BAB IV

KESIMPULAN

4.1. Kesimpulan

Penelitian ini bertujuan menganalisis bagaimana Amerika Serikat merespons peretasan terhadap SolarWinds yang dilakukan oleh kelompok APT 29 melalui lensa *Rational Actor Model* (RAM) dan strategi *cyber deterrence*. Berdasarkan analisis dokumen resmi, laporan teknis, dan literatur, ditemukan bahwa respons Pemerintah Amerika Serikat dapat dipahami sebagai hasil perhitungan rasional yang menimbang biaya dan manfaat serta meminimalkan risiko eskalasi militer. Keputusan preferensi respon yang diambil menempatkan prioritas pada pemulihan fungsi pemerintahan dan keamanan nasional, pemulihan kepercayaan publik dan sektor swasta, serta menjaga posisi normatif Amerika Serikat dalam tata kelola siber internasional.

Implementasi dari pilihan rasional Amerika Serikat setelah insiden SolarWinds terwujud dalam pengerahan strategi *cyber deterrence* yang berlapis dan terintegrasi. Pada pilar *deterrence by punishment*, kalkulasi rasional tersebut dilakukan melalui instrumen proyeksi kekuatan proaktif dan pembebanan biaya ekonomi. Amerika Serikat merespons kerentanan dengan meningkatkan agresivitas kebijakan *defend forward*. Hal ini dibuktikan dengan peningkatan pendanaan operasional siber DoD yang terus meningkat secara signifikan untuk ranah siber, serta eskalasi operasi *hunt forward* pada tahun 2023 yang mencatatkan peningkatan frekuensi misi lebih dari 300% dan perluasan jangkauan

jaringan operasi hingga 650%. Peningkatan ini menegaskan bahwa Amerika Serikat secara sadar memilih proyeksi kekuatan proaktif sebagai respons paling rasional untuk mencegah ancaman langsung di titik asalnya. Meskipun perluasan operasi ini bukan murni sebagai serangan balasan langsung terhadap Rusia, insiden SolarWinds memantik Amerika Serikat untuk lebih ketat menerapkan kebijakan *defend forward* tersebut.

Di saat yang sama, pembebanan biaya secara langsung dilakukan melalui penerbitan Executive Order 14024. Kebijakan ini menghukum Rusia secara nyata melalui pembekuan aset perusahaan teknologi, pelarangan entitas Amerika Serikat untuk berpartisipasi di pasar surat utang Rusia, serta pengusiran 10 diplomat. Keputusan ini secara rasional dirancang untuk menciptakan isolasi finansial dan politik yang menekan ruang gerak strategis Rusia. Sementara itu, untuk melengkapi instrumen ofensif tersebut, Amerika Serikat menerapkan *deterrence by denial* melalui reformasi fundamental terhadap arsitektur keamanan siber domestiknya. Melalui Executive Order 14028, Amerika Serikat menerapkan adopsi *Zero Trust Architecture* dan meningkatkan standar transparansi melalui kewajiban Software Bill of Materials (SBOM). Langkah ini merupakan kalkulasi defensif untuk menutup celah keamanan, sekaligus mencegah serangan musuh dengan cara mempersulit eksploitasi serupa di masa depan.

Lebih jauh lagi, Amerika Serikat menyadari bahwa respons bilateral dan domestik tidak akan cukup untuk membendung ancaman siber berskala global. Oleh karena itu, rasionalitas strategis ini diperluas dampaknya melalui penerapan *deterrence by entanglement* dan *deterrence by norms*. Dengan memobilisasi j*oint*

attribution bersama aliansi Five Eyes dan NATO, Amerika Serikat berhasil menginternasionalisasi isu siber ini dengan mengubahnya dari sekadar konflik bilateral menjadi ancaman keamanan kolektif yang menjerat Rusia dalam tekanan geopolitik blok Barat secara keseluruhan. Langkah integratif ini tidak hanya mengisolasi Rusia, tetapi juga secara aktif menegakkan kembali norma internasional yang mengecam keras eksploitasi terhadap infrastruktur sipil. Pada akhirnya, keseluruhan respons terkoordinasi ini menempatkan Amerika Serikat kembali sebagai pemimpin dalam tata kelola keamanan siber global dan penjaga stabilitas tatanan internasional di era digital.

Secara teoritis, temuan pada penelitian ini memperkuat kelayakan penggunaan RAM dalam menganalisis pengambilan keputusan negara pada insiden siber yang kompleks dengan menyadari bahwa keputusan tersebut tetap dipengaruhi koordinasi antar lembaga dan keterbatasan informasi publik. Selain itu, penerapan kerangka *cyber deterrence* menjelaskan mengapa kombinasi *denial, punishment, entanglement, dan norms* menjadi pilihan rasional, dimana masing-masing instrumen menutup celah berbeda dalam menghadapi ancaman. Namun penelitian ini juga menemukan keterbatasan penting, yaitu kesulitan mengukur besaran kerugian sebenarnya karena adanya bukti yang terklasifikasi dan keterbatasan data publik, sehingga analisis dampak ketidakpastian secara pasti.

4.2. Saran untuk Penelitian Selanjutnya

Berdasarkan temuan dan batasan dalam penelitian ini, terdapat beberapa aspek yang dapat dikembangkan untuk penelitian masa depan. Pertama, penelitian selanjutnya disarankan untuk mengkaji efektivitas dari berbagai preferensi yang diterapkan Amerika Serikat, dengan melihat apakah instrumen *deterrence* tersebut benar-benar berhasil mengubah perilaku Rusia atau justru memicu evolusi taktik serangan siber yang lebih canggih. Kedua, melihat serangan SolarWinds bermula dari sektor swasta, penelitian mendatang dapat mengeksplorasi peran aktor non-negara, seperti perusahaan teknologi multinasional, dalam diplomasi siber dan mekanisme pertahanan negara. Kemudian terakhir, studi komparatif antara respons terhadap SolarWinds dan insiden siber besar lainnya seperti *Ransomware* Colonial Pipeline pada tahun 2021 dengan tipe serangan siber yang berbeda akan sangat bermanfaat untuk memetakan konsistensi dan adaptabilitas strategi keamanan siber Amerika Serikat dalam menghadapi berbagai tipe ancaman.