BAB II

TINJAUAN PUSTAKA

2.1. Tinjauan Literatur

No	Judul	Penulis	Persamaan	Perbedaan
1	Governing the European Intelligence: Multilateral Intelligence Cooperation in the European Union (2021)	Ahmet ATEŞ dan Anıl Çağlar ERKAN.	Membahas kerja sama intelijen multirateral.	Literartur ini berfokus pada dinamika, tata kelola, dan perhatian akademis terhadap kerja sama intelijen di Uni Eropa.
2	The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement (2021)	Peter R.J. Trim dan Yang-Im Lee	Membahas pentingnya kerja sama internasional dalam menanggulangi ancaman keamanan cyber.	Literatur ini membahas mengenai penggunaan AI dalam kemanan siber.
3	Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security Framework (2018)	Rudy Agus Gemilang Gultom, Asep Adang Supriyadi, Tatan Kustana	Kedua literartur membahas fokus isu keamanan siber dan kejahatan siber, serta pentingnya menanggapi ancaman siber tersebut.	Literatur ini berfokus tentang bagaimana cara menanggapi terorisme siber.

No	Judul	Penulis	Persamaan	Perbedaan
4	"Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China" (2020)	Merrill Warkentin P. Edward French	Kedua literatur membahas fokus tanggung jawab negara terkait keamanan siber dan melindungi warga negara dari ancaman siber.	Literatur ini memiliki cakupan yang lebih luas, membahas konsep keamanan siber, kerangka kerja teoretis, dan tanggung jawab secara umum
5	The Social Ties that Bind: Unraveling the Role of Trust in International Intelligence Cooperation (2023)	Pepijn Tuinier, Thijs Brocades Zaalberg & Sebastiaan Rietjens	Kedua literatur membahas bahwa pentingnya kerja sama intelijen internasional dalam menanggapi tantangan dan ancaman.	Literatur ini lebih spesifik mengkaji pentingnya kepercayaan dalam membina kerja sama yang efektif di antara badan-badan intelijen internasional.
6	The Phantom Eye: New Zealand and the Five Eyes (2023)	John Battersby & Rhys Ball	Kedua literarur membahas sejarah awal berdirinya Five Eyes dan tujuan negara-negara Five Eyes dalam meningkatkan keamanan.	Literatur ini berfokus pada partisipasi Selandia baru sebagai anggota Five Eyes.

Adapun literatur pertama sebagai pembanding yaitu jurnal yang ditulis oleh Ahmet ATEŞ dan Anıl Çağlar ERKAN pada tahun 2021, dengan judul penelitian

"Governing the European Intelligence: Multilateral Intelligence Cooperation in the European Union" (ATEŞ & ERKAN, 2021). Teori penelitian yang digunakan adalah Liberal Governmentality dan Teori Perdamaian Demokratis. Liberal Governmentality yang digunakan untuk menganalisa dan menjelaskan keberhasilan relatif pemerintahan intelijen Eropa dan kerja sama intelijen di Uni Eropa. Teori Perdamaian Demokratis, yang menyatakan bahwa negara-negara demokrasi liberal enggan untuk terlibat dalam kerja sama intelijen multilateral dengan rezim otoriter. Tujuan penelitian adalah untuk menganalisa dan memahami dinamika dan tata kelola kerja sama intelijen di Uni Eropa (UE), serta mengeksplorasi evolusi kerja sama intelijen, hambatan dan faktor-faktor yang mempengaruhinya, dan keberhasilan relatif kerja sama intelijen di Uni Eropa. Adapun perbedaan dalam penelitian adalah berfokus pada dinamika, tata kelola, dan perhatian akademis terhadap kerja sama intelijen di Uni Eropa. Adapun persamaan penelitian ini dengan penelitian penulis adalah membahas kerja sama intelijen multirateral.

