BAB II

KEBIJAKAN KEAMANAN SIBER AMERIKA SERIKAT, AKTOR SIBER UTAMA AMERIKA SERIKAT, PERETASAN TERHADAP SOLARWINDS DAN DAMPAK PERETASAN

Kasus Peretasan terhadap SolarWinds oleh kelompok Cozy Bear pada tahun 2020 menimbulkan perhatian yang cukup besar di Amerika Serikat, hal ini semakin mengkhawatirkan dengan adanya peran Rusia di balik serangan ini. Serangan siber ini berpotensi menyasar data krusial terkait militer dan intelijen yang memang tidak akan berdampak langsung terhadap kehidupan sehari-hari masyarakat Amerika Serikat, namun hal ini menimbulkan pertanyaan terkait respons dalam menangani serangan yang bersifat siber ini, dimana sebelum melihat respons Amerika Serikat, perlu untuk mengetahui bagaimana kebijakan keamanan siber Amerika Serikat, proses terjadinya serangan serta dampaknya.

2.1. Kebijakan Keamanan Siber Amerika Serikat

Melalui berbagai kejadian siber yang dialami Amerika Serikat, kebijakan keamanan siber Amerika Serikat telah berkembang sejak awal abad ke-21, dari yang awalnya tidak terkoordinasi menjadi sebuah kerangka kerja yang lebih terstruktur dan menyeluruh. Perkembangan kebijakan siber dilakukan seiring perkembangan teknologi yang menyertakan ancaman baru bagi ruang siber Amerika Serikat. Pada tahap awal terdapat perdebatan terkait lembaga manakah yang memiliki wewenang penuh pada ranah siber serta apakah koordinasi harus

dipimpin oleh kantor eksekutif, departemen kabinet, atau badan khusus (Newmeyer, 2012). Hal ini mengakibatkan tidak adanya sebuah struktur yang padu dalam menangani serangan siber di Amerika Serikat.

Tahun 1998 menjadi titik awal dimulainya kebijakan yang mendeklarasikan perlunya keamanan pada sektor siber di Amerika Serikat. Melalui Presidential Decision Directive 63 (PDD-63) pada Mei 1998, Presiden Amerika Serikat saat itu Bill Clinton menandai pengakuan resmi bahwa infrastruktur nasional Amerika Serikat seperti energi, keuangan, dan telekomunikasi memiliki kerentanan terhadap ancaman serangan berbasis komputer dan perlu dilindungi melalui koordinasi lintas lembaga (Lardner, 2000). Melalui PDD-63 diresmikannya National Infrastructure Protection Center (NIPC) yang sebelumnya sudah lebih dulu terbentuk pada bulan Februari di bawah FBI sebagai pusat koordinasi nasional dan mewajibkan setiap lembaga federal memiliki pejabat khusus yang menangani keamanan infrastruktur siber (The White House, 1998). PDD-63 menjadi kebijakan pertama yang memberikan pengakuan formal bahwa infrastruktur siber nasional membutuhkan perlindungan terkoordinasi.

Pada kebijakan PDD-63, Amerika Serikat hanya menyatakan bahwa adanya ancaman nyata di ranah siber, yang kemudian membentuk kebijakan The National Strategy to Secure Cyberspace pada tahun 2003. The National Strategy to Secure Cyberspace merupakan kebijakan publik yang diterbitkan oleh Presiden George W. Bush pada 14 Februari 2003. Menjadi strategi nasional pertama yang secara komprehensif menetapkan kerangka kerja keamanan siber nasional, dengan

tujuan melindungi infrastruktur kritikal, memperkuat kerjasama dari sektor publik bersama swasta, kebijakan ini muncul setelah serangan terorisme 9/11 dengan anggapan bahwa terdapat kekhawatiran kejadian 9/11 dapat terjadi di lingkup digital, melalui strategi ini Amerika Serikat memperkenalkan peran Department of Homeland Security (DHS) sebagai koordinator utama keamanan siber nasional menggantikan NIPC yang sebelumnya berada dibawah FBI (The White House, 2003). The National Strategy to Secure Cyberspace 2003 memperluas fungsi dari sekadar pengakuan ancaman menjadi kerangka kebijakan nasional yang memposisikan DHS sebagai koordinator utama dan menekankan kemitraan antara publik dan swasta.

Selanjutnya President George W. Bush membentuk Comprehensive National Cybersecurity Initiative (CNCI) pada Januari 2008. Setelah meningkatnya kesadaran akan ancaman siber, inisiatif CNCI dibentuk dengan tujuan untuk memperkuat keamanan jaringan dan sistem federal, CNCI merupakan serangkaian inisiatif nasional yang dirancang untuk memperkuat keamanan jaringan pemerintah melalui peningkatan deteksi, pengurangan kerentanan, penguatan kerjasama antar lembaga baik publik dan swasta, serta investasi pada *research and development* (*R&D*) dan tenaga ahli (Rollins & Henning, 2009). Beberapa bagian CNCI bersifat terklasifikasi, namun diketahui dari inisiatif ini mendorong implementasi berbagai alat teknis seperti program EINSTEIN yang merupakan program deteksi intrusi tingkat federal yang mengaplikasikan teknologi dengan tujuan memantau lalu lintas jaringan dan aktivitas sistem untuk menemukan tanda-tanda aktivitas berbahaya melalui sistem

Intrusion Detection System (*IDS*) (Rollins & Henning, 2009). Kebijakan CNCI menggeser fokus kebijakan dari kerangka strategis yang bersifat normatif ke implementasi teknis operasional seperti program deteksi dan pengurangan kerentanan.

