BAB II

TINJAUAN PUSTAKA

2.1.Tinjauan Literatur

Pada penelitian ini, penulis akan mengaitkan dengan beberapa penelitian/karya ilmiah terdahulu yang kredible untuk mengidentifikasi berbagai hubungan pengetahuan pada topik yang dibahas dalam penelitian terdahulu dengan penelitian penulis, serta untuk mencari kesenjangan dari penelitian terdahulu dengan penelitian penulis. Hal tersebut dilakukan untuk mencari orisinalitas pada penelitian penulis dengan penelitian-penelitian lainnya. Adapun penelitian yang penulis maksud adalah sebagai berikut:

1. ***Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks*** **(2023)**

Karya ilmiah ini berfokus pada peningkatan keamanan siber dalam skala global dengan cara mengembangkan dan mengadapatasi norma-norma dan standar internasional. Hal ini karena norma internasional esensial untuk membangun pemahaman umum terkait serangan siber dan mendorong kolaborasi antar negara dalam menangani masalah tersebut. Penulis dalam karya ilmiah ini berpendapat bahwa peningkatan kerja sama internasional yang menghasilkan pembentukan perjanjian dan kerangka kerja merupakan cara paling jitu dalam menanggapi keamanan siber beserta ancamannya. Selain itu, penulis juga berpendapat bahwa

dengan adanya perjanjian dapat memberikan dasar hukum untuk kerja sama serta membangun kepercayaan dengan negara-negara yang terlibat, sehingga dapat menghasilkan keputusan-keputusan keamanan siber yang efektif. (Francis, 2023)

2. *Illegal: The SolarWinds Hack under International Law* (2022)

Karya ilmiah yang ditulis oleh Antonio Coco, Talita Dias, dan Tsvetelina van Benthem berfokus pada analisis terkait serangan siber SolarWinds melalui kacamata hukum internasional secara komprehensif. Penulis pada penelitian ini berpendapat bahwa peretasan yang terjadi kepada SolarWinds merupakan tindakan pelanggaran hukum internasional yang berlaku. Adapun hukum internasional yang telah dilanggar yaitu terkait prinsip-prinsip kedaulatan, non-intervensi, dan hukum hak asasi manusia. Karya ilmiah ini berpendapat bahwa peretasan SolarWinds telah melanggar hukum-hukum tersebut. Selain itu, karya ilmiah ini juga berasumsi bahwa ketiadaan fungsionalitas infrastruktur siber merupakan pelanggaran kedaulatan. Hal ini mencakup pelanggaran integritas teritorial dalam konteks operasi siber. Karya ilmiah ini juga menyinggung soal norma internasional dalam PBB sebagai tanggung jawab negara dan pihak lain yang bersangkutan, seperti menjaga integritas rantai pasokan teknologi informasi serta mencegah dan memperbaiki kerugian yang disebabkan oleh Nobelium. Kesimpulan pada karya ilmiah ini adalah peretasan SolarWinds merupakan tindakan yang ilegal di berbagai bidang, serta diperlukan penguatan analisis hukum untuk memecahkan masalah serangan siber dalam konteks hukum internasional.(Coco et al., 2022)

3. *Not Illegal: The SolarWinds Incident and International Law* (2022)

Karya ilmiah yang ditulis oleh Kristen E. Eichensehr berfokus pada analisis terkait kompleksitas dan ketidakmungkinan implementasi hukum internasional dalam konteks serangan siber dan aktivitas negara di dunia maya. Secara garis besar, karya ilmiah ini berpendapat bahwa peretasan SolarWinds sebagai perantara spionase ke AS belum dapat diklasifikasikan sebagai bentuk pelanggaran hukum internasional. Ini karena minimnya regulasi terkait kegiatan espionase serta tidak ada larangan kegiatan espionase dalam hukum internasional secara eksplisit. Karya ilmiah ini menegaskan bahwa kegiatan espionase oleh Rusia ke AS dan sebaliknya adalah hal yang lumrah terjadi dalam politik internasional, sehingga penulis mengasumsikan kegiatan espionase bisa dikatakan masih legal. Selain itu, karya ilmiah ini juga menekankan pentingnya peran negara dan *opinio juris* (kewajiban subjektif negara yang terlindung oleh hukum) dalam menentukan hukum adat internasional. Hal tersebut karena tidak adanya negara yang menganggap peretasan SolarWinds adalah pelanggaran hukum internasional, sehingga ini menjadi cerminan dari kompleksitas norma hukum internasional di dunia maya. Karya ilmiah ini berpendapat bahwa dibutuhkan partisipasi antar negara dan para ahli dalam merumuskan standar hukum internasional yang jelas di forum internasional, serta dibutuhkan kelengkapan kerangka hukum yang signifikan untuk mengatasi masalah aktivitas negara di dunia maya.(Eichensehr, 2022)