Literatur kedua ditulis oleh Peter R.J. Trim dan Yang-Im Lee. Pada tahun 2021, dengan judul penelitian **"The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement"** (Trim & Lee, 2021).Penelitian ini membahas penggunaan berbagai teori dan model dalam konteks keamanan siber yang digunakan untuk memahami dan menangani berbagai aspek keamanan siber, termasuk penilaian risiko, kesadaran keamanan, pengembangan kemitraan, dan kerentanan organisasi. Metode penelitian ini menggunakan desain penelitian kualitatif, yang melibatkan wawancara kelompok dengan para ahli keamanan siber dan intelijen senior. Tujuan penelitian ini adalah untuk memberikan wawasan tentang pengembangan strategi keamanan siber yang komprehensif, dengan fokus pada pemahaman proses berpikir para ahli keamanan siber dan intelijen. Adapun perbedaan penelitian ini adalah Literatur ini membahas mengenai penggunaan AI dalam kemanan siber. Adapun persamaan penelitian ini adalah membahas pentingnya kerja sama internasional dalam menanggulangi ancaman keamanan cyber.

Literatur ketiga ditulis oleh Rudy Agus Gemilang Gultom, Asep Adang Supriyadi, Tatan Kustana. Pada tahun 2018, dengan judul penelitian **"Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security Framework"** (Gultom et al., 2018). Konsep penelitian ini berfokus pada proposal Six-Ware Cyber Security Framework (SWCSF), yang merupakan konsep komprehensif untuk solusi keamanan siber dalam meningkatkan ketahanan keamanan jaringan negara-negara ASEAN. Penelitian ini bertujuan untuk menyatukan visi negara-negara ASEAN dalam melawan kegiatan terorisme siber dan merekomendasikan langkah-langkah strategis seperti membentuk Strategi dan Kebijakan Keamanan Siber ASEAN, menciptakan Forum Keamanan Siber untuk berbagi informasi, dan mengembangkan Pusat Komando dan Kontrol Siber ASEAN. Adapun perbedaan penelitian ini adalah berfokus tentang bagaimana cara menanggapi terorisme siber. Adapun persamaan penelitian ini adalah membahas fokus isu keamanan siber dan kejahatan siber, serta pentingnya menanggapi ancaman siber tersebut.

Literatur keempat ditulis oleh Merrill Warkentin P. Edward French. Pada tahun 2020, dengan judul penelitian **"Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China"** Literatur ini menjelaskan analisis kebijakan strategi keamanan siber dari beberapa pemerintah, dengan fokus pada sejauh mana tanggung jawab keamanan siber bagi setiap warga negara. Literatur ini menggunakan beberapa teori dan metodologi untuk menganalisis tanggung jawab keamanan siber dan pengembangan kebijakan. Hal ini termasuk, ***Problematization*** fokus pada cara pembagian tanggung jawab di arena keamanan siber, ***Cyber Power*** sebagai model kontekstual yang berakar pada kebutuhan pragmatis untuk melindungi teknologi dan aset telekomunikasi dari risiko siber global, ***Governance Constructs*** membahas konstruksi tata kelola dalam konteks pengembangan kebijakan keamanan siber, ***Responsibilization Analysis*** bertujuan untuk mengungkap asumsi dan konseptualisasi implisit yang mendasari tanggung jawab yang diberikan kepada pemangku kepentingan yang berbeda dalam mengelola

risiko siber. Tujuan dari literatur ini adalah pengungkapan perbedaan antara kebijakan Tiongkok dan negara-negara neoliberal Five Eyes, dan untuk memahami bagaimana negara-negara ini mengusulkan untuk mendukung warganya dalam melawan serangan siber dan menjadi tangguh di dunia maya. Persamaan penelitian ini adalah tanggung jawab negara terkait keamanan siber dan melindungi warga negara dari ancaman siber. Perbedaan penelitian adalah pada fokus, literatur pertama memiliki cakupan yang lebih luas, membahas konsep keamanan siber, kerangka kerja teoretis, dan tanggung jawab secara umum.

Literatur kelima ditulis Pepijn Tuinier, Thijs Brocades Zaalberg & Sebastiaan Rietjens, tahun 2019, dengan judul penelitian **"The Social Ties that Bind: Unraveling the Role of Trust in International Intelligence Cooperation"** (Tuinier et al., 2023). Dalam penelitian ini, menggunakan teori sosiologi dan psikologi sosial untuk menganalisa peran kepercayaan dalam kerja sama intelijen internasional. Kemudian, mengacu pada konsep-konsep seperti hubungan sosial, identifikasi sosial, dan persepsi tentang kepercayaan untuk memahami mekanisme yang mendorong perilaku kerja sama di antara badan-badan intelijen. Penelitian ini bertujuan untuk menggarisbawahi pentingnya kepercayaan, hubungan sosial, dan persepsi bersama tentang kepercayaan dalam menanggapi tantangan dan kompleksitas kerja sama intelijen internasional, serta menawarkan wawasan tentang mekanisme kerja sama yang efektif. Adapun perbedaan penelitian ini adalah mengkaji pentingnya kepercayaan dalam membina kerja sama yang efektif di antara badan-badan intelijen internasional. Adapun persamaan penelitian ini adalah membahas pentingnya kerja sama intelijen internasional dalam menanggapi tantangan dan ancaman.

