kejahatan baru. Salah satunya adalah Spionase Siber atau spionase melalui dunia maya.

Berdasarkan buku pedoman keamanan siber, spionase siber dianggap sebagai ancaman atau motif, didefinisikan sebagai penggunaan jaringan komputer untuk mendapatkan akses terlarang ke informasi rahasia yang biasanya dimiliki oleh pemerintah atau organisasi lain (ENISA, 2020). Pada tahun 2019, banyak laporan mengungkapkan bahwa organisasi global menganggap spionase siber (atau spionase yang disponsori oleh negara) sebagai ancaman yang terus meningkat dan mempengaruhi sektor industri, serta infrastruktur penting dan strategis di seluruh dunia, termasuk kementerian pemerintah, perusahaan kereta api, penyedia layanan

telekomunikasi, perusahaan energi, rumah sakit, dan bank. Spionase siber berfokus pada mencuri rahasia negara dan perdagangan, hak kekayaan intelektual, serta informasi kepemilikan di bidang-bidang strategis. Hal ini juga memobilisasi para pelaku dari ekonomi, industri, dan badan intelijen asing, serta para pelaku yang bekerja atas nama mereka. Dalam sebuah laporan baru-baru ini, analis intelijen ancaman tidak terkejut mengetahui bahwa 71% organisasi memperlakukan spionase siber dan ancaman lainnya sebagai 'kotak hitam' dan masih mempelajarinya (ENISA, 2020). Kemudian, tercatat 86% dari seluruh serangan spionase dunia maya pada tahun 2020 dikaitkan dengan Tiongkok, salah satunya Amerika Serikat telah mendakwa lima peretas Tiongkok atas tuduhan spionase dunia maya terhadap 100 perusahaan Amerika (Lindner, 2023).

Ada banyak kasus spionase siber yang terjadi di berbagai negara. Berikut adalah beberapa contohnya, (Dewi, 2022):

1. Pencurian dan Penggunaan Akun Internet: Hal ini melibatkan pencurian atau penggunaan ID dan kata sandi orang lain secara tidak sah dengan cara mengambilnya saat digunakan di internet. Pencuri kemudian menggunakan akun yang dicuri, yang mengakibatkan tagihan ditagihkan kepada pengguna asli.
2. Pembajakan Situs Web: Sering dilakukan oleh cracker, aktivitas ini melibatkan pengubahan halaman web, yang dikenal sebagai defacement. Hal ini dapat dilakukan dengan mengeksploitasi kerentanan keamanan. Tidak seperti peretas, yang mungkin memiliki niat baik, cracker terlibat dalam aktivitas jahat seperti pencurian data, termasuk spoofing.
3. Probing dan Pemindaian Port: Sebelum mengakses server yang ditargetkan, cracker sering melakukan pengintaian dengan melakukan “pemindaian port” atau “probing” untuk mengidentifikasi layanan yang tersedia di server.

Pertumbuhan internet dan dunia siber tidak selalu mengarah pada hasil yang positif. Salah satu efek samping negatifnya adalah kejahatan dunia maya. Penghapusan batas-batas spasial dan temporal di internet telah mengubah banyak

aspek kehidupan. Sebagai contoh, seorang cracker di Rusia mampu mengakses server di Pentagon secara ilegal.

Sebelumnya, di era konservatif, aksi spionase atau aksi mata-mata dilakukan dengan melibatkan individu yang secara fisik melakukan perjalanan ke negara target atau organisasi tertentu untuk mendapatkan informasi, tetapi dengan berkembangnya teknologi dalam informasi dan komunikasi, metode spionase telah berubah, yang mengarah pada pengembangan spionase siber. Salah satu tantangan paling signifikan dalam melawan spionase siber adalah sulitnya atribusi (Wallace & Mccarthy, 2019). Sering kali sulit untuk mengidentifikasi sumber atau asal usul serangan operasi spionase siber yang sebenarnya karena penggunaan teknik yang canggih untuk menyembunyikan identitas pelaku. Selain itu, operasi siber dapat diluncurkan dari mana saja di seluruh dunia, sehingga sulit untuk melacak kembali ke lokasi tertentu. Tantangan atribusi ini menghambat respons dan pencegahan yang efektif terhadap spionase siber.

Berdasarkan karakteristik spionase siber terbagi menjadi tiga hal (Wallace & Mccarthy, 2019), yakni:

a. Jangkauan yang hampir tidak terbatas, karena operasi digital dapat diluncurkan dari mana saja dan menargetkan hampir semua tempat di dunia. Aksesibilitas global ini membuat spionase siber menjadi metode yang sangat menarik untuk memperoleh informasi.
b. Perkembangan "Internet of Things" dan masyarakat yang saling terhubung, spionase siber menimbulkan risiko yang luas terhadap infrastruktur manusia. Hal ini dapat menargetkan berbagai sektor, termasuk lembaga pemerintah, bisnis, dan individu, dan berpotensi mengganggu sistem penting.
c. Spionase siber sangat sulit untuk dilawan, meskipun ada langkah-langkah keamanan siber, dan perkembangan teknologi yang cepat, serta kemampuan untuk mengunduh informasi dalam jumlah besar dengan cepat mengakibatkan sulitnya untuk mencegah dan mengurangi efek spionase siber.

Oleh karena itu, dalam mencegah aksi spionase siber dan kejahatan siber lainnya, aspek keamanan harus diperkuat, yaitu, dalam keamanan siber *(Cyber Security*). Dalam keamanan siber, negara bertanggung jawab melindungi kepentingan nasional dan kesejahteraan masyarakatnya agar terhindar dari ancaman kejahatan siber (State, 2019).

Berdasarkan penjelasan *Cybersecurity Infrastructure Security Agency* (CISA), keamanan siber adalah upaya melindungi jaringan, perangkat, dan data dari akses atau penggunaan yang tidak sah atau berbahaya, serta tindakan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi (CISA, 2021). Dalam konteks keamanan siber tanggung jawab negara untuk melindungi warganya dari ancaman kejahatan siber menjadi semakin kritis. Salah satu pilar utama dalam menjaga keamanan siber negara adalah melalui upaya intelijen yang memiliki peran penting dalam identifikasi mengenai serangan siber, khususnya dalam serangan spionase siber. Sebagaimana diketahui, bahwa spionase siber melibatkan peretasan dan pengumpulan informasi dari entitas pemerintah, bisnis, atau individu yang memiliki ancaman serius bagi keamanan nasional dan privasi individu. Peranan intelijen negara menjadi sangat penting dalam mendeteksi mencegah dan merespon ancaman spionase siber. Selain itu, dalam meningkatkan kemampuan intelijen adalah adanya kerja sama internasional dalam bidang intelijen juga sangat penting untuk menanggapi serangan spionase siber yang bersifat lintas negara. Hal ini dikarenakan kerja sama intelijen internasional, negara-negara anggota dapat saling berbagi informasi intelijen, analisis, teknologi, keahlian, dan pelatihan antara badan-badan intelijen dari berbagai negara. Hal ini merupakan bentuk kemitraan negara-negara yang memanfaatkan kekuatan komparatif, seperti keunggulan geografis, politik, dan teknologi, untuk meningkatkan kemampuan intelijen dan menanggapi ancaman bersama secara lebih efektif (Harrington Jake & McCabe, 2022).

