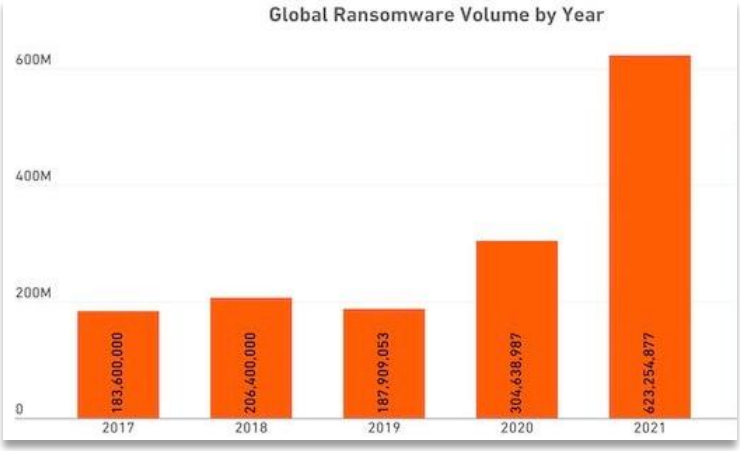
BAB I

PENDAHULUAN

1.1 Latar Belakang

Tahun 2021 menjadi tahun dengan total serangan siber tertinggi sejak 2016, di mana jumlah serangan tersebut mencapai 19,23 juta serangan (Statista, 2024). Di tahun 2021 jenis serangan siber yang paling tinggi berasal dari *malware* yaitu mencapai 45,9%, jumlah tinggi lainnya disusul oleh *Account Takeover* 10,8% dan *Vulnerability* 9,6% (Hackmageddon, 2021). *Malware* memiliki berbagai tipe, terdapat sejumlah serangan teratas dari tipe *malware* di tahun 2021 mulai dari *Trojan* (109.208), RAT (58.439), *Stealer* (37.718), *Loader* (36.275), *Installer* (22.805), *Ransomware* (16.120), *Keylogger* (4.640), *Adware* (2.815), *Miner* (1.724) (ANY.RUN, 2022). Di antara berbagai jenis *malware* tersebut, *ransomware* menjadi serangan yang paling disorot oleh masyarakat global. Hal ini dikarenakan meskipun *ransomware* tidak menempati urutan pertama sebagai tipe *malware* dengan serangan terbanyak, *ransomware* memiliki efek domino yang paling berbahaya di antara tipe *malware* yang lain. Serangan *ransomware* cenderung menargetkan infrastruktur penting di sebuah negara sehingga dampaknya dapat mengganggu stabilitas negara hingga keamanan sebuah negara melalui serangan yang dilakukan. *Ransomware* sendiri merupakan perangkat lunak jahat yang sistem kerjanya yaitu dengan mengenkripsi data atau sistem komputer korban kemudian meminta tebusan melalui mata uang digital seperti *cryptocurrency* (Hartono, 2023). Menurut data dari *SonicWall Cyber Threat Report*, upaya serangan *ransomware* secara global meningkat dua kali lipat di

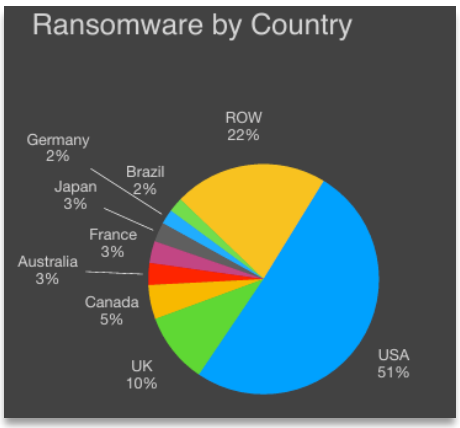
tahun 2021 dengan total mencapai 623,2 juta upaya serangan (CRN, 2023). Total serangan tersebut menunjukkan adanya peningkatan signifikan karena di tahun 2020, serangan *ransomware* global hanya mencapai 304,6 juta serangan.



Gambar 1.1.1 Grafik serangan *ransomware* global (2017-2021)

Sumber: (*SonicWall Cyber Threat Report* melalui CRN, 2023)

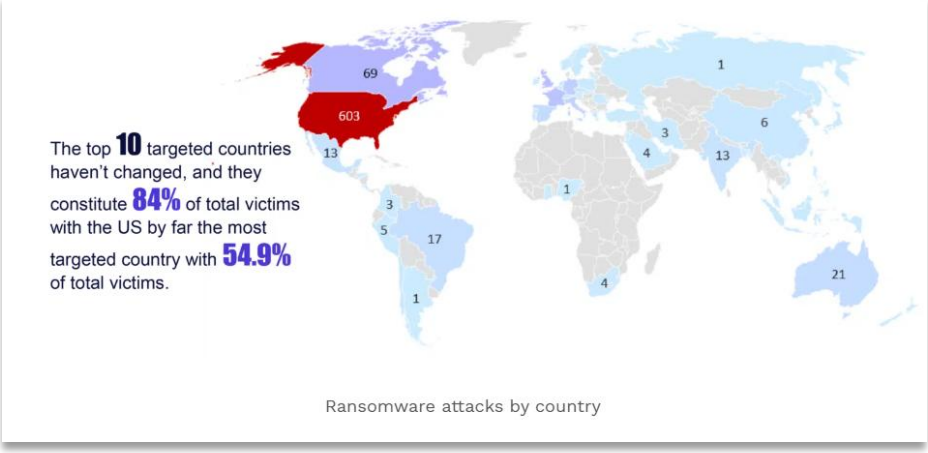
Di samping itu, laporan dari BlackFog menunjukkan bahwa 51% dari 100% serangan *ransomware* global menyasar ke AS, menjadikan AS sebagai target utama serangan *ransomware* global di tahun 2021 (BlackFog, 2024). Disusul oleh UK 10%, Kanada 5%, hingga Australia dan Prancis yang sama-sama menerima 3% total serangan (BlackFog, 2024). Dari sini dapat diketahui bahwa dibandingkan dengan negara-negara lain, AS menerima jauh lebih banyak serangan *ransomware* pada tahun tersebut dibandingkan dengan negara lain. Hal ini semakin diperparah karena serangan *ransomware* tersebut tidak hanya mengenkripsi data saja, tetapi juga 80% melibatkan pencurian data yang kemudian data tersebut di antaranya dijual ke negara seperti Rusia dan China (BlackFog, 2024).