4. ***Cyber Conflict and International Relations: A Comprehensive Analysis of Cyber Deterrence Strategies in Contemporary Geopolitics*** **(2024)**

Karya ilmiah ini berfokus pada mengeksplorasi serta menganalisis secara komprehensif terkait kesenjangan pada implikasi keamanan siber, konflik siber,

dan pencegahan serangan siber. Penulis pada karya ilmiah ini berpendapat bahwa diperlukan analisis multidisiplin, yaitu dengan menggabungkan pengetahuan keamanan siber secara teknis dengan teori-teori hubungan internasional. Hal ini sangat penting untuk memahami keamanan siber karena dapat menciptakan pandangan serta sudut pandang yang lebih komprehensif terkait tantangan dan strategi-strategi keamanan siber. Selain itu, karya ilmiah ini juga mencakup beberapa peristiwa historis yang bersangkutan seperti peristiwa SolarWinds 2020, WannaCry 2017, dan lain-lain. Hal ini dimaksud untuk memberikan gambaran-gambaran terkait peristiwa serangan siber dengan dibalut oleh perspektif akademis yang luas serta analisis komprehensif, sehingga memperluas pemahamanan terkait keamanan siber secara kompleks. Tidak hanya itu, karya ilmiah ini juga menyatakan bahwa diperlukan kerangka kerja kompleks untuk penelitian di masa depan, mendorong dialog tentang strategi keamanan siber di antara pelaku yang bersangkutan, dan implementasi pemeriksaan terhadap efektivitas dan tantangan strategi pencegahan siber di masa kontemporer.(Negrea Petru-Cristian, 2024)

5. ***The Federal Acquisition Supply Chain Act, The SolarWinds Cyber-Attack, and What Might Have Been Different Had FASCA Been Federal Law at the Time of the Attack*** **(2022)**

Karya ilmiah yang ditulis oleh Donald L. Buresh berfokus pada penelitian undang-undang AS tentang *Federal Acquisition Supply Chain Act* (FASCA) dan potensi dampaknya jika diberlakukan ketika peristiwa SolarWinds terjadi. FASCA diratifikasi menjadi undang-undang pada 21 Desember 2018 untuk meningkatkan keamanan rantai pasokan di setiap lembaga federal AS dengan melakukan

pendekatan terkoordinasi untuk mengelola risiko yang terkait dengan teknologi informasi dan alat telekomunikasi yang digunakan oleh pemerintah. Penulis berpendapat bahwa jika FASCA diberlakukan pada saat serangan SolarWinds, maka respons dari lembaga yang terdampak akan sangat berbeda. Hal ini karena struktur birokrasi yang ada dalam FASCA akan memperkenalkan susunan secara kompleks yang memungkinkan dapat menyebabkan penundaan dalam mengatasi ancaman siber. Selain itu, karya ilmiah ini juga menyatakan bahwa proses birokrasi tanpa FASCA memungkinkan menghambat tindakan tepat waktu serta berpotensi konsekuensi yang buruk dari peristiwa SolarWinds. Penulis berpendapat bahwa konsekuensi yang terjadi akibat serangan SolarWinds kemungkinan akan berbeda dari konsekuensi apabila FASCA diproyeksikan, hal ini karena respon FASCA cenderung lebih administratif daripada legislatif. Singkatnya, FASCA memberikan ketegasan dalam proses birokrasi serta memberikan balasan yang cepat terhadap ancaman keamanan rantai pasokan dan keamanan siber.(Buresh, 2022)

6. *On SolarWinds Orion Platform Security Breach* (2021)