Terdapat banyak cara untuk mengumpulkan informasi rahasia intelijen: Sumber manusia, seperti mata-mata atau pembelot (HUMINT), fotografi atau sumber gambar (IMINT), atau komunikasi yang disadap atau sinyal elektronik (SIGINT). Kemampuan SIGINT telah berevolusi seiring dengan kemajuan teknologi, dari

kriptografi tangan ke kriptanalisis mekanis pada tahun 1930-an dan 1940-an, ke kriptanalisis berbantuan komputer pada tahun 1950-an, dan pengumpulan satelit pada tahun 1960-an. Transformasi SIGINT terbesar terjadi pada tahun 1990-an dengan adanya internet. Sinyal yang dikumpulkan diproses dan dianalisis untuk menghasilkan penilaian situasional, atau seperti yang disebutkan di atas, produk intelijen (Aldrich, 2021) .

Terdapat perbedaan antara dua jenis intelijen, yaitu SIGINT (Signal Intelligence) dan HUMINT (Human Intelligence), serta bagaimana masing-masing beroperasi dalam konteks kerja sama internasional, khususnya antara negara-negara di sisi Atlantik (transatlantik) (GIOE et al., 2021):

1. SIGINT dan Kerja sama Internasional

   SIGINT memiliki pendekatan yang sangat terintegrasi dan kolaboratif dalam hal berbagi informasi dan operasi bersama. Negara-negara yang terlibat dalam SIGINT saling berbagi beban kerja dan tugas intelijen. Contohnya, hubungan erat antara GCHQ (agen intelijen Inggris) dan NSA (agen intelijen Amerika) yang bahkan memiliki kantor penghubung di lantai eksekutif NSA, menunjukkan tingkat kolaborasi yang tinggi.
2. Humint dan Operasi Unilateral

   Humint, di sisi lain, cenderung bekerja secara unilateral atau sendiri-sendiri kecuali jika ada operasi tertentu yang dilakukan bersama. Ini menunjukkan bahwa dalam Humint, operasi biasanya dilakukan oleh satu negara tanpa banyak berbagi informasi atau koordinasi dengan negara lain, kecuali dalam ka operasi khusus.
3. Sejarah dan Filosofi Kerja sama

   Filosofi berbagi beban dan pekerjaan dalam SIGINT telah membentuk aliansi intelijen transatlantik selama bertahun-tahun. Proses evolusi kerja sama ini dari awal hingga menjadi jaringan kolaborasi yang erat dan intim merupakan bagian penting dari sejarah dan perkembangan operasi intelijen kontemporer serta potensi masa depannya.

Pendekatan antara SIGINT dan HUMINT dalam hal kerja sama internasional dan operasi intelijen, serta bagaimana hal ini telah mempengaruhi sejarah dan perkembangan aliansi intelijen transatlantik.

Tujuan kerja sama intelijen internasional adalah untuk memperluas akses terhadap sumber daya dan keahlian intelijen. Dengan bekerja sama, negara-negara dapat menggabungkan sumber daya mereka, memanfaatkan kekuatan satu sama lain dalam meningkatkan kemampuan intelijen, dan meningkatkan pemahaman tentang tantangan keamanan global (Harrington & Riley, 2022).

Salah satu contoh kerja sama intelijen internasional terkemuka adalah aliansi intelijen yang dikenal sebagai *Five Eyes* atau Five Eyes. *Five Eyes* adalah aliansi intelijen internasional yang terdiri dari badan-badan intelijen utama Australia, Kanada, Selandia Baru, Inggris, dan Amerika Serikat, yang dibentuk pada tahun 1946. Awalnya, aliansi ini tumbuh dari hubungan intelijen yang sukses antara Amerika Serikat dan Inggris selama perang dunia II, dan pada tahun 1946 kedua negara sepakat membuat persetujuan kerja sama yang dikenal dengan Perjanjian UKUSA, yaitu perjanjian pembagian intelijen antara Inggris dan Amerika Serikat dan berfokus pada operasi intelijen sinyal (SIGINT), kemudian berkembang selama dekade berikutnya, melalui serangkaian perjanjian yang menambahkan Kanada pada tahun 1948, Australia dan Selandia Baru pada tahun 1956 (Williams, 2023).

Adapun salah satu tanggung jawab setiap anggota aliansi Five Eyes adalah menganalisis intelijen di kawasan tertentu di dunia. Sebagaimana Inggris memantau Eropa, Rusia Barat, Timur Tengah, dan Hong Kong. Sementara itu, Amerika Serikat mengawasi Timur Tengah, ditambah dengan Cina, Rusia, Afrika, dan Karibia. Australia bertanggung jawab atas Asia Selatan dan Timur, kemudian Selandia Baru atas Pasifik Selatan dan Asia Tenggara. Kanada mengawasi wilayah pedalaman Rusia dan Cina serta sebagian Amerika Latin. Namun, terlepas dari pembagian ini, Five Eyes tetap bekerja secara kolaboratif dan saling membantu yang merupakan bagian penting dalam perjanjian ini (Tossini, 2020a). Five Eyes bukanlah entitas yang terorganisir secara terpusat, melainkan sebuah koalisi badan-badan intelijen independen yang terkait. Pada dasarnya organisasi intelijen sinyal (SIGINT), Five

Eyes tidak melakukan operasi rahasia, tetapi melengkapi kemampuan intelijen nasional masing-masing negara dengan cakupan yang luas dalam skala global (J, 2017).

Gambar 1.3 Mind Map Kerja Sama Five Eyes

Sumber: (Idal, 2022)

Kemitraan Five Eyes adalah sebuah aliansi berbagi intelijen yang kuat, terbentuk karena kesamaan tujuan diplomatik di antara negara-negara anggotanya. Para pemimpin badan intelijen dari masing- masing negara merasakan adanya hubungan yang erat dengan rekan-rekan mereka, dan militer mereka memiliki asumsi, tujuan, serta peralatan yang serupa. Dukungan politik untuk kemitraan ini sangat solid, yang dibuktikan oleh manfaat signifikan bagi semua anggotanya dan hubungan jangka panjang yang telah mengamankan aliansi ini, meskipun ada perselisihan politik yang serius.