Gambar 1.1.2 Persentase serangan *ransomware* berdasarkan negara (2021)

Sumber: (BlackFog, 2024)

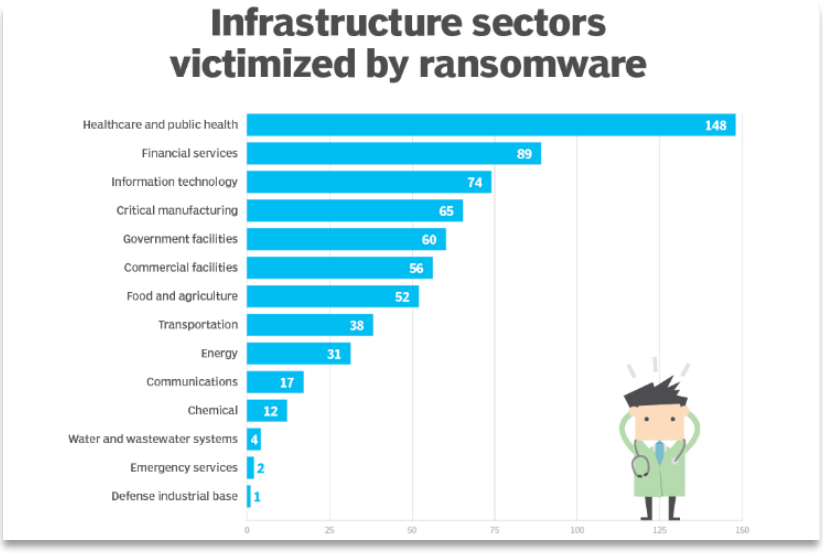
Data dari Cognyte juga menunjukkan bahwa 84% dari total korban *ransomware* global berasal dari sepuluh negara teratas yang paling diserang dan menempatkan AS sebagai negara utama yang paling ditargetkan (Cognyte CTI Research Group, 2021). Tercatat total korban serangan *ransomware* AS mencapai 603 korban atau 54,9% dari total korban global. Angka ini menempatkan AS jauh di atas negara-negara lain seperti Kanada, Australia, dan Jerman, yang jumlah korbannya tergolong jauh lebih rendah. Hal ini menunjukkan bahwa para aktor siber secara strategis menargetkan negara dengan infrastruktur digital yang kompleks dan nilai ekonomi yang tinggi, di mana AS menjadi sasaran yang paling menonjol.



Gambar 1.1.3 Peta korban serangan *ransomware* (2021)

Sumber: (Cognyte CTI Research Group, 2021)

Berdasarkan grafik laporan dari FBI, sasaran serangan *ransomware* di AS berdasarkan sektor dapat ditunjukkan mulai dari serangan terhadap sektor kesehatan, layanan keuangan, IT, lembaga pemerintah, infrastruktur kritikal, layanan komersial, makanan dan agrikultur, transportasi, energi, komunikasi, kimia, sistem air dan limbah, layanan darurat, hingga basis industri pertahanan (TechTarget, 2022). Dari grafik laporan FBI tersebut, terlihat bahwa sektor kesehatan menerima 148 serangan dan menjadikannya sebagai sektor yang paling banyak diserang. Di sini dapat diketahui bahwa pelaku *ransomware* tidak hanya menargetkan sektor yang berkaitan dengan keuntungan finansial langsung, tetapi juga sektor yang memiliki peran krusial dalam pelayanan publik dan kestabilan negara. Selain itu, berbagai sektor lain yang turut diserang memperkuat bukti bahwa *ransomware* menargetkan berbagai macam infrastruktur penting negara.



Gambar 1.1.4 Grafik target serangan *ransomware* 2021 berdasarkan sektor

Sumber: (FBI IC3 Annual, 2022)

Di samping itu, nilai pembayaran tebusan *ransomware* di AS berdasarkan laporan Financial Crimes Enforcement Network menunjukkan adanya peningkatan yang signifikan di tahun 2021. Di mana nilai pembayaran tebusan di 2021 mencapai $1,2 miliar, nilai pembayaran tersebut jauh berbeda dari tahun sebelumnya yang hanya mencapai $416 juta (Cybersecurity Dive, 2022). Melihat dari data tersebut, menunjukkan dampak finansial yang disebabkan oleh serangan *ransomware* semakin besar di setiap tahunnya. Dengan total tebusan mencapai $1,2 miliar, angka terserbut sebanding dengan 2,6% dari total anggaran perlindungan AS di tahun 2021 (USGovernmentSpending.com, 2025). Dalam hal ini, meskipun nilai tebusan serangan *ransomware* yang telah disebutkan tidak seluruhnya ditanggung oleh pemerintah AS, nominal tersebut menunjukkan besarnya kerugian finansial yang ditanggung oleh berbagai aktor nasional.