Literatur keenam ditulis oleh John Battersby & Rhys Ball, pada tahun 2023, yang berjudul **"The Phantom Eye: New Zealand and the Five Eyes"** (Battersby & Ball, 2023)**.** Literatur ini menjelaskan tentang konteks peristiwa sejarah, operasi intelijen, dan dinamika keamanan nasional Selandia Baru sebagai anggota Five Eyes. Tujuan dari penelitian adalah untuk memberikan analisis dan diskusi yang mendalam mengenai sejarah, operasi, dan transparansi badan intelijen, khususnya berfokus pada peran Selandia Baru dalam aliansi Five Eyes. Adapun perbedaan

dalam penelitian adalah berfokus pada partisipasi Selandia baru sebagai anggota Five Eyes. Adapun persamaan penelitian adalah sejarah awal berdirinya Five Eyes dan tujuan negara-negara Five Eyes dalam meningkatkan keamanan.

Berdasarkan dari keenam literatur diatas, adapun perbedaan penelitian dengan penulis yaitu penelitian ini lebih menyoroti pentingnya kerja sama lintas negara dalam menghadapi ancaman spionase siber yang semakin berkembang. Dengan fokus pada Five Eyes, penulis menyelidiki bagaimana negara-negara dalam aliansi ini saling berbagi informasi sumber daya dan teknologi untuk melindungi sistem keamanan siber dari serangan siber yang berpotensi merusak dan strategi pencegahan siber seperti apa yang harus dilakukan.

2.2. Kerangka Teoritis / Konseptual

1. Teori Kerja sama Internasional

Koesnadi K menegaskan bahwa kerja sama internasional tidak hanya terjadi antar negara secara individual tetapi juga antar negara yang tergabung dalam organisasi atau lembaga internasional. Menurutnya, kerangka kerja sama internasional muncul sebagai akibat dari hubungan saling ketergantungan dan semakin kompleksnya kehidupan manusia di dalam komunitas internasional (Oktora et al., 2019). Berdasarkan pernyataan Koesnadi K diatas menegaskan bahwa kerja sama internasional adalah elemen vital dalam hubungan antar negara di era modern. Bahwa kerja sama ini tidak terbatas pada interaksi bilateral antara negara-negara secara individual, melainkan juga mencakup hubungan multilateral yang melibatkan berbagai negara yang tergabung dalam organisasi atau lembaga internasional. Contoh konkret dari organisasi semacam itu adalah Perserikatan Bangsa-Bangsa (PBB), Organisasi Perdagangan Dunia (WTO), dan Uni Eropa (UE), yang semuanya memainkan peran krusial dalam memfasilitasi kolaborasi dan dialog antar negara untuk mengatasi tantangan global.

Menurut Koesnadi K, dorongan utama di balik terbentuknya kerangka kerja sama internasional adalah hubungan saling ketergantungan antar negara. Dalam dunia yang semakin terhubung dan terglobalisasi, tidak ada negara yang dapat berdiri sendiri tanpa membutuhkan dukungan dan sumber daya dari negara lain.

Ketergantungan ini mencakup berbagai aspek, termasuk ekonomi, politik, keamanan, teknologi, dan lingkungan. Kompleksnya kehidupan manusia di dalam komunitas internasional juga menjadi faktor pendorong kerja sama internasional. Kompleksitas ini muncul dari berbagai tantangan global yang dihadapi, seperti perubahan iklim, krisis ekonomi, terorisme, pandemi, dan isu-isu kesehatan global lainnya. Tantangan-tantangan ini tidak dapat diselesaikan secara efektif oleh satu negara saja, melainkan memerlukan kolaborasi dan koordinasi yang erat antar negara. Dalam konteks ini, organisasi internasional berperan sebagai platform untuk negosiasi, perumusan kebijakan bersama, dan pelaksanaan program-program yang bertujuan untuk mengatasi masalah-masalah tersebut.