Perekat utama dari aliansi Five Eyes adalah warisan peradaban yang sama di antara para anggotanya, yang mengukuhkan seperangkat nilai bersama. Nilai-nilai bersama ini memungkinkan kemitraan untuk bertahan dari perbedaan pendapat sementara mengenai isu-isu tertentu. Tanpa adanya kesamaan nilai ini, kepercayaan di antara para anggotanya akan mudah goyah. Selain itu, aliansi ini diuntungkan oleh berbagi informasi intelijen yang cepat dan efisien, yang memungkinkan setiap

negara anggota untuk meningkatkan keamanan nasionalnya. Kolaborasi yang intensif dalam berbagai operasi global juga memperkuat kemampuan Five Eyes dalam menghadapi ancaman keamanan yang kompleks dan beragam. Misalnya, berbagi data intelijen secara real-time telah membantu dalam mencegah serangan teroris, mengungkap jaringan kriminal internasional, dan menangani ancaman dunia maya. Kepercayaan yang dibangun melalui warisan bersama dan nilai-nilai yang sama ini memberikan dasar yang kuat untuk kerja sama berkelanjutan dan sukses di masa depan.

Selama tujuh dekade terakhir, Five Eyes telah memainkan peran penting dalam keamanan internasional, dengan saling berbagi informasi dan koordinasi yang erat antar negara anggota dalam melawan berbagai ancaman, termasuk terorisme, keamanan siber, proliferasi senjata, kejahatan terorganisir, serta spionase campur tangan yang didukung negara. Salah satu contoh Five Eyes memainkan perannya dalam kerangka anggota adalah pada tahun 2023 lalu, *The Five Eyes Law Enforcement Group (FELEG)*, yaitu kelompok penegak hukum Five Eyes, mengadakan pertemuan di Australia untuk berbagi intelijen, strategi dan hasil operasional untuk membantu menjaga negara Australia aman dari kriminalitas dan menjaga supremasi hukum (ACIC, 2023). FELEG adalah komunitas penegak hukum yang berkolaborasi dalam berbagi informasi intelijen. Pertemuan tahunan ini dihadiri oleh mitra FELEG yaitu FBI, U.S. *Drug Enforcement Administration* (DEA), *Australian Criminal Intelligence Commission* (ACIC), *Australian Federal Police* (AFP), *Royal Canadian Mounted Police* (RCMP), *U.K. National Crime Agency* (UK NCA), *U.K. Counter Terrorism Police* (UK CTP), dan Kepolisian Selandia Baru (ACIC, 2024).

Kebijakan keamanan siber dari masing-masing anggota Five Eyes (Inggris, Amerika Serikat, Kanada, Australia, dan Selandia Baru) dapat dianalisis berdasarkan beberapa aspek utama. Berikut adalah ringkasan kebijakan utama dari setiap negara berdasarkan dokumen yang diberikan (Renaud et al., 2020):

Tabel 1.1 Kebijakan Keamanan Siber Anggota Five Eyes

1. Inggris	- Dokumen Kebijakan: "HM Government 2016". - Fokus Kebijakan: Pemerintah Inggris menekankan pengawasan tindakan entitas (warga negara/industri) untuk memastikan mereka mengakui tanggung jawab mereka dalam keamanan siber.
2. Amerika Serikat	- Dokumen Kebijakan: "White House 2018". - Fokus Kebijakan: Pemerintah AS menugaskan tanggung jawab keamanan siber kepada pemangku kepentingan tertentu, seperti warga negara dan industri.
3. Kanada	- Dokumen Kebijakan: "Public Safety Canada 2018". - Fokus Kebijakan: Seperti AS, Kanada menugaskan tanggung jawab keamanan siber kepada pemangku kepentingan tertentu.
4. Australia	- Dokumen Kebijakan: "Australian Government 2016". - Fokus Kebijakan: Pemerintah Australia menugaskan tanggung jawab kepada warga negara dan industri.
5. Selandia Baru	- Dokumen Kebijakan: "New Zealand Government 2015, 2018". - Fokus Kebijakan: Selandia Baru

	juga menugaskan tanggung jawab kepada warga negara dan industri.

Berdasarkan situs web pemerintah Kanada, negara-negara mitra dalam perjanjian Five Eyes berbagi berbagai jenis intelijen dalam salah satu pengaturan multilateral yang paling erat di dunia. Perjanjian ini unik karena para pihak yang terlibat adalah masyarakat yang beragam, diatur oleh prinsip hukum dan hak asasi manusia yang kuat, serta menggunakan bahasa yang sama. Karakteristik ini memfasilitasi para mitra dalam berbagi informasi untuk melindungi kepentingan nasional mereka (TEAM, 2023).

Setiap tahun Five Eyes menyelenggarakan pertemuan guna memainkan peran penting dalam koordinasi dan kerja sama lintas batas. Pertemuan ini mencakup Ringkasan Eksekutif untuk Pertemuan Tahunan Dewan Pengawasan dan Peninjauan Intelijen Five Eyes atau *Five Eyes Intelligence Oversight and Review Council* (FIORC), pertemuan ini memberikan gambaran sekilas tentang diskusi yang diadakan oleh badan-badan pengawas intelijen dari negara-negara Five Eyes (FIORC, 2022). Kemudian Pertemuan Tingkat Menteri Lima Negara merupakan forum bagi para menteri keamanan Five Eyes untuk bertemu dan mendiskusikan peluang untuk berkerja sama. Topik-topik yang dibahas mencakup berbagai masalah keselamatan publik dan keamanan nasional yang dihadapi oleh masing-masing mitra Five Eyes (Canada.ca, 2023). Tidak semua kegiatan Five Eyes diselimuti kerahasiaan. Pada tahun 2019, perwakilan dari masing-masing badan intelijen Five Eyes naik ke panggung di konferensi tahunan *National Cyber Security Centre* (NCSC) Inggris, CYBERUK 2019, yang diadakan di Glasgow. Pada tahun 2020, badan-badan intelijen Five Eyes mempublikasikan upaya mereka dalam menanggapi serangan siber yang disponsori negara terhadap para peneliti yang mengembangkan vaksin Covid-19. Bahkan Five Eyes mengeluarkan panduan untuk menanggapi disinformasi yang disebarkan oleh aktor-aktor yang didukung negara yang berusaha mengacaukan upaya untuk menahan penyebaran virus (Mash, 2022).

Sementara itu, tidak hanya bekerja dalam kerangka negara anggota, tetapi Five Eyes juga bekerja sama dengan mitra internasional untuk menanggapi kejahatan transnasional yang semakin kompleks dan terhubung secara global. Salah satu contoh keterlibatan Five Eyes dalam keamanan internasional adalah keberhasilan Operasi Trojan Shield (2021), adalah operasi gabungan Five Eyes yang bekerja sama dengan berbagai lembaga seperti Kepolisian Federal Australia, FBI, dan Europol, operasi ini berhasil menangkap orang-orang yang terlibat dalam perdagangan narkoba di dunia maya (CND, 2023). Operasi ini menghasilkan penyitaan mata uang dan kripto senilai 148 juta, penyitaan berton-ton narkoba, senjata api, dan lebih dari 800 penangkapan di seluruh dunia, operasi menunjukkan keberhasilan dalam skala global (CND, 2023). Dengan menggabungkan sumber daya intelijen dari negara-negara anggotanya, Five Eyes dapat menciptakan efek jaringan yang kuat dalam upaya memberantas kegiatan kejahatan transnasional. Operasi seperti ini menggarisbawahi pentingnya kerja sama internasional dalam menghadapi tantangan keamanan yang melibatkan jaringan transnasional yang canggih dan terorganisir.