Dengan kata lain, hal ini menunjukkan bahwa kerugian finansial yang disebabkan oleh serangan *ransomware* secara tidak langsung membebani negara melalui gangguan ekonomi, krisis kepercayaan publik, hingga tekanan terhadap kebijakan keamanan nasional. Setidaknya jika dana dengan nilai besar tersebut tidak terserap untuk menanggulangi insiden, dapat disalurkan untuk pembangunan infrastruktur digital atau program strategis lain yang dapat memperkuat daya tahan nasional terhadap serangan ke depannya.

Dalam membahas terkait serangan *ransomware* di AS, setidaknya terdapat tiga insiden besar serangan *ransomware* yang terjadi di sepanjang tahun 2021. Dimulai pada 7 Mei 2021, Colonial Pipeline sebagai perusahaan penyuplai 45% bahan bakar di wilayah Timur AS dan mengoperasikan pipa sepanjang 8.850 km mengalami serangan dari kelompok DarkSide yang berbasis di Rusia (IEA, 2021). Akibat serangan tersebut, perusahaan harus membayar tebusan sebesar $4,4 juta dalam bentuk Bitcoin, sementara kerugian ekonomi tidak langsung diperkirakan mencapai ratusan juta dolar akibat gangguan logistik dan lonjakan harga bahan bakar (BBC, 2021). Serangan tersebut mendorong Presiden Joe Biden mengeluarkan Executive Order (EO) 14028 pada 12 Mei 2021. Biden menekankan pentingnya perbaikan sistem keamanan, tidak hanya secara teknis, tetapi juga melalui kolaborasi antara pemerintah dan sektor swasta. EO 14029 ini juga mencakup pendeteksian dini, respons cepat, pembaruan sistem keamanan, serta penegakan hukum terhadap pelaku serangan. Dengan demikian, EO 14028 menjadi fondasi awal bagi AS dalam membangun sistem pertahanan digital yang lebih kuat dan adaptif terhadap ancaman siber yang semakin kompleks.

Setelah dikeluarkannya EO 14028, serangan *ransomware* kembali terjadi pada 30 Mei 2021. JBS USA, perusahaan yang memainkan peran penting dalam pasokan pangan AS, memproses sekitar 20% dari total kebutuhan daging domestik (Supply Chain Dive, 2022). Serangan ini menyebabkan penutupan fasilitas di AS, Kanada, dan Australia, mengganggu rantai pasok pangan, menunda distribusi, serta memicu kelangkaan dan kenaikan harga daging. JBS juga harus membayar tebusan sebesar $11 juta dalam bentuk Bitcoin kepada kelompok REvil yang juga berbasis di Rusia (JBS Foods, 2021). Kemudian pada 2 Juli 2021, serangan kembali terjadi terhadap Kaseya yang merupakan perusahaan IT. Kelompok REvil mengeksploitasi celah Zero-day dalam produk *Virtual System Administrator* (VSA) milik Kaseya (CSO Online, 2021). Serangan ini menyebar secara luas melalui pembaruan berbahaya dan berdampak pada ribuan bisnis di berbagai negara. REvil menuntut tebusan sebesar $70 juta, namun Kaseya menolak membayar dan berhasil memulihkan sistem dengan bantuan pihak ketiga terpercaya (Cybersecurity Dive, 2021). Ketiga insiden besar di atas menjadi bukti nyata bahwa *ransomware* adalah ancaman serius bagi keamanan nasional AS karena menyasar sektor-sektor kritikal seperti energi, pangan, dan teknologi, serta bersifat lintas sektor dan lintas negara. Di mana dampak yang ditimbulkan tidak hanya pada kerugian ekonomi, tetapi juga mengguncang stabilitas dan keamanan nasional.

Situasi ini semakin diperparah dengan adanya bisnis *ransomware* melalui sistem yang dinamakan *Ransomware-as-a-Service* (RaaS). Terdapat developer yang membuat perangkat lunak jahat dalam hal ini *ransomware*, kemudian ini

disewakan atau dijual kepada mitra bisnis untuk disebarkan ke korban (IBM, 2024). Temuan ini menjadi bukti nyata bahwa melalui pola bisnis yang dijalankan oleh RaaS, membuat ancaman *ransomware* semakin mudah meningkat dan menjangkau ke ranah yang semakin luas. Secara konseptual, hal ini dapat melonggarkan batasan penjahat siber karena pihak yang tidak cukup mumpuni dalam IT dapat melakukan kejahatan siber melalui fasilitas yang dimiliki oleh RaaS.