Setelah memiliki kebijakan teknis dalam menjaga keamanan ruang siber, pada Mei 2009 Amerika Serikat selanjutnya melakukan peninjauan kebijakan yang dinamai Cyberspace Policy Review 2009. Kebijakan peninjauan menyeluruh ini diperintahkan pemerintahan Obama setelah menjabat untuk menilai posisi kebijakan siber Amerika Serikat saat itu dan memberi rekomendasi cepat untuk memperbaikinya. Laporan ini menemukan bahwa terdapat kelemahan yang antara lain seperti tanggung jawab antar lembaga yang tidak jelas, pemantauan nasional terhadap ancaman siber masih lemah, dan perlunya sinergi kuat antar kemitraan pemerintah bersama swasta (The White House, 2009) Untuk menanggulanginya, dalam dokumen ini juga merekomendasikan berbagai kebijakan seperti penunjukan pejabat kebijakan siber di White House (*cyber coordinator*), peningkatan kemampuan deteksi dan rencana respons nasional, pengembangan tenaga ahli, serta mekanisme berbagi informasi yang melindungi privasi. Tinjauan kebijakan siber ini berfungsi sebagai evaluasi korektif yang mengidentifikasi kelemahan implementasi dan merekomendasikan perbaikan struktural serta kapasitas, berbeda dari CNCI yang lebih berorientasi pada peluncuran alat-alat teknis daripada reformasi kebijakan lintas lembaga.

Setelah melakukan peninjauan terhadap kebijakan siber Amerika Serikat serta memberikan rekomendasi kebijakan terhadap kelemahan yang ada,

pemerintahan Presiden Obama selanjutnya membangun kebijakan luar negeri Amerika Serikat pada ranah siber. Melalui International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World pada Mei 2011, strategi kebijakan ini menempatkan dunia maya sebagai arena internasional yang memerlukan aturan, norma, dan kerja sama multilateral, selain tindakan domestik diperlukan juga kerjasama internasional dalam rangka melindungi kepentingan nasional dan menjaga kebebasan di dunia maya (The White House, 2011). Dengan kata lain, kebijakan ini memperluas jangkauan kebijakan dari ranah domestik ke diplomasi internasional dan pembentukan norma, sehingga fungsinya bukan hanya proteksi nasional tetapi juga upaya menata perilaku negara di ruang siber.

Kemudian pada April 2015 Department of Defense (DoD) mengeluarkan kebijakan DoD Cyber Strategy, kebijakan ini menjelaskan bagaimana peran militer Amerika Serikat akan melindungi jaringan, sistem, dan operasi militernya dari ancaman siber, sekaligus mengembangkan kemampuan ofensif bila diperlukan. Melalui DoD Cyber Strategy 2015 Amerika Serikat menyatakan bahwa serangan siber dapat memicu dampak fisik, sehingga rahan siber dianggap bagian dari arena tempur resmi bagi militer Amerika Serikat, karena hal tersebut United States Cyber Command (USCYBERCOM) dan National Security Agency (NSA) ditetapkan sebagai komando utama dalam operasi pertahanan dan serangan siber (U.S. Dod, 2015). Kebijakan DoD 2015 menegaskan siber sebagai domain operasi militer dengan pengembangan kapabilitas defensif dan ofensif, yang membedakannya dari strategi sebelumnya karena memasukkan unsur-unsur militerisasi dan respons yang dapat bersifat proaktif.

Setelah memiliki kebijakan yang dilakukan oleh lembaga eksekutif, Amerika Serikat melalui Cybersecurity Act of 2015 (CSA 2015) pada Desember 2015 menegaskan landasan legislatif utama yang diresmikan oleh kongres untuk arsitektur pertahanan siber modern Amerika Serikat dengan fungsi menjembatani kesenjangan komunikasi dan memfasilitasi pertukaran informasi ancaman siber secara langsung antara sektor swasta dan pemerintah federal. Secara mendasar undang-undang ini menciptakan kerangka hukum yang memberikan perlindungan liabilitas bagi entitas non-federal yang secara sukarela membagikan indikator ancaman siber dan langkah defensif kepada Department of Homeland Security (DHS), sehingga memungkinkan deteksi dini terhadap serangan siber yang kompleks tanpa ketakutan akan tuntutan hukum atau pelanggaran privasi pengguna (U.S. Congress, 2015). Dengan demikian, kebijakan ini berfungsi sebagai payung hukum fundamental yang mengubah paradigma pertahanan siber dari yang sebelumnya terfragmentasi menjadi kolaborasi terintegrasi, memungkinkan respons nasional yang lebih cepat terhadap insiden berskala besar seperti peretasan rantai pasok.

Melengkapi landasan legislatif tersebut, pada ranah operasional eksekutif, pemerintah Amerika Serikat menerbitkan Presidential Policy Directive 41 (PPD-41) yang berjudul *United States Cyber Incident Coordination* pada Juli 2016 sebagai upaya untuk mengatur tata kelola respons krisis dan mencegah tumpang tindih kewenangan antar-lembaga saat menghadapi serangan siber. PPD-41 menetapkan arsitektur koordinasi nasional dengan membagi peran penanganan insiden ke dalam tiga jalur upaya serentak, yaitu *threat response* yang

dipimpin oleh FBI untuk investigasi penegakan hukum, *asset response* oleh DHS melalui CISA untuk perlindungan aset dan pemulihan sistem, serta *intelligence support* oleh ODNI untuk analisis atribusi ancaman, yang semuanya disatukan dalam wadah komando Cyber Unified Coordination Group (UCG) (The White House, 2016). Keberadaan PPD-41 ini menjadi mekanisme yang mengubah pendekatan penanganan insiden dari yang sebelumnya bersifat sektoral menjadi pendekatan *whole-of-government* yang terintegrasi, memastikan bahwa respons negara terhadap intrusi masif seperti SolarWinds dapat dilakukan secara terkoordinasi di bawah satu komando strategis.

Pada September 2018 DoD Cyber Strategy 2015 diperbaharui dengan DoD Cyber Strategy 2018, dimana pada Cyber Strategy 2015 bersifat reaktif dan defensif sedangkan DoD Cyber Strategy 2018 menggeser kearah proaktif dan ofensif. Strategi ini memperkenalkan konsep operasional *Defend Forward* yang menugas pasukan siber Amerika Serikat untuk mengganggu atau menghentikan aktivitas siber berbahaya langsung di sumbernya termasuk pada jaringan asing sebelum serangan tersebut mencapai infrastruktur Amerika Serikat (U.S. DoD, 2018). Dengan demikian, perubahan doktrin ini memberikan legitimasi strategis bagi militer Amerika Serikat untuk melakukan operasi siber di luar perbatasan digitalnya guna menciptakan efek *deterrence* yang nyata dalam menghadapi kompetisi kekuatan besar seperti Rusia dan Tiongkok.