Kemudian pada masa pandemi COVID-19 tahun 2020, para menteri dari aliansi 'Five Eyes' melakukan kerja sama dalam menghadapi ancaman global yang meningkat akibat pandemi COVID-19. Pertemuan virtual ini dipimpin oleh Menteri Dalam Negeri Inggris, Priti Patel. Dalam pertemuan ini, menteri-menteri dari Australia, Kanada, Selandia Baru, Inggris, dan Amerika Serikat membahas berbagai ancaman seperti peningkatan risiko pelecehan seksual terhadap anak secara online, penyebaran disinformasi, dan aktivitas negara yang bermusuhan. Priti Patel menyatakan bahwa di masa yang belum pernah terjadi sebelumnya ini, kerja sama dengan sekutu dekat sangat penting untuk melindungi warga negara. Priti Patel senang bisa berdiskusi dengan rekan-rekan 'Five Eyes' tentang ancaman bersama dan cara mengatasinya. Para menteri membahas ancaman yang terus-menerus dari aktivitas negara yang bermusuhan dan penyebaran disinformasi selama pandemi yang dapat membahayakan nyawa. Mereka sepakat untuk berbagi praktik terbaik dan bekerja sama agar masyarakat bisa mendapatkan informasi yang dapat dipercaya.

Para menteri dari Five Eyes juga khawatir tentang meningkatnya risiko terhadap anak-anak di dunia maya selama pandemi. Five Eyes menyambut baik inisiatif baru dari Koalisi Teknologi untuk menangani pelecehan anak online. Namun, mereka menekankan bahwa perusahaan teknologi harus bertindak lebih cepat dan lebih jauh untuk melindungi anak-anak dari predator online. Para menteri menyoroti bahaya dari rencana enkripsi end-to-end oleh perusahaan seperti Facebook yang bisa meningkatkan pelecehan anak dan terorisme online. Para menteri setuju bahwa perusahaan teknologi harus bekerja sama dengan pemerintah untuk memastikan rencana tersebut tidak mengganggu upaya menjaga keamanan masyarakat. Selain itu, para menteri membahas penjahat dunia maya yang memanfaatkan pandemi melalui serangan ransomware, malware, dan phishing. Mereka sepakat untuk berbagi informasi intelijen tentang penipuan semacam ini dan bekerja sama untuk menghentikannya. Menteri-menteri yang hadir dalam pertemuan ini adalah:

- Menteri Dalam Negeri Inggris, Priti Patel (ketua bersama)
- Menteri Kehakiman Selandia Baru, Andrew Little (ketua bersama)
- Menteri Dalam Negeri Australia, Peter Dutton
- Menteri Keamanan Publik Kanada, Bill Blair
- Jaksa Agung AS, William Barr
- Penjabat Wakil Menteri Keamanan Dalam Negeri AS, Ken Cuccinelli

Selain itu, Five Eyes bekerja sama dengan berbagai negara 'Pihak Ketiga', seperti Denmark, Prancis, Norwegia, dan Belanda, yang bersama-sama dikenal sebagai 'Sembilan Mata'. Kemudian, ada 'Empat Belas Mata', yang terdiri dari negara-negara Sembilan Mata ditambah dengan Belgia, Jerman, Italia, Spanyol, dan Swedia. Nama resmi Empat Belas Mata adalah SIGINT Seniors Europe (SSEUR), dan tujuan utamanya adalah mengkoordinasikan pertukaran sinyal militer di antara anggotanya (Tossini, 2020b). Selain itu, banyak negara yang disebutkan tersebut juga memiliki hubungan kerja sama intelijen lainnya, terutama melalui Komite Khusus NATO yang mengumpulkan kepala-kepala badan keamanan dari negara-negara anggota NATO. Setelah lebih dari 70 tahun, Five Eyes dianggap sebagai "standar emas" dalam aliansi intelijen. Jangkauannya berkembang seiring dengan

teknologi baru dan masalah keamanan yang muncul dari teknologi tersebut, sehingga Five Eyes menyadari pentingnya dunia digital. Lawan-lawan Inggris dan Amerika Serikat juga menyadari hal ini, yang terlihat dari meningkatnya jumlah serangan siber.

Berikut adalah beberapa poin mengenai bagaimana aliansi Five Eyes merespons ancaman siber (IISS, 2021a).

a. Berbagi Intelijen: Five Eyes memfasilitasi pembagian informasi rahasia dan wawasan tentang ancaman siber di antara negara-negara anggotanya. Kolaborasi ini meningkatkan kesadaran situasional mereka dan memungkinkan pemahaman yang lebih komprehensif tentang ancaman siber.
b. Operasi Bersama: Negara-negara Five Eyes melakukan operasi siber bersama untuk melawan ancaman siber. Mereka memanfaatkan kemampuan siber kolektif dan kelincahan operasional mereka untuk merespons serangan siber dan mengganggu aktivitas jahat.
c. Kemampuan Siber Ofensif: Aliansi ini mengembangkan dan memanfaatkan kemampuan siber ofensif untuk menangkal dan melawan ancaman siber. Mereka melakukan operasi siber ofensif terhadap musuh untuk mengganggu aktivitas mereka dan memberikan konsekuensi.
d. Teknologi dan Inovasi: Aliansi Five Eyes berinvestasi dalam penelitian dan pengembangan teknologi canggih untuk meningkatkan kemampuan pertahanan siber mereka. Mereka terus beradaptasi dan berinovasi untuk mengimbangi ancaman siber yang terus berkembang serta mengembangkan alat dan teknik canggih.
e. Kerangka Kerja Kebijakan dan Hukum: Negara-negara anggota bekerja sama untuk mengembangkan kerangka kerja kebijakan dan hukum yang menangani ancaman siber. Mereka berkolaborasi dalam menetapkan norma dan standar untuk perilaku yang bertanggung jawab di dunia maya dan mengadvokasi kerja sama internasional dalam menanggapi ancaman dunia maya.

f. Keterlibatan Diplomatik: Aliansi Five Eyes terlibat dalam upaya diplomatik untuk menanggapi ancaman siber di tingkat internasional. Mereka berpartisipasi dalam forum internasional, terlibat dengan negara lain, dan mempromosikan kerja sama keamanan siber untuk menanggapi ancaman siber secara kolektif.
g. Kesadaran dan Transparansi Publik: Aliansi ini mengakui pentingnya kesadaran dan transparansi publik dalam mengelola ancaman siber. Upaya yang dilakukan untuk meningkatkan pemahaman publik tentang risiko siber, mempromosikan transparansi dalam berbagi informasi ancaman dengan industri dan publik, serta mendorong debat publik nasional dan internasional yang lebih terinformasi tentang keamanan siber.