Kerja sama internasional memungkinkan negara-negara untuk saling mendukung, berbagi sumber daya, dan bekerja bersama dalam mencapai tujuan bersama, seperti kestabilan, kemakmuran, dan perdamaian dunia. Dengan demikian, kerangka kerja sama internasional yang dibangun atas dasar saling ketergantungan dan kompleksitas kehidupan global menjadi fondasi penting bagi terciptanya komunitas internasional yang lebih harmonis dan sejahtera.

Menurut Kalevi Jaakko Holsti (1988) kerja sama internasional dapat didefinisikan sebagai berikut (Pujonggo et al., 2022):

a. Pandangan bahwa dua atau lebih kepentingan nilai atau tujuan saling bertemu dan dapat menghasilkan sesuatu dipromosikan atau dipenuhi oleh semua pihak sekaligus.
b. Pandangan atau harapan suatu negara bahwa kebijakan yang diputuskan oleh negara lain akan membantu negara tersebut untuk mencapai kepentingan dan nilai-nilainya.
c. Kesepakatan atau hal-hal tertentu antara dua negara atau lebih dalam rangka mengambil keuntungan dari kepentingan bersama.
d. Aturan resmi atau tidak resmi mengenai transaksi di masa depan yang dibuat untuk melaksanakan perjanjian tersebut.
e. Transaksi antar negara untuk memenuhi perjanjian.

Dalam konteks penelitian, hal ini dapat dipahami dikaitkan dengan konsep diatas bahwa kerja sama intelijen internasional Five Eyes muncul sebagai akibat dari hubungan saling ketergantungan antara negara-negara anggotanya dalam menghadapi ancaman, termasuk serangan spionase siber yang semakin kompleks. Negara-negara tersebut menyadari bahwa mereka perlu saling berkaitan dan berbagi informasi untuk memenuhi kepentingan dan nilai-nilai bersama. Kemudian, kerja sama intelijen Internasional Five Eyes melibatkan transaksi informasi antar negara-negara anggota. Informasi dan tujuan yang diperoleh suatu negara, dapat digunakan untuk memenuhi kepentingan dan nilai-nilai negara anggota lainnya dalam menghadapi serangan spionase siber.

2. Teori Intelijen

Berdasarkan buku petunjuk lapangan Angkatan Darat AS (2019) yang berlaku, intelijen mengacu pada hasil yang diperoleh dari pengumpulan, pemrosesan, penggabungan, penilaian, analisis, dan penafsiran informasi yang dapat diakses terkait negara asing, kekuatan atau elemen yang bermusuhan atau berpotensi bermusuhan, atau wilayah operasi saat ini atau yang berpotensi. Dapat dipahami bahwa intelijen didefinisikan sebagai pengumpulan, pemrosesan, analisis, dan penyebaran informasi yang sangat penting bagi pengambilan keputusan dalam keamanan nasional dan operasi militer. Dalam buku berjudul Intelligence and National Security (2007), karya J. Ransom Clark, dijelaskan bahwa terdapat lima cara utama dalam mengumpulkan intelijen yang sering disebut sebagai "disiplin pengumpulan intelijen" atau "INT", antara lain;

a. ***Human Intelligence*** **(HUMINT)**, diperoleh melalui berbagai cara yang melibatkan manusia secara langung, seperti spionase atau pengintaian, atase militer, dan kegiatan terbuka yang melibatkan diskusi dengan pejabat asing. Di Amerika Serikat, pengumpulan HUMINT adalah tanggung jawab FBI. Di luar perbatasan AS, HUMINT umumnya dikumpulkan oleh CIA.
b. ***Imagery Intelligence*** **(IMINT)**, berasal dari gambar yang diambil dari udara menggunakan balon, pesawat terbang, atau satelit. Saat ini, fotografi hanya merupakan salah satu metode pencitraan, sehingga istilah IMINT

lebih umum digunakan daripada istilah PHOTINT atau intelijen fotografi yang lebih kuno. Cara ini digunakan oleh Badan Intelijen Geospasial Nasional dalam merancang, membangun, dan mengoperasikan satelit citra.