Berangkat dari melonjaknya serangan *ransomware* di tahun 2021 dengan AS sebagai target utama, meningkatnya pembayaran tebusan, terjadinya berbagai insiden serangan besar yang turut membawa dampak serius kepada negara, hingga adanya bisnis *ransomware* yang dapat menembus batas yurisdiksi, semakin menunjukkan bahwa ancaman *ransomware* telah menjadi ancaman lintas batas negara yang nyata. Hal ini mendorong adanya urgensi AS untuk melakukan kerja sama internasional dalam menangani ancaman *ransomware* global. Ini sejalan dengan pernyataan European Union Agency for Cybersecurity (EUAC) yang menekankan pentingnya kerjasama internasional dalam menghadapi ancaman siber. Sebelumnya, AS telah menjalin banyak kerja sama untuk menangani ancaman siber baik bilateral maupun multilateral (Sullivan & Lizar, 2022). Kerja sama ini mulai dari EU-US Cyber Dialogue; kerja sama dengan Korea Selatan, Jepang, dan Australia di bidang teknis, pertukaran informasi, dan pelatihan bersama; Cyber Defence Pledge; United Nations Group of Government Expert (UN GGE); aliansi intelijen Five Eyes; Global Forum on Cyber Expertise (GFCE); Budapest Convention on Cybercrime; Indo-Pacific

Cybersecurity Framework; hingga Quad Cybersecurity Cooperation, yang melibatkan AS, Jepang, India, dan Australia.

Meskipun telah memiliki banyak kerja sama internasional dalam menangani ancaman siber, meningkatnya intensitas dan kompleksitas serangan *ransomware* dalam beberapa tahun terakhir mendorong AS dalam membentuk kerja sama yang lebih spesifik dan terfokus untuk menangani ancaman tersebut. Dalam hal ini AS menginisiasi pembentukan kerja sama multilateral Counter Ransomware Initiative (CRI) untuk secara khusus menangani ancaman *ransomware* secara lebih efektif. CRI dibentuk pada 13 Oktober tahun 2021 yang merupakan sebuah forum kerja sama internasional bersifat *ad hoc* dan multilateral. Forum ini mempertemukan negara-negara dan organisasi internasional dengan kepentingan bersama dalam menghadapi ancaman *ransomware* global. Pembentukan CRI ini merupakan respons lanjutan atas meningkatnya frekuensi serangan *ransomware* serta lingkup serangan yang semakin luas. Meskipun CRI bukan kerja sama siber pertama AS, tetapi ini merupakan kerja sama internasional pertama yang secara khusus dibentuk untuk menangani ancaman *ransomware* secara sistematis, multilateral, dan proaktif.

Saat ini CRI telah memiliki lebih dari 60 anggota, meskipun AS menjadi inisiator kerja sama ini tetapi tidak semua negara di kawasan Amerika masuk ke dalam keanggotaan CRI. Meskipun demikian, terdapat banyak negara besar di kawasan Amerika yang turut menjadi anggota seperti Kanada, Brasil, Argentina, Kolombia, Meksiko, Kosta Rika, Chili termasuk negara-negara di kawasan Amerika Utara, Eropa, Asia, Oceania hingga Afrika (Counter Ransomware

Initiative, n.d.). Pada dasarnya keanggotaan dalam CRI tidak didasarkan pada kawasan geografis atau aliansi politik tertentu, melainkan lebih kepada kepentingan bersama dan *concern* terhadap masalah *ransomware*. Negara yang bergabung umumnya memiliki perhatian serius terhadap meningkatnya ancaman *ransomware* dan berkomitmen untuk bekerja sama dalam menangani isu ini secara kolektif.

Selain itu, keanggotaan CRI turut melibatkan aktor non-negara seperti Council of Europe, European Union, INTERPOL, Organization of American States, Economic Community of West African States Commission, hingga Global Forum on Cyber Expertise (Counter Ransomware Initiative, n.d.). Dalam konteks ini, organisasi internasional seperti INTERPOL, Council of Europe, dan European Union memiliki kapasitas struktural dan mandat kebijakan yang memungkinkan mereka memperkuat kolaborasi antarnegara. Kerja sama mereka fungsional karena menjadi simpul koordinatif dan teknokratis dalam mengisi celah yang tidak bisa dijangkau oleh kerja sama bilateral semata. Selain itu, ini mencerminkan pendekatan *multi-stakeholder*, di mana keamanan siber tidak bisa ditangani oleh negara secara eksklusif, tetapi menuntut sinergi dengan institusi yang memiliki mandat dan kapabilitas lintas negara. Hal ini menunjukkan bahwa kerja sama organisasi internasional dalam CRI merefleksikan pendekatan kolektif dan teknokratik dalam menanggulangi kejahatan siber transnasional. Berbeda dengan EO 14028 yang memfokuskan pada perbaikan sistem internal, CRI menjadi perluasan respon AS dari internal ke kerja sama global.

Berbagai studi telah mengkaji respons negara-negara terhadap ancaman

siber serta urgensi kerja sama siber dalam mengatasi kejahatan siber lintas negara. Seperti penelitian yang ditulis oleh Ho Ting (Bosco) Hung (2024) berjudul *"Multilateral cooperation in building critical infrastructure security and resilience: case of American deterrence of Chinese cyberthreats"* menggunakan konsep *integrated deterrence* yang menjadi bagian dari strategi keamanan nasional AS. Konsep ini menekankan pentingnya koordinasi dengan sekutu dan mitra internasional, penggunaan diplomasi digital, serta pengembangan kemampuan siber untuk menghadapi ancaman dari negara seperti Tiongkok. Hasil penelitian menunjukkan bahwa kerja sama multilateral, seperti pembentukan *Bureau of Cyberspace and Digital Policy*, menjadi instrumen kunci dalam membangun sistem pertahanan siber kolektif yang tangguh. Penelitian ini juga menekankan bahwa efektivitas pencegahan terhadap serangan siber, termasuk *ransomware*, bergantung pada Kerja Sama berbagai aktor internasional serta peningkatan kemampuan atribusi dan respons siber bersama.