Dalam era teknologi yang terus berkembang pesat, ancaman siber telah menjadi tantangan utama yang membutuhkan respons dinamis dan adaptif. Adaptasi Five Eyes dapat diartikan sebagai kemampuannya untuk menanggapi tantangan baru dan berubah sesuai dengan perkembangan teknologi dan lingkungan geopolitik. Five Eyes telah memainkan perannya dalam merespon dan beradaptasi dan bereaksi terhadap ancaman siber melalui pendekatan kolaboratif dan terkoordinasi.

Pembentukan Five Eyes sebagai aliansi intelijen telah menjadi pilar penting dalam keamanan nasional masing-masing negara anggota. Namun keberadaannya tidak lepas dari berbagai tantangan, salah satunya adalah ancaman spionase siber yang semakin merajalela. Berbagai pihak dari negara-negara lain seringkali melancarkan serangan siber terhadap anggota Five Eyes, hal ini seperti yang dialami oleh Amerika Serikat. Berdasarkan laporan terbaru oleh *Forescout Research*, lebih dari 420 juta serangan antara Januari dan Desember 2023. Tercatat, para pelaku ancaman telah melakukan kejahatan siber secara luas berdampak pada 163 negara. Amerika Serikat menjadi target utama, yang menanggung beban terbesar dengan adanya 168 aktor jahat yang mengincar negara tersebut. Negara lainnya termasuk Inggris (88), Jerman (77), India (72) dan Jepang (66). Sementara itu, negara-negara yang dicurigai biasanya memiliki konsentrasi aktor ancaman yang tinggi: Cina (155), Rusia (88) dan Iran (45), yang secara kolektif mewakili hampir setengah dari semua kelompok ancaman yang teridentifikasi. Sasaran

entitas jahat ini sebagian besar tertuju pada tiga sektor utama: pemerintah, layanan keuangan, serta media dan hiburan (Staff, 2024).

Adapun alasan Amerika Serikat menjadi target utama:

a. Kekuatan Ekonomi dan Teknologi

   Amerika Serikat adalah negara dengan ekonomi terbesar di dunia dan merupakan pemimpin global dalam teknologi. Hal ini menjadikan Amerika Serikat sebagai target yang menarik bagi aktor jahat siber yang ingin mencuri informasi rahasia atau melakukan sabotase untuk mendapatkan keuntungan ekonomi atau teknologi. Brdasarkan laporan CB Insight, tercatat Amerika Serikat merupakan negara dengan perekonomian terbesar di dunia, dengan Produk Domestik Bruto (PDB) lebih dari $25,5 triliun USD pada tahun 2022 (Calimanu, 2023). Kemudian di tahun 2021, dalam lima industri berbeda, Amerika Serikat dipandang sebagai pemimpin teknologi di dunia (Dyvik, 2023).

b. Keterbukaan Politik dan Media

   Amerika Serikat memiliki budaya politik dan media yang terbuka di mana informasi tentang serangan siber dapat dipublikasikan dengan mudah, hal ini karena Amerika Serikat memberikan kebebasan pers, berpendapat, serta hak mengajukan petisi yang diatur dalam Amandemen Pertama Konstitusi Amerika Serikat. Hal ini juga yang membuat Amerika Serikat terlihat lebih rentan terhadap serangan siber dibandingkan dengan budaya politik dan media yang lebih tertutup.

c. Posisi Amerika Serikat Dalam Geopolitik

   Amerika Serikat memainkan peran penting dalam geopolitik global dan sering terlibat dalam konflik dan perselisihan internasional. Hal ini menjadikan Amerika Serikat sebagai target utama bagi aktor jahat siber yang ingin melakukan spionase atau melumpuhkan infrastruktur penting. Sebagai contoh, Amerika Serikat memilki hubungan yang tegang dengan beberapa negara, salah satunya adalah Rusia yang telah terjadi sejak Perang Dunia II.

Kasus spionase siber telah menjadi ancaman serius bagi keamanan nasional di seluruh dunia, termasuk Amerika Serikat. Dua insiden besar yang mencuat adalah kasus SolarWinds (2020) dan Volt Typhoon (2023), yang tidak hanya menggemparkan dunia maya tetapi juga mengungkap kerentanan infrastruktur digital Amerika Serikat. Serangan ini menunjukkan betapa canggih dan terkoordinasinya upaya peretasan oleh pelaku yang diduga memiliki hubungan dengan pemerintah asing. Dampak dari kedua kasus ini tidak hanya dirasakan oleh Amerika Serikat, tetapi juga oleh sekutunya dalam aliansi intelijen Five Eyes, yang terdiri dari Amerika Serikat, Kanada, Inggris, Australia, dan Selandia Baru. Kanada adalah salah satu negara Five Eyes selain Amerika Serikat yang terkena dampak SolarWinds. Berdasarkan pernyataan dari Global Affairs Canada tentang kompromi siber SolarWinds, yang diadakan Ottawa, Ontario pada 21 April 2021. Menjelaskan bahwa Kanada bergabung dengan Amerika Serikat dan mitra internasional dalam menyuarakan keprihatinan terkait dengan kampanye spionase siber Rusia yang mengeksploitasi platform SolarWinds Orion. Setelah diketahui pada bulan Desember 2020 bahwa pelaku telah membahayakan jaringan ribuan pelanggan SolarWinds, termasuk lebih dari seratus entitas Kanada, dengan memasang malware melalui pembaruan program (Canada.ca, 2021).

Sementara itu, dalam kasus Volt Typhoon, Canadian Centre for Cyber Security (CCCS) menilai bahwa ancaman langsung terhadap infrastruktur penting Kanada yang dilakukan oleh Volt Typhoon kemungkinan besar lebih rendah daripada ancaman terhadap infrastruktur A.S., tetapi jika infrastruktur A.S. terganggu, Kanada kemungkinan besar akan terpengaruh juga, karena integrasi lintas batas yaitu hubungan erat antara infrastruktur penting Kanada dan Amerika Serikat yang berarti bahwa gangguan atau serangan terhadap faktor Amerika Serikat dapat berdampak langsung pada Kanada dan sebaliknya. Australian Cyber Security Centre (ACSC) dan New Zealand National Cyber Security Centre (NCSC-NZ) dari Australian Signals Directorate's (ASD) menilai bahwa infrastruktur penting Australia dan Selandia Baru, masing-masing, dapat menjadi rentan terhadap aktivitas serupa dari Volt Typhoon (CISA, 2024).

Dalam respons terhadap ancaman yang semakin kompleks ini, Amerika Serikat bekerja sama dengan negara-negara anggota Five Eyes, aliansi intelijen yang terdiri dari Amerika Serikat, Inggris, Kanada, Australia, dan Selandia Baru. Kerja sama internasional ini menjadi kunci dalam upaya mendeteksi, menganalisis, dan merespons ancaman siber yang semakin mengglobal, memastikan bahwa negara-negara ini dapat bertukar informasi intelijen dengan cepat dan efektif untuk melindungi kepentingan nasional mereka.