Bergeser dari tataran operasional ke arah strategis, Amerika Serikat memperkuat postur pertahanannya melalui penerbitan National Cyber Strategy pada September 2018 di masa pemerintahan Presiden Donald Trump. Dengan

fungsi sebagai landasan strategis nasional yang menetapkan visi *Peace Through Strength*. Kebijakan ini memberikan legitimasi politik bagi pemerintah untuk menggunakan seluruh instrumen kekuatan nasional dalam menghukum aktor negara yang melakukan serangan siber, terdiri dari empat pilar utama yaitu bertujuan untuk melindungi rakyat dan infrastruktur nasional, mendorong kemakmuran amerika, menjaga perdamaian melalui kekuatan dan *deterrence*, serta memperluas pengaruh Amerika di ranah global, melalui strategi ini Amerika Serikat menggunakan konsep *defend forward* yang lebih agresif dengan menekankan gabungan pendekatan *whole of government,* melalui koordinasi lintas lembaga DHS, DoD, NSA, FBI dengan *White House* sebagai pengarah utama (The White House, 2018). Dengan demikian, kebijakan ini menjadi landasan politis yang mengintegrasikan instrumen diplomasi, hukum, ekonomi, dan kekuatan militer untuk menciptakan efek *deterrence* yang nyata bagi aktor negara asing.

Perkembangan kebijakan siber Amerika Serikat berubah seiring dengan pergantian presiden dengan diterbitkannya National Cybersecurity Strategy oleh Presiden Joe Biden pada Maret 2023. Hal ini menandai pergeseran kebijakan dari upaya penangkalan dan kekuatan negara menuju pendekatan tata kelola, pencegahan struktural, dan akuntabilitas pasar. National Cybersecurity Strategy 2023 menekankan lima pilar, yaitu melindungi infrastruktur kritis, mengganggu dan melumpuhkan aktor jahat, mengarahkan insentif pasar agar keamanan menjadi prioritas, berinvestasi untuk meningkatkan ketahanan jangka panjang, dan memperkuat kerja sama internasional sambil menuntut tanggung jawab lebih

besar dari perusahaan teknologi dan penyedia layanan. (The White House, 2023). National Cyber Strategy era Biden ini banyak dipengaruhi oleh kejadian peretasan terhadap SolarWinds dengan menuntut akuntabilitas lebih besar dari perusahaan, berbeda dengan National Cyber Strategy 2018 era Trump yang lebih menitikberatkan pada *deterrence* dan konsep *defend forward*.

2.2. Aktor Utama Siber Amerika Serikat

Aktor kelembagaan keamanan siber nasional Amerika Serikat melibatkan jaringan kompleks dari berbagai lembaga pemerintah federal, dimana masing-masing lembaga memiliki otoritas dan kapabilitas tersendiri yang saling terkait dalam upaya untuk melindungi aset digital dan fisik negara. Sebagai lembaga sipil utama, Cybersecurity and Infrastructure Security Agency (CISA), merupakan lembaga yang berada di bawah Department of Homeland Security (DHS). CISA memimpin upaya perlindungan infrastruktur kritis non-militer seperti energi, keuangan, kesehatan dan jaringan pemerintah federal sipil. Fokus CISA adalah pada pemahaman, pengelolaan, dan pengurangan risiko siber dan fisik, yang mencakup analisis kerentanan, fasilitasi berbagi informasi ancaman melalui platform seperti *Automated Indicator Sharing* (AIS), dan melalui koordinasi respons insiden nasional untuk ranah sipil yang seringkali bekerjasama dengan sektor swasta (CISA, 2025). Dengan tugas utama pada perlindungan infrastruktur sipil, CISA memiliki peran penting dalam menjaga keamanan siber di Amerika Serikat.

Pada dimensi militer, keamanan siber dipegang oleh Department of Defense (DoD) melalui komando U.S. Cyber Command (USCYBERCOM). USCYBERCOM bertanggung jawab dalam mempertahankan jaringan militer, mendukung misi tempur dengan kapabilitas siber, serta membela negara dari serangan siber (U.S. DoD, 2015). Dengan ranah dunia digital ditetapkan sebagai wilayah operasionalnya, USCYBERCOM mengelola *Cyber Mission Force* dan melakukan operasi penuh di ranah siber secara *defensif* maupun *ofensif* sesuai kerangka hukum nasional dan internasional (U.S. DoD, 2018). Koordinasi erat antara USCYBERCOM dengan lembaga lain menjadi krusial terutama dalam menangani ancaman keamanan nasional.

Dukungan intelijen dan teknis untuk operasi siber yang khususnya berkaitan dengan aktor asing dilakukan oleh National Security Agency (NSA). Sebagai lembaga intelijen utama untuk *signals intelligence* (SIGINT) dan *information assurance* (IA), NSA mengumpulkan informasi mengenai kapabilitas dan niat aktor siber asing (NSA, n.d.). Dengan keahlian pada bidang kriptografi dan analisis kerentanan, NSA tidak hanya menyediakan intelijen vital tetapi juga mengembangkan kapabilitas siber canggih, melalui kerjasama dengan USCYBERCOM dalam mendukung operasi militer dan pertahanan jaringan keamanan nasional.

Di sisi penegakan hukum dan keadilan, Federal Bureau of Investigation (FBI), di bawah naungan Department of Justice (DOJ), bertindak sebagai penyelidik utama untuk kejahatan siber dan aktivitas siber berbahaya yang mengancam keamanan nasional. FBI menangani investigasi intrusi jaringan,

pencurian kekayaan intelektual, spionase siber, ransomware, dan terorisme siber, FBI memiliki program seperti InfraGard yang mengidentifikasi dan merespons ancaman terhadap keamanan nasional melalui kerjasama dengan sektor swasta dan kerjasama internasional yang berupaya dalam mengganggu operasi kriminal dan menganalisis serangan, kemudian DOJ bertanggung jawab atas penuntutan pelaku kejahatan siber sesuai hukum federal (U.S. Congress, 2020). FBI yang memiliki fokus pada fungsi investigasi, dapat bekerjasama dengan lembaga siber dalam negeri lainnya seperti CISA maupun USCYBERCOM dalam mengungkap suatu kasus.