c. ***Measurement and Signature Intelligence*** **(MASINT)**, melibatkan penggunaan intelijen teknis selain citra dan sinyal. Metode ini menggunakan nuklir, optik, frekuensi radio, akustik, seismik, dan ilmu material untuk menemukan, mengidentifikasi, atau menggambarkan karakteristik khas target.
d. ***Open-Source Intelligence*** **(OSINT)**, berhubungan dengan informasi yang tersedia untuk umum, seperti surat kabar, siaran radio dan televisi, jurnal, internet, atau database komersial. Termasuk dalam OSINT adalah video, grafik, gambar, dan informasi yang tidak diklasifikasikan yang memiliki akses atau distribusi publik yang terbatas.
e. ***Signals Intelligence*** **(SIGINT),** berasal dari komunikasi yang disadap (COMINT), termasuk komunikasi tertulis yang menggunakan tinta yang tidak terlihat atau enkripsi. Selain itu, SIGINT juga mencakup pancaran elektromagnetik (ELINT) yang berasal dari emisi radar, atau aktivitas eletronik.

Dalam salah satu tujuan intelijen keamanan yang tercantum dalam *National Intelligence Strategy* 2023, disebutkan bahwa peran intelijen salah satunya adalah memberikan peringatan dini dengan memperjelas bahwa tantangan transnasional yang semakin meningkat merupakan inti dari keamanan nasional dan internasional. Oleh karena itu, badan intelijen bertekad untuk meningkatkan kemampuannya dalam memahami, mengantisipasi, dan memberikan peringatan dini tentang ancaman transnasional, serta mengidentifikasi peluang bagi Amerika Serikat, sekutu, dan mitranya (NIS, 2023).

Berdasarkan penjelasan teori inteljen diatas dapat dipahami bahwa penelitian penulis terkait " Kerja Sama Intelijen Internasional Five Eyes Dalam Menanggapi Serangan Spionase Siber: Studi Kasus di Amerika Serikat ", hal ini sesuai dengan teori intelijen tentang ***Signals Intelligence*** **(SIGINT)** yang mengumpulkan

informasi dari sinyal dan aktivitas elektronik. Sebagaimana yang diketahui bahwa serangan spionase siber ini melibatkan penggunaan sinyal dan sistem elektronik.

3. Cyber Deterrence Theory

Sejarah awal 'cyber deterrence' dimulai pada tahun 1994, ketika James Der Derian, yang saat ini menjabat sebagai direktur Centre for International Security Studies di Universitas Sydney, pertama kali memperkenalkan istilah ini dalam artikelnya di Wired (Soesanto, 2022b). Pada saat itu, Der Derian menggunakan istilah 'cyber deterrence' untuk menggambarkan dominasi militer digital AS yang ditunjukkan melalui media voyeurisme, pameran teknologi, dan simulasi strategis. Definisi ini sangat relevan dalam konteks operasi militer Desert Storm, yang menampilkan teknologi stealth, amunisi yang diarahkan dengan presisi, dan akses luas dari jurnalis yang terintegrasi dalam operasi combat. Meskipun konsep 'cyber deterrence' secara resmi diperkenalkan pada tahun 1994, elemen- elemennya telah muncul dalam praktik sejak tahun 1970-an. Ini termasuk worm pertama yang menyebar secara mandiri (Creeper) yang dihentikan oleh worm lain (Reaper), dan lahirnya industri perlindungan diri siber pada pertengahan tahun 1980-an.

Dalam perkembangannya, konsep 'cyber deterrence' beralih dari definisi awal yang diberikan oleh Der Derian menjadi kumpulan teori dan mekanisme yang diterapkan dalam domain siber. Pada tahun 1998-1999, konflik di Kosovo, yang dianggap sebagai "perang Internet" pertama, melibatkan aktivitas siber seperti serangan malware dan serangan DDoS terhadap server email NATO, yang menandakan awal dari spionase digital negara. Setelah itu, diskusi akademis tentang 'cyber deterrence' berkembang pesat, terutama setelah serangan DDoS terhadap Estonia pada tahun 2007 (Soesanto, 2022b). Konsep ini mulai mencakup berbagai mekanisme deterrence yang diterapkan dalam domain siber, termasuk teori relasi internasional, metode kriminologi, dan teknik perang psikologis.

Secara keseluruhan, sejarah awal 'cyber deterrence' menunjukkan perjalanan dari definisi yang berfokus pada dominasi militer digital menuju kumpulan mekanisme yang dirancang untuk menavigasi dan mengelola ancaman dalam domain siber.