Karya ilmiah yang ditulis oleh Lindsay Sterle dan Suman Bhunia berfokus pada rekomendasi terkait usulan-usulan yang harus dilakukan negara untuk menyelesaikan masalah serangan siber SolarWinds 2020. Karya ilmiah ini menekankan perlunya organisasi negara yang mengedepankan pendekatan proaktif daripada reaktif terhadap keamanan siber. Pendekatan proaktif yang dimaksud yaitu menekankan pentingnya pencegahan dan peningkatan berkelanjutan dalam strategi-strategi keamanan siber. Selain itu, karya ilmiah ini juga menyoroti pentingnya mengembangkan strategi yang efektif untuk mencegah serangan siber

di masa depan, mengadvokasi undang-undang *federal disclosure* untuk memperkuat transparansi serta pembelajaran kolektif dalam ranah keamanan siber.(Sterle & Bhunia, 2021)

7. ***The SolarWinds Hacks: Lessons for International Humanitarian Organizations*** **(2022)**

Karya ilmiah yang ditulis oleh Massimo Marelli berfokus pada analisis komprehensif terkait implikasi serangan SolarWinds terhadap organisasi kemanusiaan serta kompleksitas keamanan siber bagi operasi organisasi kemanusiaan. Karya ilmiah ini memberikan perspektif kemanusiaan yaitu tentang "kedaulatan data" dan "kedaulatan digital" dalam pembahasan peristiwa SolarWinds. Hal ini yaitu dengan menekankan pentingnya organisasi kemanusiaan untuk menavigasi berbagai masalah keamanan siber sembari menjalankan prinsip-prinsip kemanusiaan yang baik. Selain itu, karya ilmiah ini juga mengedepankan pendekatan proaktif sebagai strategi dalam menghadapi serangan siber, terutama pada sektor yang menangani data sensitif seperti pekerjaan kemanusiaan. Penulis berpendapat bahwa peristiwa SolarWinds telah melanggar prinsip-prinsip kemanusiaan. Penulis menyoroti beberapa contoh pelanggaran tersebut, seperti pelanggaran pada jaringan Restoring Family Links dan Gerakan Palang Merah Internasional yang merasakan dampak serangan siber tersebut. Karya ilmiah ini juga menyoroti betapa pentingnya operasi organisasi kemanusiaan di dalam dunia maya, seperti mempertahankan prinsip-prinsip kemanusiaan di dunia maya.(Marelli, 2022)

8. ***SolarWinds Software Supply Chain Security: Better Protection with Enforced Policies and Technologies*** **(2022)**

Karya ilmiah yang ditulis oleh Jeong Yang dkk berfokus pada signifikansi keamanan siber terhadap interaksi antara insentif pasar (rantai pasokan) dan praktik keamanan. Penulis berpendapat bahwa pendekatan keamanan 'reduksi' seperti perangkat lunak antivirus dan sistem pencegahan peretasan untuk meningkatkan keamanan secara keseluruhan berpotensi menciptakan kerentanan baru. Penulis berargumen bahwa dibutuhkan transformasi keamanan 'reduksi' yang mampu menekankan penghapusan layanan dan fitur yang tidak penting untuk meminimalisir permukaan serangan, sehingga diperlukan pendekatan yang lebih efisen untuk mencegah serangan siber. Selain itu, karya ilmiah ini juga menekankan pentingnya strategi-strategi keamanan jangka panjang dalam kerangka operasional perusahaan SolarWinds. Penulis berargumen bahwa dibutuhkan perubahan pendekatan dalam bagaimana keamanan dinilai dalam industri perangkat lunak. Selain itu, karya ilmiah ini juga menegaskan pentingnya peningkatan keamanan rantai pasokan perangkat lunak melalui peningkatan kebijakan dan teknologi dalam perusahaan SolarWinds. Contohnya adalah advokasi kebijakan sebagai tanggung jawab apabila terjadinya pelanggaran atas praktik keamanan yang gagal.(Yang et al., 2022)

9. ***Assessing Security Risks of Software Supply Chains Using Software Bill of Materials*** **(2024)**