Selanjutnya terdapat peran Office of the Director of National Intelligence (ODNI) sebagai pengarah pusat yang mengintegrasikan seluruh komunitas intelijen Amerika Serikat dan menjadi penghubung utama antara badan-badan intelijen dengan pembuat kebijakan nasional. Secara hukum, Direktur Intelijen Nasional memegang mandat untuk melaksanakan *National Intelligence Program* dan menyediakan produk intelijen strategis bagi Presiden serta Dewan Keamanan Nasional, sehingga ODNI memiliki wewenang dan tanggung jawab koordinatif yang jelas (U.S. Congress, 2025). Dalam insiden berskala nasional, ODNI berfungsi mengoordinasikan respons intelijen, membantu alokasi sumber daya melalui pengelolaan anggaran *National Intelligence Program*, serta memadukan bukti teknis dan analisis untuk mendukung proses mengidentifikasi pelaku serangan dan rekomendasi kebijakan.

Koordinasi strategis tertinggi untuk seluruh upaya keamanan siber nasional berada di Gedung Putih (The White House), dengan peran sentral dipegang oleh

National Security Council (NSC) dan Office of Science and Technology Policy (OSTP). Berdasarkan National Cyber Strategy 2018, NSC berfungsi sebagai badan utama yang mengintegrasikan isu siber ke dalam agenda keamanan nasional serta memimpin koordinasi antar-lembaga dalam merespons insiden siber signifikan melalui mekanisme Cyber Unified Coordination Group (UCG), sementara itu OSTP berfokus pada aspek koordinasi riset dan pengembangan teknologi (R&D) untuk memastikan keunggulan kompetitif Amerika Serikat di ranah siber (The White House, 2018). Secara umum Gedung Putih menetapkan arah kebijakan, menengahi perselisihan yurisdiksi, dan memastikan pendekatan *whole of government* yang padu dan selaras dengan prioritas nasional.

Terakhir terdapat peran dari Kongres Amerika Serikat, dimana peran dari kongres lebih bersifat fundamental dalam membentuk dan mengawasi seluruh arsitektur kelembagaan terkait siber ini. Melalui fungsi legislatifnya, Kongres menciptakan dasar hukum dan otoritas bagi lembaga eksekutif untuk bertindak, sekaligus menetapkan batasan hukum seperti perlindungan privasi, kemudian melalui wewenang anggarannya, Kongres mengendalikan pendanaan untuk semua program siber, yang secara langsung mempengaruhi prioritas dan kapabilitas lembaga, Kongres juga menjalankan fungsi pengawasan penting melalui dengar pendapat, investigasi, dan permintaan laporan untuk memastikan akuntabilitas dan efektivitas pelaksanaan kebijakan keamanan siber oleh cabang eksekutif (Trautman, 2015). Seluruh peran antara lembaga-lembaga yang memiliki otoritas tersendiri pada ranah siber ini membentuk dinamika implementasi kebijakan keamanan siber Amerika Serikat yang krusial.

Lembaga	Peran Utama	Yurisdiksi
CISA (Cybersecurity & Infrastructure Security Agency	Perlindungan dan ketahanan infrastruktur sipil non-militer	Fokus pada jaringan pemerintahan sipil sektor kritis seperti sektor energi, keuangan, kesehatan
USCYBERCOM (U.S. Cyber Command)	Komando militer untuk operasi siber	Fokus pada jaringan militer dengan keterlibatan terbatas pada jaringan sipil
NSA (National Security Agency)	Sinyal intelijen (SIGINT) dan kapabilitas teknis siber	Fokus pada mengumpulkan, menyimpan, menganalisis dan menyebarluaskan informasi sinyal intelijen asing
FBI (Federal Bureau of Investigation	Penegakan hukum federal atas kejahatan siber	Fokus pada kasus domestik untuk tindak pidana federal dengan bekerja sama dengan CISA, mitra internasional, dan lembaga intelijen bila diperlukan
ODNI (Office of the Director of National Intelligence)	Koordinasi komunitas intelijen dan pemberi produk intelijen strategis	Fokus melakukan fungsi koordinatif dan kebijakan dengan tidak menjalankan operasi langsung tetapi menyatukan informasi intelijen
The White House (NSC dan OSTP)	Penetapan kebijakan nasional dan koordinasi strategis	Fokus sebagai pengambilan keputusan strategis dengan memimpin *whole-of-government response*
Kongres	Legislasi, pengawasan, dan penganggaran	Fokus pada menentukan mandat jangka panjang, pembiayaan, dan batasan hukum untuk tindakan eksekutif setiap lembaga

Tabel 2.1. Peran dan Yurisdiksi Lembaga Amerika Serikat
(*Sumber: U.S. Congress, 2021; The White House, 2016*)

2.3. Kasus Peretasan Terhadap SolarWinds

Aktivitas mencurigakan pertama kali teridentifikasi di jaringan internal SolarWinds pada September 2019. Hasil analisis internal SolarWinds mengonfirmasi jejak aktivitas mencurigakan sejak September 2019 ketika para pelaku melakukan *dry run* atau uji coba dengan menyuntikkan kode uji ke dalam Produk SolarWinds Orion (Ramakrishna, 2021). Kemudian pada Februari 2020 para pelaku menyisipkan kode trojan ke dalam pembaruan Orion yang resmi (U.S. GAO, 2021). Meskipun telah memiliki akses sejak September 2019, para peretas tidak langsung menyerang, melainkan memantau proses pengembangan perangkat lunak SolarWinds untuk memahami bagaimana cara menyisipkan kode tanpa terdeteksi.