Konsep *cyber deterrence* (pencegahan dunia maya) mengacu pada penggunaan strategi dan tindakan untuk mencegah musuh terlibat dalam aktivitas kejahatan dunia maya, tujuan *cyber deterrence* adalah untuk memengaruhi perilaku musuh dan mencegah pelaku melakukan serangan siber (Jaikaran, 2022). Dalam konteks menanggapi ancaman serangan siber, *cyber deterrence* dipandang sebagai langkah yang diperlukan untuk menciptakan ketertiban dan keamanan. Namun, mencapai *cyber deterrence* merupakan hal yang menantang karena karakteristik unik dunia maya. Tidak seperti pencegahan secara tradisional, di mana ada aktor yang diketahui dan konsekuensi yang ditetapkan, dunia maya dicirikan oleh banyak musuh potensial dan ketidakjelasan mengenai tindakan pembalasan. Selain itu, rendahnya biaya untuk memperoleh kemampuan serangan siber membuat aktor jahat lebih mudah terlibat dalam agresi siber. Meskipun demikian, negara-negara terus mengejar strategi *cyber deterrence* sebagai cara untuk menanggapi dan mengurangi ancaman siber.

Terdapat enam mekanisme *cyberdeterrence* telah muncul selama bertahun-tahun yang mencoba mempengaruhi dan menguraikan dinamika di dunia maya (Soesanto, 2022):

1) *Deterrence by denial*: Sebuah konsep dalam kerangka kerja pencegahan siber yang lebih luas. Hal ini mengacu pada strategi yang menghalangi musuh dalam meluncurkan serangan siber, dengan mempersulit atau membuat mereka tidak dapat mencapai tujuannya. Pendekatan ini berfokus pada penguatan langkah-langkah dan kemampuan pertahanan untuk menolak atau mengurangi efek serangan siber. Dalam konteks pencegahan siber, *deterrence by denial* melibatkan penerapan langkah-langkah keamanan siber yang kuat seperti, firewall, sistem deteksi, enkripsi, dan kontrol akses untuk melindungi infrastruktur, jaringan, dan sistem yang penting. *Deterrence by denial* mencakup langkah-langkah proaktif seperti intelijen ancaman, pemantauan berkelanjutan, dan kemampuan merespons insiden. Langkah-langkah ini memungkinkan organisasi untuk mendeteksi dan merespons ancaman siber dengan cepat, meminimalkan potensi kerusakan dan gangguan yang disebabkan oleh serangan. Postur pertahanan

yang kuat dan kemampuan yang ditunjukkan untuk merespons insiden siber secara. menghalangi musuh potensial untuk menargetkan organisasi yang dipertahankan. Contoh *deterrence by denial* adalah penerapan otentikasi multi-faktor (MFA) dalam mengakses sistem dan data sensitif. Membutuhkan beberapa bentuk otentikasi, seperti kata sandi atau kode unik yang dikirim ke perangkat seluler, dapat sangat mengurangi potensi akses yang tidak sah. Hal ini membuat lebih sulit bagi penyerang potensial untuk membobol sistem dan membuat mereka enggan untuk mencoba melakukan serangan sejak awal.

2) *Deterrence by delegitimization*: Sebuah konsep dalam kerangka kerja pencegahan siber yang mengacu pada strategi menghalangi musuh potensial untuk meluncurkan serangan siber dengan merusak legitimasi dan kredibilitas mereka di komunitas internasional. Pendekatan ini bertujuan untuk mengekspos dan mengutuk tindakan pelaku kejahatan dalam menimbulkan kerusakan reputasi dan konsekuensi diplomatik. *Deterrence by delegitimization* melibatkan upaya untuk mengaitkan serangan siber dengan aktor tertentu dan secara terbuka mengekspos keterlibatan keduanya. *Deterrence by delegitimization* juga dapat melibatkan pembentukan opini publik dan narasi seputar serangan siber. Dengan menyoroti dampak negatif dari serangan siber terhadap individu, organisasi, dan masyarakat, tujuannya adalah untuk membangkitkan kemarahan publik dan dukungan untuk tindakan balasan terhadap calon penyerang. Hal ini selanjutnya dapat berkontribusi untuk mendelegitimasi tindakan mereka dan mengurangi kemampuan mereka untuk beroperasi dengan kekebalan hukum. Contoh pencegahan dengan delegitimasi adalah mengaitkan serangan siber dengan kelompok peretasan yang disponsori negara. Ketika serangan siber dikaitkan dengan negara-bangsa tertentu, hal itu dapat menyebabkan ketegangan diplomatik dan merusak reputasi negara yang bertanggung jawab. Hal ini dapat mengakibatkan kecaman internasional, sanksi ekonomi, atau bentuk pembalasan lainnya, yang dapat menghalangi

calon penyerang dengan membuat mereka berpikir dua kali sebelum meluncurkan serangan serupa.