Karya ilmiah yang ditulis oleh Eric O'Donoghue dkk berfokus pada pentingnya penggunaan teknologi Software Bill of Materials (SBOM) sebagai alternatif baru dalam keamanan rantai pasokan perangkat lunak. Karya ilmiah ini menyoroti Perintah Eksekutif Amerika Serikat 14028 tentang perangkat SBOM sebagai teknologi yang memadai untuk meningkatkan keamanan siber di seluruh rantai pasokan perangkat lunak. SBOM adalah inventarisasi seluruh komponen seperti perpustakaan pihak ketiga, artefak, lisensi, dan skrip yang membentuk aplikasi perangkat lunak, dalam hal ini SBOM memberikan transparansi ke semua bagian penyusun perangkat lunak. Penulis berpendapat bahwa dengan perangkat SBOM dapat memberikan pengetahuan yang lebih luas terkait risiko keamanan rantai pasokan perangkat lunak pihak ketiga.(O'Donoghue et al., 2024)

10. *Disclosure of Software Supply Chain Risks* (2022)

Karya ilmiah yang ditulis oleh Sasha Romanosky dan Jonathan W. Welburn berfokus pada pembahasan tentang meningkatnya ketergantungan pada perangkat lunak dalam mengelola layanan perusahaan serta pemerintah beserta risiko ketergantungan tersebut. Serangan SolarWinds mengeksploitasi kerentanan pada komponen perangkat lunak pihak ketiga, sehingga terciptanya ketergantungan pada perangkat tersebut. Penulis berargumen bahwa diperlukan peningkatan proteksi dan langkah-langkah keamanan dalam rantai pasokan perangkat lunak untuk melindungi data perusahaan dan pemerintah. Selain itu, karya ilmiah ini juga menyoroti pentingnya gerakan/pendekatan proaktif dalam menanggulangi serta mengurangi kerentanan yang melekat dalam rantai pasokan perangkat lunak,

sehingga memberikan keamanan rantai pasokan yang lebih aman dan kuat.(Romanosky & Welburn, 2022)

Secara singkat, seluruh tinjauan literatur di atas dapat diketahui persamaan serta perbedaannya dengan penelitian penulis dalam bentuk tabel yaitu sebagai berikut:

Tabel 2.1 Tinjauan Literatur

No.	Judul	Penulis	Persamaan	Perbedaan
1.	*Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks*	Callistus Francis	Salah satu inti pembahasan pada karya ilmiah ini adalah menekankan pentingnya kerja sama internasional dalam menangani isu keamanan siber beserta ancaman serangan siber.	Fokus karya ilmiah ini adalah analisis komprehensif mengenai keselarasan isu keamanan siber dengan konflik internasional, terutama mengenai serangan siber yang disponsori negara.
2.	*Illegal: The SolarWinds Hack under International Law*	Coco Antonio, Talita Dias,	Karya ilmiah ini menyoroti negara sebagai aktor utama, dimana	Fokus karya ilmiah ini adalah analisis komprehensif terkait investigasi

		Tsvetelina Van Benthem	negara yang bersangkutan (kedua belah pihak) akan serangan siber SolarWinds bertanggung jawab atas kerusakan dari serangan tersebut.	serangan siber SolarWinds dalam konteks hukum internasional.
3.	*Not Illegal: The SolarWinds Incident and International Law*	Kristen E. Eichenseher	Karya ilmiah ini menegaskan bahwa dibutuhkan kolaborasi antar negara dalam menghadapi isu keamanan siber beserta ancamannya.	Fokus karya ilmiah ini adalah analisis terkait kompleksitas implementasi hukum internasional terhadap serangan siber SolarWinds.
4.	*Cyber Conflict and International Relations: A Comprehensive Analysis of Cyber Deterrence*	Negrea Petru-Cristian	Karya ilmiah ini menyatakan bahwa pendekatan hubungan internasional menjadi salah satu	Fokus karya ilmiah ini adalah analisis komprehensif tentang kesenjangan implikasi pada