Tabel 1.2 Profil Insiden Serangan SolarWinds (2020)

Serangan SolarWinds (2020)	
Tanggal	Pada bulan November 2020, Fire Eye sebuah perusahaan profesional yang menyediakan layanan keamanan siber mengumumkan bahwa telah menemukan adanya serangan terhadap sistem mereka. Kemudian, Fire Eye memberitahu SolarWinds yang merupakan perusahaan pengembang perangkat jaringan lunak dan pengelola infrastruktur TI, tentang penggunaan yang tidak sah pada platform Orion mereka. Selain itu dengan bantuan Fire Eye, Microsoft juga mengungkap bahwa para penyerang berhasil meretas beberapa platform cloud microsoft. Serangan ini memungkinkan para penyerang untuk mendapatkan akses ilegal ke jaringan (D'Souza, 2021).
Aktor yang dicurigai	- Pada 15 April 2021, Inggris dan Amerika Serikat pertama kalinya mengungkapkan bahwa Badan Intelijen Luar Negeri Rusia (SVR) berada di balik serangkaian intrusi dunia maya, termasuk pembobolan SolarWinds (NCSC, 2021). - Dilansir dari CNBC, menurut Microsoft, dibalik serangan SolarWinds tahun 2020 adalah Nobelium, yaitu aktor yang disponsori oleh negara Rusia (CNBC, 2021)
Target	Solar Winds menjadi sasaran yang ideal dalam serangan rantai pasokan semacam ini karena aplikasi Orion (aplikasi memantau jaringan komputer) milik SolarWinds sering digunakan oleh sejumlah besar perusahaan besar dan entitas

	pemerintah. Para peretas hanya perlu menyisipkan kode berbahaya ke dalam pembaruan atau perbaikan perangkat lunak yang didistribusikan oleh SolarWinds untuk berhasil melancarkan serangan (Oladimeji & Kerner, 2023).
Sistem Sasaran	Platform SolarWinds Orion atau disebut "Sunburst"
Jenis Serangan	SolarWinds dan Microsoft mengkonfirmasi adanya tanda-tanda Malware yang mempengaruhi sistem pelanggan (CNBC, 2021).
Motif	Berdasarkan konfrensi pers gedung putih oleh Anne Neuberger, wakil penasihat keamanan nasional untuk teknologi siber dan teknologi Gedung Putih pada 17 Februari 2021. Pernyataan Anne terkait motif serangan " ketika kami melihat badan-badan tersebut, ada sejumlah badan yang memiliki kepentingan intelijen asing yang tinggi bagi pemerintah asing. Jadi kami tahu bahwa itu pasti salah satu tujuannya, tetapi seperti yang saya sebutkan sebelumnya, ketika ada kompromi dalam lingkup dan skala seperti ini, baik di seluruh pemerintahan maupun di seluruh sektor teknologi AS yang mengarah pada penyusupan lanjutan, ini lebih dari sekadar insiden spionase tunggal; ini pada dasarnya merupakan kekhawatiran akan kemampuannya untuk menjadi gangguan" (PRESS BRIEFINGS, 2021). Dapat dipahami berdasarkan pernyataan Anne Neuberger, bahwa motif dibalik pelaku serangan SolarWinds adalah ingin menargetkan badan intelijen asing dan pemerintah asing yang tujuannya adalah politik dan intelijen. Selain itu, Anne juga menjelaskan bahwa yang dilakukan oleh para pelaku lebih dari sekadar spionase melainkan sudah menjadi kekhawatiran pada tahap mengganggu.
Dampak	Malware ini mempengaruhi banyak perusahaan dan organisasi. Bahkan departemen pemerintah seperti Keamanan Dalam Negeri, Negara Bagian, Perdagangan, dan Departemen Keuangan juga terkena dampaknya, karena ada bukti bahwa email hilang dari sistem mereka. Perusahaan

	swasta seperti FireEye, Microsoft, Intel, Cisco, dan Deloitte juga mengalami serangan ini (Oladimeji & Kerner, 2023).

Sumber Dikelola Oleh Peneliti

Tabel 1.3 Profil Insiden Serangan Volt Typhoon (2023)

Serangan Volt Typhoon (2023)	
Tanggal	Pada bulan Mei 2023, analis keamanan Microsoft *(Microsoft Threat Intelligence)* menyatakan bahwa terdapat aktivitas berbahaya tersembunyi yang menargetkan sistem jaringan organisasi infrastruktur penting di Amerika Serikat (Microsoft, 2023).
Aktor yang dicurigai	Serangan tersebut dilakukan oleh Volt Typhoon, aktor yang disponsori oleh negara Tiongkok yang biasanya berfokus pada spionase dan pengumpulan informasi (Microsoft, 2023).
Target	Setelah diselidiki Volt Typhoon telah aktif sejak pertengahan tahun 2021 dan telah menargetkan organisasi infrastruktur penting di Guam dan tempat lain di Amerika Serikat (Microsoft, 2023).
Sistem Sasaran	Volt Typhoon menggunakan perangkat lunak berbahaya yang menembus sistem yang terhubung ke internet dengan mengeksploitasi kerentanan seperti kata sandi administrator yang lemah, login default pabrik, dan perangkat yang belum diperbarui secara berkala. Para peretas menargetkan sistem komunikasi, energi, transportasi, air dan air limbah di Amerika Serikat dan wilayahnya, seperti Guam (Forno, 2024).
Jenis Serangan	Dalam banyak hal, Volt Typhoon mirip dengan operator botnet tradisional yang telah mengganggu internet selama beberapa dekade. Dibutuhkan kendali atas perangkat internet yang rentan seperti router dan kamera keamanan

	untuk menyembunyikan dan membangun landasan sebelum menggunakan sistem tersebut untuk melancarkan serangan di masa depan (Forno, 2024)
Tujuan	Berdasarkan laporan Microsoft, kampanye Volt Typhoon ini sedang mengejar pengembangan kemampuan TI yang dapat mengganggu infrastruktur komunikasi penting antara Amerika Serikat dan kawasan Asia selama krisis di masa depan (Microsoft, 2023).
Dampak	Dilansir dari Microsoft, Volt Typhoon telah aktif sejak pertengahan tahun 2021 dan telah menargetkan organisasi infrastruktur penting di Guam dan tempat lain di Amerika Serikat. Dalam kampanye ini, organisasi yang terkena dampak, mencakup sektor komunikasi, manufaktur, utilitas, transportasi, konstruksi, maritim, pemerintahan, teknologi informasi, dan pendidikan (Microsoft, 2023). Salah satunya bidang maritim, Sekretaris Angkatan Laut Carlos Del Toro mengatakan kepada Morgan Brennan dari CNBC pada hari Kamis, 25 Mei 2023. Del Toro mengatakan bahwa Angkatan Laut AS "telah terkena dampak" dari serangan siber tersebut, dan menambahkan bahwa "tidak mengherankan jika China telah berperilaku seperti ini, tidak hanya dalam beberapa tahun terakhir, tetapi juga selama beberapa dekade." Del Toro menolak untuk memberikan rincian lebih lanjut tentang serangan siber tersebut, tetapi menyarankan bahwa Angkatan Laut telah menghadapi serangan siber seperti ini selama bertahun-tahun. Perilaku yang diamati menunjukkan bahwa aktor ancaman berniat melakukan spionase dan mempertahankan akses tanpa terdeteksi selama mungkin (Goswami, 2023).