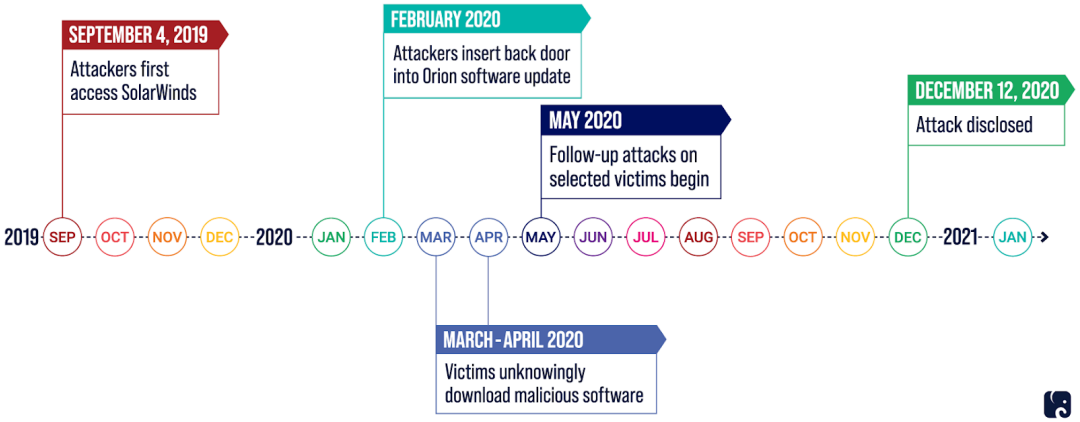
Awalnya para peretas melakukan *reconnaissance* yaitu memetakan layanan publik dan titik akses SolarWinds untuk mendapatkan akses secara tidak sah melalui pencurian kredensial atau eksploitasi layanan yang terpapar. Dengan akses tersebut para peretas dapat bergerak hingga mencapai *build environment* dan *server* SolarWinds yang menjadi target kritis, dimana dalam lingkungan *build,* para peretas menanam implant yang memantau proses kompilasi dan menyisipkan komponen tertentu sehingga *backdoor* terkompilasi bersama produk resmi, sebelum pelepasan penuh para peretas melakukan uji coba untuk memastikan modifikasi tidak menimbulkan kegagalan *build* atau kecurigaan (Anisa & Widianingsih, 2021). Proses ini menjadi tahap uji coba yang dilakukan pelaku untuk memastikan bahwa kegiatan mereka tidak memicu kecurigaan, sehingga para pelaku dapat melancarkan serangan yang tidak terdeteksi.

Setelah mengetahui bahwa aktivitas para peretas tidak teridentifikasi, tahap selanjutnya menyisipkan *malware* ke dalam produk Orion secara tersembunyi. Pada Februari 2020 para pelaku yang berafiliasi dengan Badan Intelijen Asing Rusia (SVR) menggunakan implant bernama SUNSPOT yang berjalan pada *server build* SolarWinds dan memantau proses kompilasi pembaharuan SolarWinds Orion, kemudian SUNSPOT menyisipkan salah satu file *backdoor* yang dinamai SUNBURST tanpa terdeteksi oleh tim pengembang (NSA, CISA, & FBI, 2021). Sementara itu, tim forensik SolarWinds menemukan bahwa mekanisme injeksi ini dilakukan dengan alat modifikasi kode terselubung, sehingga ketika proses perancangan produk pembaharuan selesai SUNBURST telah masuk ke paket pembaruan resmi tanpa menimbulkan kecurigaan (CrowdStrike, 2021). Teknik penyisipan *malware* melalui proses *build internal* seperti ini memperlihatkan bahwa langkah pengembangan perangkat lunak menjadi titik lemah kritis.

Setelah SUNBURST tertanam dalam produk pembaharuan, pelaku dapat mendistribusikan pembaruan SolarWinds Orion melalui mekanisme trojan ke basis pelanggan SolarWinds secara masif. FireEye melaporkan bahwa antara Maret hingga Mei 2020 beberapa pembaruan Orion yang diresmikan oleh SolarWinds telah diposting ke situs resmi update, dimana pembaharuan tersebut memuat *backdoor malware* SUNBURST yang akan aktif secara otomatis di lingkungan korban tanpa menimbulkan kecurigaan keamanan (Mandiant, 2022). Selanjutnya terkhusus pada bulan Mei 2020 para peretas memilih target yang dianggap krusial seperti Microsoft dan berbagai lembaga Federal Amerika Serikat

(U.S. Senate Republican Policy Committee, 2021). Trojan sendiri merupakan jenis *malware* yang menyamar sebagai program atau file yang tampak sah dimana distribusi pembaruan melalui trojan ini memastikan penyebaran *malware* ke skala yang sangat luas dan tanpa diketahui korban.

Setelah terinstal di jaringan korban, backdoor SUNBURST menjalankan kegiatan mata-mata dan eksploitasi lanjutan secara tersembunyi. SUNBURST memanfaatkan masa dormansi (*sleep period*) hingga dua minggu sebelum menghubungi *server* kendali dan menerima instruksi lebih lanjut, FireEye sebagai perusahan keamanan siber pertama yang melaporkan insiden peretasan terhadap SolarWinds mencatat bahwa backdoor tersebut kemudian mengeksekusi beragam perintah seperti transfer file, eksekusi payload, pengambilan profil sistem, dan reboot sistem, dengan menyamarkan lalu lintas jaringannya seolah terkait protokol sah SolarWinds (Mandiant, 2022). Rangkaian teknik ini memungkinkan backdoor SUNBURST dan modul pendukungnya berfungsi lama tanpa mudah terdeteksi.