	Strategies in Contemporary Geopolitics		komponen penting dalam membahas isu keamanan siber.	keamanan siber, serangan siber, dan pencegahan serangan siber dalam studi hubungan internasional.
5.	*The Federal Acquisition Supply Chain Act, the SolarWinds Cyber-Attack, and What Might Have Been Different Had FASCA Been Federal Law at the Time of the Attack*	Donald L. Buresh	Karya ilmiah ini menyoroti peran pemerintah Amerika Serikat dalam membentuk kebijakan/undang-undang terkait keamanan siber serta implikasi keamanan rantai pasokan di dunia maya.	Fokus karya ilmiah ini adalah analisis potensi undang-undang FASCA apabila masih berlaku ketika serangan siber SolarWinds sedang terjadi.
6.	*On SolarWinds Orion Platform Security Breach*	Lindsay Sterle, Suman Bhunia	Karya ilmiah ini menjelaskan pentingnya mereformasi	Fokus karya ilmiah ini adalah mengidentifikasi berbagai usulan

			kebijakan-kebijakan negara mengenai isu keamanan siber yang harus bersifat proaktif.	terkait langkah-langkah yang harus dilakukan negara dalam menghadapi isu keamanan siber
7.	*The SolarWinds Hack: Lessons for International Humanitarian Organizations*	Massimo Marelli	Karya ilmiah ini merekomendasikan strategi-strategi pemerintah negara yang bersifat proaktif dalam menghadapi isu keamanan siber.	Fokus karya ilmiah ini adalah analisis komprehensif mengenai implikasi serangan siber SolarWinds terhadap organisasi kemanusiaan.
8.	*SolarWinds Software Supply Chain Security: Better Protection with Enforced Policies and Technologies*	Jeong Yang, Young Lee, Arlen P. McDonald	Tidak ada persamaan pada karya ilmiah ini.	Fokus karya ilmiah ini adalah analisis terkait signifikansi keamanan siber terhadap interaksi antara insentif pasar (rantai pasokan) dan praktik keamanan.

9.	*Assessing Security Risks of Software Supply Chains Using Software Bill of Materials*	Eric O'Donoghue, Ann Marie Reinhold, Clemente Izurieta	Tidak ada persamaan pada karya ilmiah ini	Fokus karya ilmiah ini adalah analisis tentang penggunaan teknologi Software Bill of Materials (SBOM) sebagai alternatif baru dalam keamanan rantai pasokan perangkat lunak.
10.	*Disclosure of Software Supply Chain Risks*	Sasha Romanosky, Jonathan W. Welburn	Karya ilmiah ini merekomendasi langkah-langkah pemerintah negara yang bersifat proaktif dalam menghadapi isu serangan siber	Fokus karya ilmiah ini adalah pembahasan tentang meningkatnya ketergantungan pada perangkat lunak dalam mengelola layanan perusahaan dan pemerintah juga risiko

				ketergantungan tersebut.

Semua tinjauan literatur di atas dapat diketahui kesimpulannya bahwa terdapat banyak komponen yang saling keterhubungan satu sama lain, sehingga menciptakan kompleksitas dalam mempelajari isu keamanan siber serta keamanan rantai pasokan di *cyberspace*. Maka, untuk mencari kesenjangan/*gap* serta relevansi isu keamanan siber dalam studi ilmu hubungan internasional, penulis memfokuskan penelitiannya pada peran pemerintah Amerika Serikat dalam menghadapi serangan siber terhadap Pentagon AS oleh Rusia tahun 2020-2021.

2.2.Kerangka Teoritis/Konseptual

2.2.1. Teori Liberalisme

Liberalisme merupakan salah satu teori yang mendasari munculnya ilmu hubungan internasional (Jackson & Sorensen, 2013). Secara etimologis, istilah 'liberalisme' berasal dari bahasa Latin yaitu '*liber*' yang artinya 'bebas' atau 'merdeka'. Istilah liberalisme melekat dengan konsep manusia merdeka, baik merdeka sejak lahir maupun merdeka dari status perbudakan (Noersaleha, 2017). Liberalisme merupakan teori yang mengedepankan nilai dasar kebebasan individu, hak asasi manusia, kesetaraan hak bagi semua manusia, mengedepankan rasionalitas, dan moral. Ideologi/teori liberalisme memiliki tiga asumsi dasar, di antaranya: a) percaya terhadap kemampuan akal manusia; b) bersifat

kooperatif/kerja sama dibandingkan konfliktual; c) menekankan kebebasan individu (Burchill et al., 2001).