3) *Deterrence by punishment*: Sebuah konsep dalam kerangka kerja *cyber deterrence* yang mengacu pada strategi untuk menghalangi musuh potensial meluncurkan serangan siber dengan membebankan biaya atau konsekuensi yang signifikan atas tindakan mereka. Pendekatan ini bertujuan untuk menciptakan efek jera dengan membuat musuh takut akan konsekuensi potensial dari tindakan mereka. *Deterrence by punishment* melibatkan penetapan kebijakan dan konsekuensi yang jelas untuk serangan siber. Hal ini mencakup kerangka kerja hukum, perjanjian internasional, dan norma-norma yang mendefinisikan serangan siber sebagai perilaku yang tidak dapat diterima dan menguraikan hukuman dan tanggapan yang akan dikenakan pada mereka yang bertanggung jawab. Contoh *deterrence by punishment* adalah termasuk sanksi ekonomi, tindakan diplomatik, atau tanggapan militer. Misalnya, jika suatu negara ditemukan terlibat dalam serangan siber besar, negara lain dapat menjatuhkan sanksi ekonomi dan memutuskan hubungan perdagangan dan keuangan. Langkah-langkah diplomatik dapat mencakup kecaman publik, isolasi diplomatik, dan pengusiran diplomat.
4) *Deterrence by entan- glement*: Sebuah konsep dalam kerangka kerja pencegahan siber yang mengacu pada strategi untuk menghalangi musuh potensial meluncurkan serangan siber dengan menciptakan saling ketergantungan dan interkoneksi. Pendekatan ini bertujuan untuk menghalangi penyerang potensial dengan menekankan potensi pembalasan dan keterkaitan dunia maya. Dalam konteks pencegahan siber, *deterrence by entan- glement* melibatkan pembentukan dan peningkatan ketergantungan di antara berbagai aktor seperti negara, organisasi, dan sistem infrastruktur penting. Contoh pencegahan melalui keterikatan adalah pembentukan perjanjian pertahanan bersama dan aliansi di dunia maya. Melalui kemitraan dan perjanjian, negara-negara dapat berjanji untuk saling mendukung dan membela satu sama lain jika terjadi serangan siber. Hal ini

menciptakan rasa keamanan dan pencegahan kolektif, karena penyerang potensial harus mempertimbangkan konsekuensi potensial dari menyerang satu entitas dalam aliansi, karena mengetahui bahwa hal itu dapat memicu respons dari banyak pihak.

5) *Deterrence by reputation*: Sebuah konsep dalam kerangka kerja pencegahan siber yang mengacu pada strategi untuk menghalangi musuh potensial meluncurkan serangan siber dengan membangun reputasi yang kuat untuk perilaku pembalasan dan konsekuensinya. *Deterrence by reputation* melibatkan demonstrasi rekam jejak tanggapan yang kuat dan efektif terhadap serangan siber. Dengan secara konsisten mengaitkan serangan dengan aktor tertentu dan secara konsisten dan terbuka menjatuhkan konsekuensi seperti sanksi ekonomi, tindakan diplomatik, dan tindakan hukum, reputasi untuk pembalasan yang kuat akan terbentuk. Tujuan dari *deterrence by reputation* adalah untuk membuat calon penyerang percaya bahwa biaya dan risiko yang terkait dengan peluncuran serangan siber lebih besar daripada potensi manfaatnya. Contoh *deterrence by reputation* adalah ketika sebuah negara secara konsisten merespons serangan siber dengan kecaman publik, tekanan diplomatik, dan sanksi ekonomi. Hal ini menciptakan persepsi bahwa negara berkomitmen untuk melindungi kepentingannya dan tidak akan mentolerir serangan siber. Akibatnya, calon penyerang mungkin berpikir dua kali sebelum menargetkan negara tersebut, karena takut akan potensi kerusakan reputasi mereka dan konsekuensi yang mungkin mereka hadapi.
6) *Cross-domain deterrence*: Sebuah konsep yang mengacu pada strategi untuk menghalangi musuh potensial agar tidak melancarkan serangan di satu domain dengan mengancam untuk membalas di domain lain. Konsep ini mengakui bahwa konflik dan ancaman dapat melampaui batas-batas tradisional dan melibatkan berbagai ranah: ruang siber, darat, laut, udara, dan ruang angkasa. Dalam konteks pencegahan siber, pencegahan lintas domain adalah penggunaan kemampuan dan tindakan dalam satu domain untuk menghalangi musuh potensial agar tidak meluncurkan serangan siber.