Penelitian lain dari Brandon Valeriano (2020) berjudul *"Cybersecurity and Multilateralism: The US and Its Role in Shaping Global Cyber Norms*" menggunakan pendekatan teori normatif dan kebijakan luar negeri untuk menganalisis peran AS dalam membentuk norma-norma keamanan siber global melalui kerja sama multilateral. Hasil penelitian mengungkapkan bahwa AS aktif memimpin pembentukan standar dan kerangka kerja keamanan siber di berbagai organisasi internasional, namun terdapat tantangan akibat perbedaan kepentingan dan pendekatan dengan negara lain, seperti China dan Rusia, yang memengaruhi proses pembentukan norma global secara efektif.

Penelitian dari André Barrinha dan Rebecca Turner (2024) berjudul *"Strategic Narratives and the Multilateral Governance of Cyberspace: The Cases of European Union, Russia, and India"* menggunakan konsep *strategic narratives*, yaitu narasi strategis yang digunakan negara untuk memproyeksikan kepentingan dan membentuk norma dalam forum internasional. Penelitian ini juga mengadopsi kerangka kerja *regime complex theory* untuk menjelaskan fragmentasi tata kelola siber global. Hasil penelitian menunjukkan bahwa negara-negara utama seperti Uni Eropa, Rusia, dan India menggunakan narasi yang berbeda tergantung forum internasional yang mereka ikuti. Temuan ini menunjukkan bahwa narasi yang dibangun dalam forum multilateral dapat mempengaruhi arah kebijakan siber global.

Penelitian oleh Robles-Carrillo dan García-Teodoro (2022) yang berjudul *"Ransomware: An Interdisciplinary Technical and Legal Approach"* menggunakan pendekatan interdisipliner antara dimensi teknis dan hukum. Hasil penelitian ini menunjukkan bahwa perlawanan terhadap *ransomware* memerlukan integrasi antara respons teknologi dan instrumen hukum, serta mendorong pengakuan *ransomware* sebagai tindak pidana yang berdiri sendiri, dan penelitian ini juga menyoroti pentingnya kerja sama internasional seperti CRI meskipun kerja sama tersebut masih dinilai belum mengikat secara hukum.

Meskipun demikian, penelitian-penelitian tersebut belum ada yang secara khusus mengkaji bagaimana implementasi kerja sama siber AS melalui CRI terutama pada periode 2021-2024. Atas dasar tersebut, tujuan penelitian ini yaitu mengisi celah penelitian melalui analisis terhadap implementasi kerja sama siber

AS yang menitikberatkan terhadap perlawanan ancaman *ransomware* global melalui CRI mulai dari tahun 2021-2024 karena melihat insiden serangan siber terutama *ransomware* yang semakin meningkat, meluas, dan kompleks. Melalui penelitian ini akan dapat diketahui peran dan langkah yang dilakukan oleh AS melalui CRI selama periode tersebut.

1.2 Rumusan Masalah

Mengangkat terkait dengan upaya AS dalam melawan ancaman *ransomware*, berdasarkan latar belakang yang telah diuraikan dalam hal ini rumusan masalahnya itu "Bagaimana implementasi kerja sama siber AS melalui CRI pada periode tahun 2021-2024?"

1.3 Tujuan Penelitian

1.3.1 Secara Umum

Secara umum, tujuan penelitian ini yaitu untuk memenuhi persyaratan dalam memperoleh gelar sarjana (S1) Hubungan Internasional, Fakultas Ilmu Sosial, Budaya, dan Politik di Universitas Pembangunan Nasional "Veteran" Jawa Timur.

1.3.2 Secara Khusus

Secara khusus, tujuan penelitian ini menjelaskan bagaimana AS mengimplementasikan kerja sama siber melalui CRI dalam merespons ancaman *ransomware* yang bersifat lintas negara. Penelitian ini berupaya memahami secara mendalam apa saja yang dilakukan AS melalui kerja sama CRI, baik dalam bentuk inisiatif, strategi, maupun struktur kerja sama yang dibangun

bersama anggota CRI. Pendekatan ini tidak hanya melihat CRI sebagai forum koordinasi, tetapi juga sebagai bagian dari kebijakan luar negeri AS dalam menghadapi isu keamanan non-tradisional di era digital. Melalui analisis terhadap aktivitas dan kontribusi AS di dalam kerja sama CRI, penelitian ini diharapkan dapat memberikan perspektif baru dalam studi Hubungan Internasional, khususnya mengenai bagaimana kerja sama siber multilateral dijalankan oleh aktor negara sebagai respons atas ancaman yang tidak berbatas wilayah, dan bagaimana AS memposisikan diri dalam tatanan keamanan siber global.

1.4 Kerangka Pemikiran

1.4.1 Ancaman Siber

Ancaman dapat dimaknai sebagai upaya berbahaya yang dapat menimbulkan kekacauan seperti terancamnya keselamatan masyarakat, hingga terganggunya kedaulatan negara yang berasal dari faktor internal maupun eksternal negara (Chiara Vincha, 2024). Sedangkan ancaman siber merupakan tindak kejahatan di dunia digital yang memiliki tujuan untuk melakukan eksploitasi kelemahan digital, mulai dari mencuri data, mengunci data, melakukan perusakan pada sistem digital maupun jaringan komputer, hingga melumpuhkan layanan publik (Mijwil, 2023). Perbedaan antara ancaman siber dan ancaman konvensional yaitu dimensi lintas batas negara tanpa terhalang letak geografis serta dapat menembus yurisdiksi negara manapun serta dapat menargetkan siapapun. Situasi tersebut semakin diperparah dikarenakan pelaku

serangan siber semakin terorganisir, pelaku juga dapat berasal dari aktor negara yang bertujuan mengganggu stabilitas negara lawan melalui dunia digital. Ancaman siber merupakan isu yang semakin mendesak dalam konteks keamanan global, di mana berbagai aktor, baik negara maupun non-negara, berusaha untuk mengeksploitasi kerentanan dalam sistem informasi dan infrastruktur kritis (Choo, 2011). Dalam kajian ancaman siber, penting untuk memahami bagaimana, mengapa, dan apa saja bentuk ancaman yang muncul, serta dampaknya terhadap keamanan nasional dan internasional (Hathaway, et al., 2012).