Robert Jackson dan George Sorensen dalam bukunya yang berjudul *Pengantar Studi Hubungan Internasional* mengemukakan bahwa terdapat empat aliran utama teori liberalisme. Adapun empat aliran tersebut adalah sebagai berikut:

1. Liberalisme Sosiologi: paham ini menjelaskan bahwa hubungan internasional tidak hanya mempelajari hubungan antara pemerintah, tetapi juga mempelajari hubungan antara individu, kelompok dan aktor non-negara lainnya.
2. Liberalisme Interdependensi: paham ini menyatakan bahwa modernisasi memperluas tingkat interdependensi/saling ketergantungan antara aktor negara dan aktor non-negara menjadi semakin krusial.
3. Liberalisme Institusional: paham ini menyatakan bahwa institusi internasional meningkatkan kerjasama di antara negara-negara dan aktor non-negara. Liberalisme institusional percaya bahwa kehadiran institusi internasional dapat mengurangi masalah yang berkaitan dengan ketidak-percayaan antara aktor negara.
4. Liberalisme Republikan: paham ini menyatakan bahwa negara-negara demokrasi tidak akan berperang satu sama lain (Jackson & Sorensen, 2013).

Melihat keempat aliran liberalisme di atas, maka teori liberalisme mendeskripsikan hubungan internasional sebagai arena dimana semua aktor negara

dan aktor non-negara saling berinteraksi satu sama lain. Berbeda dengan teori realisme yang menganggap negara sebagai satu-satunya aktor hubungan internasional, liberalisme melihat semua aktor non-negara juga memiliki peran krusial dalam kancah politik global. Perspektif liberalisme tidak meyakini aliran realisme bahwa negara adalah di atas semuanya dalam hubungan internasional. Perspektif liberalisme meyakini realita pentingnya kehadiran negara dalam sistem internasional, namun aktor individu/kelompok adalah kunci dalam hubungan internasional. Dengan demikian, fokus utama liberalisme adalah menempatkan pada aksi dan kepentingan individu/kelompok yang dapat diwujudkan dalam aksi dan kepentingan negara (Dugis, 2016).

Teori liberalisme meyakini bahwa di dalam sistem internasional yang bersifat anarki, kerjasama merupakan cara terbaik menuju terlaksananya kepentingan bersama. Liberalisme mengungkapkan bahwa dibutuhkan kehadiran organisasi-organisasi, baik di tingkat regional maupun tingkat internasional. Organisasi international menurut perspektif liberalisme adalah dapat membuat kerjasama antar aktor negara dan non-negara menjadi lebih mudah. Selain itu, perspektif liberalisme percaya bahwa kerjasama internasional juga dapat dilakukan melalui berbagai instrumen aturan yang dibuat untuk mengatur tindakan negara dalam hal tertentu. Maka dari itu, teori liberalisme meyakini bahwa organisasi/institusi internasional dapat membantu meningkatkan kerjasama di antara aktor-aktor negara dan non-negara (Dugis, 2016).

Selain itu, teori liberalisme juga percaya bahwa semakin tinggi level institusionalisasi yang terjadi dalam hubungan internasional, maka semakin

signifikan situasi ini dapat mengurangi efek kerusuhan yang diakibatkan situasi anarki multipolar. Liberalisme menganggap bahwa masalah maupun ketidakpercayaan antar negara dapat terfasilitasi melalui kehadiran institusi internasional. Oleh karena itu, interaksi antar aktor-aktor negara yang bermusuhan melalui institusi internasional yang sah, memungkinkan dapat menghilangkan rasa saling ketidakpercayaan mereka satu sama lain. Dalam hal ini kedaulatan negara tetap terjaga, sementara kerjasama untuk terlaksananya kepentingan bersama juga tetap bisa berjalan (Dugis, 2016).

Visensio Dugis dalam bukunya yang berjudul *Teori Hubungan Internasional Perspektif-Perspektif Klasik* menyoroti fitur hubungan internasional dalam perspektif liberalisme yaitu sebagai berikut.