Bagan 2.1. Alur Peretasan Terhadap SolarWinds
(*Sumber: U.S. Senate Republican Policy Committee, 2021)*

Dampak peretasan SolarWinds sangat luas hingga mempengaruhi sektor publik dan swasta secara internasional. GAO pada tahun 2021 melaporkan hampir 18.000 pelanggan SolarWinds menerima pembaruan tertrojan, termasuk berbagai lembaga federal Amerika Serikat yang merupakan target prioritas pelaku (U.S. GAO, 2021). Korban dari peretasan terhadap SolarWinds diketahui menjalar ke berbagai perusahaan seperti perusahaan keamanan siber, konsultansi, teknologi, telekomunikasi hingga energi serta banyak lembaga pemerintahan, bahkan Komisi Eropa mengonfirmasi bahwa dari 14 lembaga Uni Eropa yang menggunakan Orion, 6 unit teridentifikasi telah terinfeksi serangan ini (Marelli, 2022). Banyaknya korban yang terdampak dari berbagai entitas sektor global lainnya selain Amerika Serikat menunjukkan bahwa skala serangan SolarWinds bersifat sangat luas dan berimplikasi internasional.

Insiden ini menyebabkan pelanggaran data sensitif dan gangguan operasional yang serius bagi organisasi terdampak. FireEye sebagai perusahan keamanan siber yang pertama kali mendeteksi telah terjadi intrusi di jaringan SolarWinds melaporkan pada Desember 2020, sedangkan Microsoft mengkonfirmasi beberapa sistem *cloud* mereka sempat disusupi (Marelli, 2022). Akibat jangka panjangnya meliputi pemulihan infrastruktur yang memakan waktu lama serta peningkatan tekanan kebijakan keamanan siber di beberapa negara. Dengan demikian, peretasan ini bukan sekadar kegagalan teknis, melainkan krisis keamanan siber skala besar yang memaksa evaluasi ulang praktik keamanan rantai pasokan teknologi.

Penyelidikan teknis dan intelijen secara konsisten mengaitkan serangan ini dengan aktor negara. Terdapat bukti kuat yang menetapkan kegiatan yang dilabeli UNC 2452 sebagai nama internal untuk serangan dari kelompok APT 29 atau dikenal dengan Cozy Bear kepada SolarWinds (Mandiant, 2022). Hal tersebut sejalan dengan pernyataan pemerintah Amerika Serikat pada bulan April 2021 yang secara resmi menyebut Badan Intelijen Asing Rusia (SVR) bertanggung jawab atas serangan terhadap SolarWinds (The White House, 2021). Penyidikan bersama antara SolarWinds, perusahaan keamanan, dan lembaga pemerintah juga terus dilakukan untuk menelusuri dampak penuh insiden tersebut. Meskipun 18.000 pelanggan terinfeksi, penyerang tidak menetas semuanya, dimana para peretas secara selektif mengaktifkan backdoor hanya pada target bernilai tinggi seperti berbagai lembaga Amerika Serikat.

2.4. Dampak Peretasan SolarWinds Oleh Kelompok Cozy Bear

Teridentifikasinya Cozy Bear atau APT 29 yang dikenal juga The Dukes sebagai aktor di balik serangan SolarWinds mempertegas keterlibatan negara dengan kapabilitas spionase siber tingkat tinggi. Kelompok ini memiliki sejarah operasi yang sangat persisten dan telah aktif setidaknya sejak tahun 2008 dengan indikasi kuat bahwa adanya sponsor dari SVR, melihat dari pola serangan terarah yang secara konsisten menargetkan kementerian luar negeri, pertahanan, serta organisasi internasional seperti NATO untuk kepentingan pengumpulan intelijen strategis, keahlian kelompok ini dalam mengelola *malware* yang kompleks dan adaptif memungkinkan kelompok ini menghindari deteksi keamanan konvensional

dan mempertahankan akses dalam jaringan korban dengan rentan waktu yang panjang (F-Secure Labs, 2015). Melihat rekam jejak dan kecanggihan kelompok ini, dalam pembahasan selanjutnya akan diuraikan bagaimana kapabilitas Cozy Bear menghasilkan dampak berlapis mulai dari kerugian perusahan SolarWinds, implikasi keamanan bagi lembaga-lembaga federal Amerika Serikat, hingga konsekuensi geopolitik yang mempengaruhi posisi strategis dan kebijakan keamanan siber global.

2.4.1. Dampak Peretasan Terhadap Perusahan SolarWinds

Insiden SolarWinds secara luas mengakibatkan rusaknya reputasi perusahaan karena menunjukkan kelemahan dalam pengawasan keamanan pada proses pembaruan perangkat lunak perusahan SolarWinds. Reputasi SolarWinds tertekan setelah serangan ini dipandang sebagai kegagalan vendor dalam menjaga integrasi *supply chain software*, yang menyebabkan menurunnya kepercayaan pelanggan dan mitra bisnis (Willett, 2021). Selain itu, masifnya pemberitaan mengenai metode serangan dan banyaknya korban memperbesar tekanan reputasional terhadap perusahaan, dimana situasi ini mendorong desakan agar SolarWinds meningkatkan transparansi dan akuntabilitas dalam proses pengembangannya.

Peretasan ini juga menimbulkan tekanan finansial yang signifikan bagi SolarWinds, terutama terkait biaya pemulihan, investigasi, dan pengamanan ulang sistem. Serangan terhadap *supply chain* seperti perusahan SolarWinds sering menyebabkan beban keuangan besar, baik berupa biaya langsung maupun kehilangan pendapatan jangka panjang (Ghanbari & Wei, 2024). Selain itu,

laporan teknis mencatat bahwa beberapa pelanggan mempertimbangkan kembali kontrak layanan SolarWinds Orion akibat kekhawatiran terhadap keamanan produk (Kruti et al., 2023). Kombinasi biaya perbaikan dan potensi kehilangan kontrak menjadikan dampak keuangan yang sangat signifikan. Dengan demikian, kerugian ekonomi menjadi salah satu dampak utama yang ditanggung perusahaan.

Serangan tersebut juga menempatkan SolarWinds pada sorotan regulator dan berpotensi menimbulkan konsekuensi hukum terkait kelalaian keamanan siber. Analisis hukum internasional menegaskan bahwa perusahaan dalam kasus seperti SolarWinds dapat menghadapi investigasi, litigasi, dan peningkatan kewajiban kepatuhan (Coco et al., 2022). Selain itu, insiden ini memicu perdebatan tentang tanggung jawab vendor dalam memastikan keamanan *supply chain* yang dapat menimbulkan standar regulasi baru (Willett, 2021). Tekanan hukum ini menambah beban jangka panjang di luar aspek teknis dan finansial. Eskalasi pada dimensi regulasi menjadi bagian penting dari konsekuensi strategis bagi perusahaan.