Sumber Dikelola Oleh Peneliti

Kasus spionase siber di Amerika Serika, yaitu SolarWinds (2020) dan Volt Typhoon (2023) telah memicu respons yang kuat dari anggota Five Eyes, sebuah aliansi intelijen yang terdiri dari Amerika Serikat, Kanada, Inggris Raya, Australia,

dan Selandia Baru. Para anggota Five Eyes memandang serius insiden siber karena hal itu tidak hanya mengancam keamanan nasional masing-masing negara, tetapi juga kepentingan bersama. Five Eyes menyadari bahwa ancaman siber tidak mengenal batas negara dan dapat berdampak luas terhadap infrastruktur kritis, ekonomi, dan stabilitas global, sehingga menuntut tanggapan kolaboratif dan koordinasi yang kuat di antara mereka.

Sebagaimana yang dijelaskan dalam *f*orum Pertemuan Tingkat Menteri Lima Negara atau *Five Country Ministerial Communiqué* yang diadakan secara langsung dibawah kepemimpinan Kanada dan Selandia Baru pada tanggal 27-28 Juni 2023 oleh Menteri Dalam Negeri, Dalam Negeri, Keamanan, dan Imigrasi Australia, Kanada, Selandia Baru, Inggris, dan Amerika Serikat ('Lima Negara'). Five Eyes bersatu dalam komitmen untuk mempromosikan nilai-nilai bersama, dan bekerja secara kolaboratif dalam menangani keamanan nasional dan tanah air, serta tantangan migrasi. Dalam salah satu isu yang dibahas dalam forum tersebut, yaitu tentang keamanan siber, dikatakan bahwa "aktivitas dunia maya yang berbahaya dapat digunakan oleh negara, aktor jahat yang berafiliasi, dan peretas pada saat konflik meningkat. Kami bersatu dalam membangun strategi keamanan siber yang jelas dan saling melengkapi untuk memenuhi tujuan bersama kami, akan terus berbagi informasi untuk memastikan perlindungan yang kuat bagi infrastruktur nasional kami, dan secara kolektif akan memerangi peningkatan ancaman kejahatan siber dan aktor jahat yang ditimbulkan oleh komunitas kami" (Canada.ca, 2023a). Berikut alasan bahwa serangan spionase siber di Amerika Serikat adalah kepentingan dan perlu adanya persatuan dalam melawan serangan spionase siber di Amerika Serikat:

1. Hubungan Kemitraan Intelijen yang Kuat
    a. Sejarah: Terdapat kesepakatan kerja sama yang telah terjalin selama bertahun-tahun sejak perang dunia II yang tertulis dalam UKUSA Agreement 1946.
    b. Pertukaran intelijen: Five Eyes terkenal karena pertukaran Informasi intelijen yang luas. Dalam konteks spionase siber, berbagi intelijen antara Amerika Serikat dan mitra-mitra Five Eyes dapat meningkatkan

kemampuan mereka untuk mendeteksi, mencegah, dan merespons serangan siber secara efektif. Hal ini sesuai dengan UKUSA Agreement tahun 1946, 'para pihak menyetujui pertukaran produk dari operasi berikut yang berkaitan dengan komunikasi asing: pengumpulan lalu lintas, akuisisi dokumen dan peralatan komunikasi, analisis lalu lintas, kriptanalisis, dekripsi, dan terjemahan, akuisisi informasi mengenai organisasi, praktik, prosedur, dan peralatan komunikasi' (NSA, n.d.).

2. Kesadaran Akan Ancaman Bersama

Gambar 1.4 Pertemuan Five Eyes Summit

Dari kiri ke kanan: Direktur Jenderal Organisasi Intelijen Keamanan Australia Mike Burgess, Direktur Badan Intelijen Keamanan Kanada David Vigneault, Direktur FBI Christopher Wray, Direktur Jenderal dan Kepala Eksekutif Badan Intelijen Keamanan Selandia Baru Andrew Hampton, dan Direktur Jenderal MI5 Ken McCallum berpose untuk foto bersama dalam acara KTT Teknologi Berkembang dan Inovasi Pengamanan di Palo Alto, California, pada tanggal 16 Oktober 2023.

Sumber: (FBI, 2023)

a. Keamanan Global: Ancaman spionase siber tidak mengenal batas negara. Dalam menghadapinya, Amerika Serikat dan negara-negara anggota Five Eyes memiliki kepentingan bersama untuk memastikan keamanan digital secara global. Dalam KTT Five Eyes yang diselenggarakan oleh FBI pada 16 Oktober 2023, Direktur Jenderal Organisasi Intelijen Keamanan Australia, Mike Burgess,

mengatakan bahwa tujuan Five Eyes berkumpul dalam KTT tersebut adalah untuk merespons ancaman, dan membantu sektor teknologi untuk memahami, mengidentifikasi, dan mengelola risikonya, serta bertekad secara kolektif untuk melawannya (FBI, 2023).

b. Dukungan Teknis dan Teknologi: Anggota Five Eyes seringkali saling memberikan dukungan teknis dan teknologi dalam menanggapi ancaman siber. Jika suatu negara mengalami serangan atau membutuhkan bantuan dalam mengidentifikasi atau menanggapi serangan siber, negara-negara lain dalam aliansi dapat menyediakan bantuan ahli, sumber daya teknis, atau akses ke teknologi canggih untuk membantu menyelesaikan masalah tersebut. Direktur Jenderal Keamanan dan Kepala Eksekutif, Badan Intelijen Keamanan Selandia Baru Andrew Hampton: "Teknologi yang berkembang membawa banyak manfaat bagi Selandia Baru, termasuk potensi untuk mendorong pertumbuhan ekonomi. Pada saat yang sama, teknologi yang sama ini jika berada di tangan yang salah dapat menjadi salah digunakan dengan cara yang berbahaya atau terlarang. NZSIS senang dapat bekerja sama dengan mitra intelijen Five Eyes kami bersama dengan sektor swasta dalam menanggapi tantangan paling kritis ini (FBI, 2023).