Ancaman siber memiliki lingkup yang luas mulai dari gangguan sederhana sampai dengan gangguan besar yang mampu mengganggu serta melumpuhkan infrastruktur vital sebuah negara. Terdapat berbagai bentuk ancaman siber seperti *Phising* yang merupakan jenis serangan siber berupa penipuan digital dengan mengelabui korban demi mendapatkan data pribadi melalui email sampai situs bodong; *Distributed Denial of Service* (DDoS) menyerbu server sampai membuatnya tidak dapat digunakan atau mati total; *malware* penyusup digital yang mampu melakukan pengintaian, pencurian hingga perusakan sistem atau jaringan komputer; *ransomware* sebagai jenis *malware* yang bekerja dengan mengenkripsi data hingga sistem korban dan meminta tebusan; *Advanced Persistent Threats* (APT) sebagai salah satu bentuk ancaman siber yang masuk ke dalam sistem atau jaringan komputer secara diam-diam dan bertahan lama di dalamnya untuk dapat melakukan pencurian data dan jenis ini cenderung menargetkan instansi pemerintah hingga perusahaan besar, serta *zero-day exploit*

yaitu pemanfaatan celah keamanan yang belum diketahui dan belum diperbaiki. Berbagai ancaman siber tersebut dapat memberikan dampak serius dalam cakupan yang luas.

Di antara berbagai jenis ancaman siber, *ransomware* menjadi ancaman siber yang sedang menjadi sorotan terutama di era pandemi Covid-19 karena telah berhasil membuat berbagai kekacuan dan kerugian finansial. *Ransomware* tidak sebatas sebagai masalah teknologi, hal ini karena serangan siber mulai menargetkan infrastruktur vital hingga hingga perusahaan besar. Semakin banyak layanan publik yang berbasis digital dan kemajuan teknologi 5G, menjadi sebagian faktor pendukung yang membuat *ransomware* semakin agresif dan sifatnya lintas batas negara (Chiara Vincha, 2024). Lewis (2018) menyoroti bahwa serangan siber yang dilakukan oleh aktor negara dan kelompok kriminal memiliki dampak yang melampaui batas negara, merusak institusi politik, dan mengikis kepercayaan publik secara global. Hal ini sejalan dengan pandangan dari Kello (2013) yang menekankan pentingnya kolaborasi antara pemerintah, sektor swasta dalam menciptakan ekosistem keamanan siber yang tangguh (Kello, 2013). Dengan demikian, ancaman siber telah berkembang menjadi tantangan utama bagi keamanan dan stabilitas global, yang memerlukan perhatian serius dari berbagai negara dan aktor internasional.

1.4.2 Kerja Sama Siber

Merangkum dari penjelasan para ahli, kerja sama siber merupakan pondasi dalam membangun sistem keamanan global dengan ketahanan dan tingkat adaptabilitas yang tinggi untuk menghadapi berbagai jenis ancaman siber. Kerja

sama tidak terbatas pada antisipasi risiko, tetapi terkait menciptakan kepercayaan yang tinggi antar aktor untuk dapat saling bertukar informasi penting sampai strategi pertahanan (Nye & Welch, 2016). Seiring dengan tingkat kejahatan siber yang semakin tinggi dan dapat menggapai lingkup yang semakian luas, untuk menghadapi hal tersebut diperlukan adanya kerja sama antar negara. Kerja sama merupakan senjata efektif dalam menangani serangan digital (Nye & Welch, 2016). Kerja sama siber merupakan bentuk kolaborasi antarnegara dalam menghadapi ancaman di ruang digital, seperti serangan *ransomware,* peretasan, hingga spionase siber yang bersifat lintas batas. Untuk dapat memberikan respons cepat dan efektif ketika terjadi penyerangan, diperlukan adanya kerja sama antar negara yang saling percaya dan memiliki peraturan yang jelas (Nye & Welch, 2016). Dalam perspektif hubungan internasional, kerja sama ini masuk ke dalam praktik diplomasi keamanan karena berkaitan dengan upaya kolektif untuk menciptakan ruang siber yang aman dan stabil (Carr, 2016). Sehingga dalam hal ini terdapat sejumlah hal yang penting untuk menjadi sorotan mulai dari penguatan norma global, pembangunan kepercayaan antarnegara, serta institusi kerja sama internasional dalam mengurangi potensi konflik dan meningkatkan transparansi dalam dunia siber. Sejalan dengan hal tersebut, kerja sama siber menurut Deibert (2012) lebih baik tidak hanya melibatkan aktor negara, tetapi juga aktor non-negara seperti sektor swasta, lembaga teknis, dan komunitas keamanan digital yang memainkan peran penting dalam membangun kepercayaan dan kapabilitas kolektif global (Deibert, 2012).