Dalam jangka panjang, SolarWinds dipaksa melakukan reformasi menyeluruh terhadap prosedur internal, tata kelola keamanan, dan struktur organisasi untuk memulihkan kepercayaan publik. Insiden yang terjadi pada SolarWinds memaksa perusahaan mengadopsi standar keamanan yang lebih ketat dan meningkatkan transparansi operasional (Ghanbari & Wei, 2024). Dimana SolarWinds mengadopsi program *Secure by Design*, yaitu pembangunan kembali jalur produksi yang tersegmentasi dan komitmen untuk mengikuti pedoman National Institute of Standards and Technology (NIST) sebagai bagian dari upaya

memperketat standar keamanan dan meningkatkan transparansi operasional (SolarWinds, 2024). Perubahan struktural ini menunjukkan bahwa dampak serangan tidak hanya bersifat jangka pendek, tetapi mempengaruhi arah strategis perusahaan. Oleh karena itu, insiden ini menjadi momentum restrukturisasi besar bagi SolarWinds.

2.4.2. Dampak Peretasan Terhadap Lembaga Amerika Serikat

Peretasan SolarWinds memberikan dampak signifikan terhadap berbagai lembaga pemerintah Amerika Serikat karena pembaruan produk SolarWinds Orion yang terpapar memberikan akses tersembunyi kepada aktor asing ke jaringan internal federal. Setelah laporan FireEye pada 8 Desember 2020, CISA pada 13 Desember 2020 mengeluarkan Emergency Directive 21-01 yang memerintahkan seluruh lembaga federal sipil untuk segera mematikan produk SolarWinds Orion dari jaringan mereka (CISA, 2020). Hal ini diperlukan melihat bahwa setiap lembaga menghadapi risiko yang berbeda sesuai dengan karakter fungsi dan infrastruktur digitalnya, sehingga langkah respons dan mitigasi yang dilakukan dapat sangat bervariasi.

Emergency Directive (ED) merupakan instrumen perintah wajib yang diterbitkan oleh Cybersecurity and Infrastructure Security Agency (CISA) di bawah Department of Homeland Security (DHS) sebagai respons terhadap kerentanan atau ancaman keamanan siber yang terkonfirmasi memiliki risiko tinggi dan mendesak bagi sistem informasi pemerintah federal Amerika Serikat. ED memiliki kewenangan yang diatur dalam Cybersecurity Act of 2015 yang mewajibkan seluruh lembaga Federal Civilian Executive Branch (FCEB) untuk

segera mengimplementasikan langkah-langkah mitigasi teknis spesifik seperti pemutusan koneksi jaringan, pembaruan perangkat lunak, atau audit sistem dengan waktu yang ditentukan untuk mencegah eksploitasi lebih lanjut oleh aktor ancaman (U.S. Congress. 2015). Melalui ED 21-01 yang berlandaskan Cybersecurity Act of 2015, menjadikannya instrumen utama dalam pertahanan siber nasional yang responsif dengan mengharuskan seluruh lembaga federal memutus sistem yang terkait dengan produk SolarWinds.

Emergency Directive 21-01, yang diterbitkan pada 13 Desember 2020, merepresentasikan langkah defensif darurat yang diambil pemerintah Amerika Serikat untuk segera menghentikan kebocoran data akibat terpaparnya rantai pasok perangkat lunak SolarWinds Orion. Dalam direktif yang berjudul *Mitigate SolarWinds Orion Code Compromise* ini, CISA secara spesifik menginstruksikan seluruh lembaga Federal Civilian Executive Branch (FCEB) untuk segera memutus sambungan listrik atau jaringan dari instrumen SolarWinds Orion versi 2019.4 hingga 2020.2.1 yang terkonfirmasi mengandung *malware* SUNBURST, serta mewajibkan setiap lembaga untuk melaporkan status penyelesaian mitigasi tersebut kepada CISA paling lambat pada pukul 12.00 siang tanggal 14 Desember 2020 (CISA, 2020). Instruksi penonaktifan total dalam tempo kurang dari 24 jam ini menunjukkan kalkulasi rasional yang menempatkan keamanan data nasional sebagai prioritas utama di atas ketersediaan layanan operasional, sekaligus menandai respons taktis pertama untuk memutus akses aktor negara asing sebelum kerusakan sistemik meluas.

Meskipun instruksi mitigasi diberlakukan secara menyeluruh, dampak intrusi aktual yang berhasil dilakukan oleh aktor ancaman terkonsentrasi pada target bernilai tinggi. Dari sekitar 18.000 entitas yang mengunduh pembaruan berbahaya tersebut terkonfirmasi bahwa kurang dari 100 entitas yang diintrusi lebih lanjut oleh pelaku serangan, investigasi lanjutan mengonfirmasi bahwa aktor ancaman hanya melakukan eskalasi serangan lanjutan terhadap sembilan lembaga federal utama (The White House, 2021). Dampak terhadap lembaga-lembaga ini bukan sekadar gangguan teknis, melainkan terjadinya pencurian data intelijen dan komunikasi sensitif yang memaksa pemerintah Amerika Serikat melakukan evaluasi ulang secara menyeluruh terhadap postur keamanan siber nasional mereka.

2.4.3. Dampak Peretasan Terhadap Citra Amerika Serikat

Peretasan SolarWinds menimbulkan dampak signifikan terhadap citra Amerika Serikat sebagai pemimpin keamanan siber global karena menunjukkan bahwa infrastruktur digital pemerintahan dan sektor swasta Amerika Serikat dapat dibobol pada skala besar. Serangan siber yang mencapai perangkat lunak, digunakan oleh ribuan organisasi dan mengenai berbagai lembaga federal, sehingga menimbulkan keraguan publik dan internasional terhadap klaim Amerika Serikat tentang kemampuan proteksi sibernya (U.S. GAO, 2022). Pernyataan resmi pemerintahan Amerika Serikat yang mengaitkan serangan siber kepada Badan Intelijen Asing Rusia (SVR), dimana langkah-langkah pembalasan politik dinilai hanya untuk menutup kekosongan kepercayaan (The White House, 2021). Akibatnya, insiden ini melemahkan narasi tentang keunggulan siber Amerika

Serikat dan menempatkan kredibilitas kebijakan keamanan siber Amerika Serikat pada ujian internasional.