Misalnya, jika suatu negara mengalami serangan siber besar yang menyerang infrastruktur atau jaringan kritisnya, negara itu dapat mengomunikasikan respons militer atau sanksi ekonomi di domain lain. Tujuan *Cross-domain deterrence* adalah untuk menciptakan pencegahan yang kredibel dan efektif dengan menunjukkan kemampuan dan kemauan untuk merespons secara tegas di berbagai domain. Dengan membuat calon penyerang sadar bahwa tindakan mereka di dunia maya dapat menimbulkan konsekuensi serius di ranah lain, yang mana penyerang akan jera untuk melancarkan serangan siber karena takut akan pembalasan yang lebih luas. Contoh pencegahan lintas domain adalah ketika sebuah negara mengomunikasikan bahwa negara tersebut akan melakukan respons militer terhadap serangan siber apa pun terhadap infrastruktur kritisnya. Hal ini akan mengirimkan pesan yang jelas bahwa negara tersebut siap untuk meningkatkan konflik di luar dunia maya dan, jika perlu, terlibat dalam operasi militer konvensional. Koordinasi lintas domain semacam itu meningkatkan postur pencegahan dengan memperbesar potensi konsekuensi dari calon penyerang. yang kredibel dan menghalangi musuh potensial untuk meluncurkan serangan siber.

Berdasarkan penjelasan Cyber Deterrence Theory diatas dapat dipahami bahwa penelitian penulis terkait " Kerja Sama Intelijen Internasional Five Eyes Dalam Menanggapi Serangan Spionase Siber: Studi Kasus di Amerika Serikat", sesuai dengan enam mekanisme *cyber deterrence,* terdapat tiga kategori yang berkaitan dengan penelitian penulis, yaitu, *Detterence by Denial, Deterrence by punishment, Detterence by Delegitimization.*

2.3. Asumsi Penelitian

Dalam menghadapi serangan spionase siber yang semakin kompleks, kerja sama internasional dianggap sebagai solusi dalam melawan ancaman siber. Di era saat ini, serangan siber tidak lagi terbatas pada batas nasional. Oleh karena itu, kerja sama internasional di bidang intelijen menjadi sarana penting untuk mengurangi risiko dan merespon serangan. Kerja sama ini juga memungkinkan lembaga intelijen untuk memperoleh akses kepada intelijen dari mitra internasional,

sehingga meningkatkan kapasitas deteksi dan respons terhadap ancaman dengan lebih cepat. Selain itu, pertukaran informasi yang berkelanjutan dapat membentuk suatu ekosistem di mana lembaga intelijen dapat saling belajar dan meningkatkan kemampuan mereka secara berkelanjutan.

Pentingnya koordinasi juga ditekankan dalam asumsi ini, koordinasi antar negara menjadi kunci untuk menjaga kohesi dalam menanggapi serangan siber yang melibatkan pelaku dari berbagai wilayah. Dengan adanya kesepahaman bersama dalam prosedur yang terkoordinasi, negara-negara dapat mengoptimalkan sumber daya mereka dan menghadapi serangan dengan tindakan yang efisien. Kerja sama intelijen internasional bukan hanya tentang pertukaran informasi teknis, tetapi juga tentang membangun kepercayaan di antara negara-negara yang terlibat. Asumsi ini mencerminkan keyakinan bahwa hanya melalui kerja sama yang solid dan saling percaya, masyarakat internasional dapat membangun pertahanan yang kuat dalam menanggapi ancaman spionase siber yang terus berkembang.

2.4. Kerangka Analisis