Tabel 2.2.1 Fitur Hubungan Internasional Menurut Liberalisme

Variabel	Liberalisme
Aktor/unit analisis	Negara & Organisasi Non-negara
Pandangan tentang aktor	Negara terdiri atas berbagai komponen; sebagian beroperasi lintas batas negara
Dinamika perilaku	Keputusan tidak selalu optimal; perundingan, tawar-menawar, kompromi
Isu utama	Bervariasi, isu-ius sosial-ekonomi dan kesejahteraan mendahului keamanan

	nasional
Proses yang berlangsung	Manajemen isu-isu global
Hasil (outcome)	Perilaku berdasarkan aturan di dalam masyarakat yang poliarki
Struktur sistem internasional	Transnasional, banyak pusat kekuatan
Prinsip-prinsip dasar penanda sistem internasional	Saling ketergantungan
Distribusi power dan pengaruh	Relatif terdistribusi secara merata

Sumber: (Dugis, 2016 hal. 68)

Teori liberalisme dalam konteks penelitian penulis adalah bagaimana upaya-upaya yang dilakukan oleh pemerintah Amerika Serikat melalui CISA dalam menanggulangi serangan siber oleh Rusia terhadap perusahaan SolarWinds tahun 2020-2021. Serangan siber kepada perusahaan SolarWinds pada tahun 2020 memberikan dampak yang cukup besar terhadap keamanan nasional dan keamanan siber bagi negara AS dan keamanan aktor swasta lainnya. CISA menyadari secara penuh bahwa di dunia yang saling ketergantungan dan keterhubungan satu sama lain akibat kemajuan teknologi informasi dan telekomunikasi, isu keamanan siber merupakan isu yang dapat berdampak pada semua tingkat aktor HI. Oleh karena itu, CISA melakukan kolaborasi dengan aktor-aktor swasta yang terdampak untuk mengidentifikasi pelaku utama serangan tersebut serta menciptakan pertahanan

siber kolektif kepada negara AS dan mitra-mitranya. Dengan adanya kolaborasi tersebut dapat meningkatkan kepercayaan antar aktor negara dengan aktor non-negara yang bersangkutan. Maka dari itu, berbagai upaya yang dilakukan oleh CISA untuk menanggulangi serangan siber SolarWinds oleh Rusia selaras dengan mazhab teori liberalisme; yaitu melakukan kerjasama antar aktor negara dan non-negara yang bersangkutan terkait penanggulangan dampak serangan siber SolarWinds di dunia yang semakin keterhubungan dan interdependensi satu sama lain akibat kemajuan TIK dan modernisasi.

Selain itu, peran lembaga CISA secara umum juga selaras dengan aliran perspektif liberalisme. Dalam hal ini, CISA International melalui Strategi Global CISA memainkan peran penting dalam hubungan internasional seperti mempromosikan keamanan siber global dan keamanan infrastruktur. Strategi Global CISA mengedepankan kerjasama intensif antar mitra-mitra AS beserta sekutunya terkait peningkatan pertahanan siber kolektif, membentuk ekosistem kebijakan global terkait keamanan siber, memperkuat kolaborasi, melakukan penelitian bersama, dan meningkatkan kerjasama operasional. Dengan adanya kerjasama dengan mitra internasional, CISA mampu melindungi kepentingan domestik dan kepentingan internasional dari ancaman serangan siber dan ancaman keamanan lainnya.

2.2.2. Konsep Keamanan (*Security*)

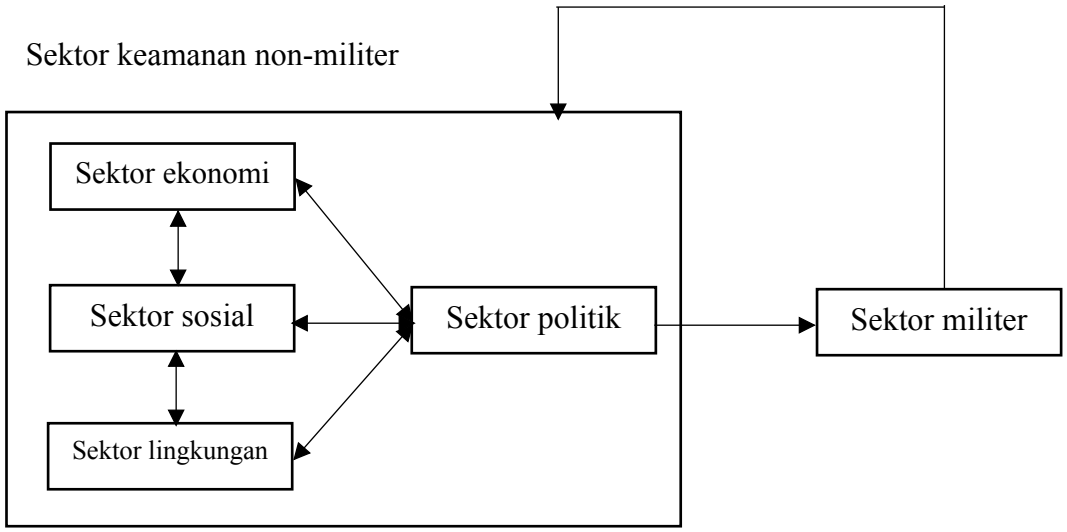
Konsep keamanan secara etimologis berasal dari bahasa latin "*securus*" (*se* + *cura*) yang artinya terbebas dari segala bahaya, terbebas dari segala ancaman dan ketakutan (*free from danger, free from fear*). Istilah 'keamanan' juga dapat diartikan dari gabungan kata *se* (tanpa/*without*) dan *curus* (rasa gelisah/*uneasiness*). Dengan demikian, kata tersebut apabila digabungkan akan bermakna menjadi '*liberation from uneasiness, or a peaceful situation without any risks or threads*' atau 'kebebasan dari kegelisahan atau situasi damai tanpa risiko atau benang merah.'(Perwita, 2008)