Dalam menganalisis kerja sama siber, penelitian ini mengadopsi lima

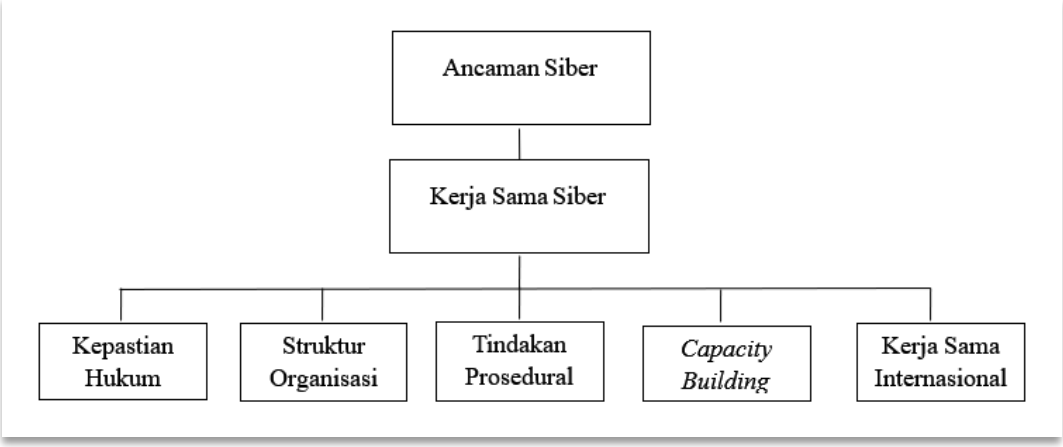
bidang strategis dari Ardiyanti (2014), yaitu kepastian hukum, struktur organisasi, *capacity building*, kerja sama internasional, dan tindakan prosedural (Ardiyanti, 2014). Meskipun kelima bidang ini berasal dari kajian mengenai strategi keamanan siber secara umum, namun masing-masing indikator tersebut juga merepresentasikan elemen-elemen utama dalam kerja sama siber global. Sehingga dapat digunakan untuk melihat sejauh mana implementasi kerja sama siber dilakukan.

Dalam penelitian ini, indikator kepastian hukum, tercermin dari keberadaan komitmen bersama dan inisiatif kebijakan yang berfungsi sebagai acuan kolektif dalam mendorong akuntabilitas, memperkuat transparansi, serta mencegah bebasnya pelaku kejahatan siber dari pertanggungjawaban hukum (Robles-Carrillo & García-Teodoro, 2022). Indikator struktur organisasi, tercermin dalam pembentukan mekanisme kelembagaan yang terstruktur dan terkoordinasi melalui beberapa pilar yang saling melengkapi, sehingga memungkinkan pembagian peran dan kolaborasi yang efektif dalam respons keamanan siber (Reibe, Kaufhold, & Reuter, 2021). Indikator tindakan prosedural, terlihat dari penerapan mekanisme teknis dan *platform* berbagi informasi yang efisien untuk deteksi, mitigasi, dan respons terhadap insiden *ransomware* (Robles-Carrillo & García-Teodoro, 2022). Indikator *capacity building*, diwujudkan melalui program pengembangan kemampuan teknis dan koordinasi antar anggota, termasuk pelatihan hingga *workshop* yang mendukung kesiapan bersama dalam menghadapi serangan *ransomware* (O'Neil , Ahmad, & Maynard, 2021). Terakhir, indikator kerja sama internasional tercermin dari

partisipasi aktif dalam forum internasional dan pertemuan tahunan yang secara berkelanjutan merumuskan strategi kolektif dan memperkuat upaya lintas sektor dalam penanggulangan ancaman siber global (Targarev, 2020).

1.5 Sintesa Pemikiran

Tabel 1.5.1 Sintesa pemikiran



Sumber: (Olahan penulis, 2025)

Seiring meningkatnya ancaman siber secara global, membuat negara perlu melakukan kerjasama siber, yang kemudian diimplementasikan dalam 5 bentuk, meliputi: yaitu kepastian hukum, struktur organisasi, tindakan prosedural, *capacity building*, dan kerja sama internasional.

1.6. Argumen Penelitian

Implementasi kerjasama siber AS melalui CRI diwujudkan dalam 5 bentuk meliputi: Dalam indikator kepastian hukum, sampai saat ini CRI belum menghasilkan hukum internasional yang mengikat, perjanjian, atau mekanisme penegakan hukum yang terstandarisasi. Dalam hal ini, AS melakukan kerja sama siber dengan menunjukkan inisiatif normatif melalui kebijakan strategis yang