Publikasi dan liputan media internasional memperkuat persepsi bahwa Amerika Serikat rentan terhadap serangan siber, sehingga menciptakan tekanan diplomatik yang nyata terhadap Washington untuk menjelaskan tindakan dan meningkatkan keamanan bersama sekutu. Saran teknis gabungan NSA, CISA dan FBI serta rilis formal pemerintahan memaparkan bukti teknis dan daftar indikator peretasan, tetapi publikasi tersebut juga menyoroti lamanya waktu deteksi serangan yang memberi sudut pandang negatif dalam penilaian dunia terhadap efektivitas pengawasan Amerika Serikat (NSA, CISA, & FBI, 2021). Dengan demikian, dampak media ini tidak hanya menjatuhkan reputasi tetapi juga merambat ke ranah hubungan diplomatik dan pembentukan norma internasional.

Dampak pada *soft power* Amerika Serikat juga terlihat melalui bagaimana publik baik domestik dan asing menilai legitimasi kebijakan luar negeri Amerika Serikat di ranah digital, khususnya ketika pemerintah harus memilih antara menetapkan pelaku secepatnya atau menunggu bukti kuat. Penelitian tentang opini publik menunjukkan bahwa tingkat kepastian pelaku dalam serangan ini mempengaruhi dukungan publik untuk respons negara, ketika kepastian pelaku tidak meyakinkan, dukungan untuk tindakan keras menurun, hal ini berdampak pada kemampuan pemerintahan Amerika Serikat untuk melegitimasi tindakan dalam menuntut tanggung jawab internasional (Jardine et al., 2024). Kombinasi antara sorotan media, keterlambatan deteksi, dan perdebatan pelaku serangan kemudian mengurangi ruang manuver diplomatik Amerika Serikat dalam

mendorong norma perilaku negara lain di dunia maya. Singkatnya, kerentanan domestik yang terekspos mengurangi daya tarik normative kepemimpinan Amerika Serikat dalam isu siber.

Meskipun liputan media internasional menyoroti kelemahan deteksi, secara operasional respons teknis pemerintah Amerika Serikat terhadap pengungkapan SolarWinds justru berlangsung sangat cepat. Pada hari yang sama ketika serangan terhadap jaringan Orion diumumkan, CISA segera mengeluarkan *Emergency Directive 21-01* yang mewajibkan seluruh lembaga federal memutus koneksi sistem Orion dan melakukan audit keamanan menyeluruh (CISA, 2020). Tiga hari kemudian, pemerintah membentuk *Unified Coordination Group* yang melibatkan CISA, FBI, NSA, dan ODNI untuk mengkoordinasikan investigasi dan mitigasi nasional, dimana hal tersebut menunjukkan mobilisasi antarlembaga yang cepat setelah insiden terungkap (U.S. GAO, 2022). Deretan tindakan cepat ini menunjukkan bahwa meskipun proses identifikasi pelaku serangan dan langkah diplomatik memerlukan waktu lebih lama, mitigasi teknis dan respons awal terhadap insiden berjalan responsif. Dengan demikian, terdapat perbedaan jelas antara kelemahan deteksi sebelum insiden terungkap dan efektivitas reaksi teknis pemerintah setelah penyusupan terhadap berbagai lembaga Amerika Serikat diketahui secara publik.

Secara domestik, insiden SolarWinds memicu kritik politik dan pengawasan kongres yang memperbesar narasi kegagalan pengawasan dan akuntabilitas, sehingga mempengaruhi persepsi lembaga pemerintahan Amerika Serikat di mata publik internasional. Kongres mengadakan dengar pendapat dan

kajian legislatif atas keamanan rantai pasok perangkat lunak, dan GAO menyoroti kebutuhan perbaikan respons federal, tindakan-tindakan ini memperlihatkan bahwa sistem pemerintahan bergerak untuk memperbaiki diri, namun juga menegaskan adanya celah yang sebelumnya tersembunyi (U.S. GAO, 2022; U.S. Congress, 2021). Reaksi kebijakan seperti penguatan standar keamanan rantai pasok dan EO terkait sanksi terhadap aktor asing menunjukkan upaya mitigasi reputasi, tetapi pemulihan kepercayaan memerlukan waktu dan bukti perubahan nyata (The White House, 2021). Dengan demikian, konsekuensi politik dalam negeri berkontribusi pada bagaiman citra Amerika Serikat dipandang dalam jangka menengah oleh audiens global.

Akhirnya, implikasi jangka panjang bagi citra Amerika Serikat memiliki berbagai dampak, meskipun serangan terhadap SolarWinds merusak klaim keunggulan teknis dan pengawasan, respons kebijakan dan kolaborasi teknis yang diikuti memberikan peluang untuk mengembalikan kredibilitas jika dijalankan transparan dan efektif. Pemerintah Amerika Serikat telah mengeluarkan *advisory*, sanksi, dan inisiasi kebijakan untuk memperkuat keamanan rantai pasok perangkat lunak sebagai langkah yang diperlukan untuk memperbaiki citra (The White House, 2021; NSA, CISA, & FBI, 2021). Namun literatur kebijakan menekankan bahwa pemulihan citra bergantung pada kemampuan Amerika Serikat menunjukkan reformasi nyata, meningkatkan kerja sama internasional, serta membangun mekanisme transparan untuk atribusi dan akuntabilitas (Willett, 2021; Coco et al., 2022). Oleh karena itu, insiden SolarWinds menjadi katalisator

perubahan kebijakan sekaligus pengingat bahwa kredibilitas global di ranah siber harus terus dibuktikan lewat tindakan dan konsistensi kebijakan.