Menteri Pertahanan Australia, pada 22-23 Juni 2020, menteri pertahanan dari negara-negara Five Eyes melakukan konfrensi video atau zoom. Dalam konfrensi tersebut dikatakan bahwa para menteri menegaskan kembali komitmen mereka untuk memajukan kerja sama pertahanan dan keamanan dalam hal-hal yang menjadi kepentingan bersama untuk mendukung dan mempertahankan tatanan global yang stabil dan berbasis aturan, yang semakin banyak ditantang. Para menteri mengakui peran mitra dan lembaga regional dalam membentuk komunitas yang stabil dan aman, serta tangguh secara ekonomi secara global dan di seluruh Indo-Pasifik, di mana hak-hak kedaulatan semua negara dihormati. Para menteri membahas peluang baru bagi mitra Five Eyes untuk lebih memperkuat hubungan

mereka, membangun ketahanan, menanggapi tantangan terhadap aturan dan norma internasional, dan memajukan kerja sama di berbagai bidang upaya dalam lingkungan (Ministers, 2020).

Serangan spionase siber di Amerika Serikat telah menjadi tantangan serius bagi keamanan nasional dalam beberapa tahun terakhir. Negara ini telah menjadi sasaran berbagai jenis serangan yang dilakukan oleh pihak yang tidak bertanggung jawab. Serangan ini tidak hanya menyebabkan kerugian finansial tapi juga memberikan dampak serius terhadap keamanan nasional dan keamanan internasional karena Amerika Serikat adalah salah satu anggota Five Eyes. Amerika Serikat menghadapi tantangan besar dalam menjaga keamanan siber negaranya, ancaman spionase siber yang lintas batas dan semakin kompleks menuntut respon yang lebih kolaboratif. Oleh karena itu, Amerika Serikat bersama Five Eyes terus meningkatkan kerja sama dalam bidang keamanan siber. Dengan meningkatnya interkoneksi dunia digital, upaya bersama ini diharapkan dapat menciptakan lingkungan yang lebih aman dan tangguh secara global. Sementara itu, kerja sama ini bukan hanya sebuah strategi melainkan sebuah suatu kebutuhan mendesak untuk menanggapi ancaman siber yang dapat merusak infrastruktur kritis, merugikan perekonomian, dan mengancam keamanan nasional.

Berikut beberapa alasan Amerika Serikat membutuhkan kerja sama dengan aliansi intelijen Five Eyes dan negara-negara lain dalam menanggapi ancaman siber (IISS, 2021b):

a. Ancaman siber yang bersifat transnasional, dan tidak ada satu negara pun yang dapat menanggapinya secara efektif sendirian. Dengan bekerja sama, Amerika Serikat dapat berbagi intelijen, keahlian, dan sumber daya untuk meningkatkan kemampuan pertahanan sibernya. Kedua,
b. Aliansi Five Eyes, yang terdiri dari Amerika Serikat, Inggris, Kanada, Australia, dan Selandia Baru, memiliki sejarah panjang dalam hal pembagian intelijen dan kerja sama. Aliansi ini memungkinkan pemahaman yang lebih dalam tentang ancaman siber dan memfasilitasi upaya bersama dalam mendeteksi, mengaitkan, dan melawan serangan siber.

c. Ancaman siber sering kali menargetkan infrastruktur penting, sistem pemerintah, dan entitas sektor swasta yang beroperasi secara global. Dengan bekerja sama, Amerika Serikat dapat memperkuat kemampuan pertahanan dan respons kolektifnya, memastikan pendekatan yang lebih komprehensif dan terkoordinasi terhadap keamanan siber. Selain itu, kerja sama internasional membantu menetapkan norma dan standar di *cyberspace.* Melalui upaya diplomatik dan keterlibatan multilateral, Amerika Serikat dapat bekerja sama dengan negara lain untuk mengembangkan aturan dan prinsip umum untuk perilaku yang bertanggung jawab di dunia maya, menghalangi aktor jahat dan mempromosikan stabilitas.

Berdasarkan penjelasan diatas, dapat dipahami bahwa Amerika Serikat membutuhkan kerja sama dengan aliansi Five Eyes dan negara-negara lain untuk secara efektif menanggapi ancaman kejahatan siber, terutama spionase siber yang sifatnya transnasional dari ancaman ini, perlunya berbagi intelijen dan upaya bersama, jangkauan global serangan dunia maya, dan pembentukan norma atau standar internasional.

Maka berdasarkan latar belakang serta permasalahan yang telah dipaparkan, penulis mengangkat fenomena ini menjadi sebuah penelitian yang berjudul **KERJA SAMA INTELIJEN INTERNASIONAL FIVE EYES DALAM MENANGGAPI SERANGAN SPIONASE SIBER: STUDI KASUS DI AMERIKA SERIKAT**

1.2.Perumusan Masalah

Mengacu pada latar belakang dan identifikasi masalah yang sudah dipaparkan sebelumnya, maka peneliti merumuskan masalah penelitian sebagai berikut:

“Bagaimana Strategi Kerja Sama Five Eyes Dalam Menanggapi Serangan Spionase Siber yang terjadi di Amerika Serikat?”

1.3.Pembatasan Masalah

Berdasarkan rumusan masalah yang sudah peneliti paparkan, dalam penelitian ini terdapat keterbatasan sumber daya, waktu, dan aksebilitas yang dapat

mempengaruhi rentan analisis penulis. Dalam hal ini penulis memilih untuk membatasi fokus penelitian pada studi kasus di Amerika Serikat agar lebih meneliti secara mendalam dan menyeluruh. Kemudian penelitian ini akan berfokus pada dua studi kasus spionase siber di Amerika Serikat, yaitu SolarWinds (2020) dan Volt Typhoon (2023). Tujuan pembatasan masalah ini adalah mempermudah penulis untuk memfokuskan dan mengarahkan penelitian ke arah yang lebih spesifik dan terarah.

1.4. Tujuan dan Kegunaan Penelitian

1.4.1. Tujuan Penelitian

Berdasarkan latar belakang penelitian dan rumusan masalah yang telah dipaparkan sebelumnya, maka tujuan dari penelitian ini sebagai berikut:

1. Untuk mengetahui identifikasi terhadap pelaku dibalik serangan spionase siber di Amerika Serikat.
2. Untuk mengetahui strategi pencegahan siber yang dilakukan Five Eyes dalam menanggapi serangan spionase siber di Amerika Serikat.
3. Untuk mengetahui tantangan yang dihadapi dalam implementasi kerja sama intelijen internasional Five Eyes.

1.4.2. Kegunaan Penelitian

Berdasarkan latar belakang penelitian dan rumusan masalah yang telah dipaparkan sebelumnya, maka tujuan dari penelitian ini sebagai berikut:

1. Memberikan pemahaman yang lebih mendalam tentang aliansi intelijen internasional dalam menghadapi ancaman spionase siber.
2. Meningkatkan kesadaran masyarakat dan pemerintah terhadap pentingnya kerja sama internasional dalam menghadapi serangan spionase siber dan mendorong langkah-langkah proaktif untuk melindungi keamanan siber.
3. Menyajikan rekomendasi kebijakan untuk penguatan kerja sama internasional dalam menanggapi serangan spionase siber dan meningkatkan keamanan siber nasional.
4. Menambahkan kontribusi baru pada literatur mengenai keamanan siber dan kerja sama intelijen internasional, terutama dalam konteks Five Eye