menjadi landasan kerja sama internasional, antara lain dengan mendorong adopsi FATF Recommendation 15 ke dalam agenda CRI, mengedepankan prinsip *No Safe Haven* bagi para pelaku kejahatan siber, serta menerapkan pendekatan *whole-of-government* dan *whole-of-society* sebagai bentuk komitmen terhadap tata kelola siber yang terintegrasi. Pada indikator struktur organisasi, AS melakukan kerja sama siber dengan mengoordinasikan pembentukan rezim CRI. Hal ini terlihat dari peran AS melalui White House sebagai pusat koordinasi yang membentuk sistem *governance* CRI. Awalnya hanya berupa *working group*, struktur CRI kemudian berevolusi menjadi empat pilar resmi, yaitu *Policy Pillar*, *Operational Pillar*, *Diplomacy* & *Capacity Building Pillar*, dan *The Private Sector Eangagement Working Group* (PSEWG), dengan AS bertindak sebagai koordinator utama sekaligus sekretariat CRI. Dalam indikator tindakan prosedural, AS melakukan kerja sama siber melalui kontribusinya dalam pelaksanaan berbagai *platform* dan inisiatif, seperti *Malware Information Sharing Platform* (MISP), *Crystal Ball,* pembentukan *International Counter Ransomware Task Force* (ICRTF). Pada indikator *capacity building*, AS melakukan kerja sama siber melalui berbagai kegiatan peningkatan kapasitas seperti *workshop "International Workshop on Fighting Ransomware at Criminal Intelligence Service"* dan latihan simulasi lain untuk meningkatkan kesiapan serta koordinasi antar negara anggota CRI. Indikator kerja sama internasional, AS melakukan kerja sama siber melalui peran sentralnya dalam menyelenggarakan CRI *Annual Summit*. Dalam forum ini, AS memfasilitasi penyusunan agenda kerja sama dan memimpin diskusi multilateral. Fokus isu

dari CRI *Annual Summit* setiap tahunnya antara lain: (2021) Penguatan ketahanan jaringan, penghentian aliran dana tebusan, penegakan hukum terhadap pelaku *ransomware*, dan peningkatan kerja sama internasional. (2022) Pembentukan ICRTF dan peningkatan koordinasi serta pertukaran informasi antar negara. (2023) Peningkatan ketahanan kolektif, pelibatan sektor swasta, serta dorongan terhadap akuntabilitas dan transparansi di ruang siber. (2024) Pemanfaatan *Artificial Intelligence* (AI) dalam penanganan *ransomware*, penguatan kebijakan asuransi siber untuk meningkatkan ketahanan organisasi, serta penyusunan panduan respons insiden khususnya untuk sektor kesehatan dan infrastruktur kritis.

1.7 Metodologi Penelitian

1.7.1 Tipe Penelitian

Penelitian ini menggunakan tipe penelitian kualitatif-deskriptif karena penulis akan fokus mengkaji terkait implementasi kerja sama siber AS melalui CRI mulai dari tahun 2021-2024. Melalui tipe penelitian ini penulis akan dapat memberikan gambaran penuh terkait kerja sama AS melawan ancaman *ransomware* global. Mengutip dari Sugiyono (2017), penelitian kualitatif-deskriptif akan menjelaskan kembali dinamika sosial melalui kata-kata serta mengumpulkan sumber data dari dokumen. Melalui tipe penelitian ini, memudahkan penulis dalam mendalami upaya kerja sama internasional dengan tujuan melawan ancaman siber khususnya ancaman *ransomware* global yang semakin agresif dan meluas.

1.7.2 Jangkauan Penelitian

Dalam membatasi penelitian ini, penulis membahas kerja sama siber AS melalui CRI selama periode 2021-2024. Tahun 2021 dipilih karena tahun tersebut sebagai tahun serangan *ransomware* yang mampu mengguncang AS dan menjadi dasar dibentuknya CRI. Tahun 2024 menjadi batasan penelitian ini karena di tahun tersebut penulis mendapati adanya fase eskalasi kerja sama yang dimotori AS semakin matang dalam pelaksanaan CRI.

1.7.3 Teknik Pengumpulan Data

Penelitian terkait kerja sama AS dalam melawan ancaman *ransomware* global ini menggunakan teknik pengumpulan studi literatur. Mengutip dari Sugiyono (2016), mendefinisikan ini sebagai teknik pengumpulan data melalui sumber yang didapatkan dari dokumen resmi, buku, laporan resmi, artikel berita, jurnal ilmiah dan sumber referensi lainnya yang kredibel dan sejalan dengan topik yang sedang diteliti oleh penulis. Dalam konteks penelitian, penulis menggunakan data-data dari dokumen resmi dari website resmi CRI, *White House Briefings*, *Executive Orders*, dan lainnya. Selain itu juga melalui laporan dari lembaga siber seperti IBM, BlackFog, kemudian jugal artikel media kredibel seperti Cybersecurity Dive serta sumber lain yang dapat membantu penulis dalam menyelesaikan penelitian ini.

1.7.4 Teknik Analisis Data

Teknik analisis data dalam penelitian ini yakni analisis kualitatif. Menurut Creswell (2014), analisis kualitatif melibatkan proses pengumpulan, analisis, dan

interpretasi data yang bersifat deskriptif dan tidak terstruktur, dengan tujuan untuk memahami makna dari pengalaman individu atau kelompok (Creswell, 2014). Dalam hal ini, analisis kualitatif dapat membantu peneliti memahami bagaimana AS dalam mengimplementasikan kerja sama siber melalui CRI.

1.7.5 Sistematika Penulisan

BAB I: Memuat Pendahuluan, Latar Belakang Masalah, Tinjauan Pustaka, Rumusan Masalah, Tujuan Penelitian, Kerangka Pemikiran, Sintesa Pemikiran, Argumen Utama, dan Metode Penelitian.

BAB II: Memuat Implementasi Kerja Sama Siber AS melalui CRI periode tahun 2021-2024 dalam Wujud Kepastian Hukum dan Struktur Organisasi

BAB III: Memuat Implementasi Kerja Sama Siber AS melalui CRI periode tahun 2021-2024 dalam Wujud Tindakan Prosedural, *Capacity Building*, dan Kerja Sama Siber

BAB IV: Memuat Penutup, Kesimpulan, dan Saran.