Sementara itu, konsep keamanan dalam konteks studi ilmu hubungan internasional merupakan suatu "*contested concept*" yang di mana seiring berjalannya waktu konsep keamanan maknanya selalu berkembang serta ditafsirkan secara berbeda oleh tradisi/perspektif yang berbeda (Adhikari, 2024). Keamanan dalam hubungan internasional memiliki dua tradisi/perspektif utama, di antaranya keamanan tradisional dan keamanan non-tradisional. Keamanan tradisional merupakan suatu kondisi di mana negara beserta masyarakatnya terbebas dari berbagai ancaman militer atau kapabilitas negara dalam melindungi negaranya dari serangan militer yang berasal dari lingkungan eksternal. Keamanan tradisional dipopulerkan oleh berbagai mazhab realisme yang menyatakan bahwa negara merupakan satu-satunya aktor dalam interaksinya di politik atau hubungan internasional. Guna melindungi negara dari ancaman militer negara lain, kapabilitas militer suatu negara untuk mempertahankan diri adalah suatu komponen penting, sehingga kemapanan militer negara menjadi indikator baik atau buruknya suatu keamanan negara (Perwita, 2008).

Sedangkan, konsep keamanan non-tradisional baru dikembangkan sejak awal tahun 1990-an, dalam hal ini definisi "keamanan" dipertanyakan dan diinterpretasikan menjadi beberapa definisi baru. Studi keamanan non-tradisional ini dipopulerkan oleh Barry Buzan (1991), ia berpendapat bahwa konsep keamanan tidak hanya mencakup aspek militer dan aktor negara saja tetapi juga mencakup aspek-aspek non-militer dan aktivitas aktor non-negara lainnya. Buzan (1991) dalam bukunya yang berjudul "*People, States and Fear*" menyatakan bahwa terdapat lima sektor keamanan utama, yaitu: Militer, politik, ekonomi, lingkungan, dan sosial. Buzan dalam bukunya menjelaskan bahwa konsep keamanan merupakan konsep yang lebih luas dan universal meliputi sektor politik, lingkungan, ekonomi, dan sosial baik dari tingkat global, regional, nasional, hingga tingkat individu. Hal ini bukan berarti Buzan mendiskreditkan keamanan militer. Menurut Buzan, keamanan militer merupakan salah satu sektor penting dan saling melengkapi dengan sektor lainnya (Buzan, 1991).

Perwita (2008) memberikan penggambaran terkait keterhubungan sektor militer dengan sektor non-militer dalam berbentuk tabel adalah sebagai berikut:

Tabel 2.2.2 Keterkaitan antara keamanan militer dan non-militer



Sumber: (Perwita, 2008, hal. 6)

Dari tabel di atas, dapat disimpulkan bahwa kelima sektor tersebut saling keterhubungan satu sama lain. Seperti contoh, ketidakstabilan sektor politik dan sektor ekonomi dalam negeri memberikan dampak negatif terhadap sektor militer. Selain itu, keadaan lingkungan eksternal yang sedang berperang juga mempengaruhi kapasitas dan personil militer, untuk meningkatkan kedua hal tersebut dibutuhkan ekonomi yang kuat serta reaksi dan partisipasi sosial.

2.2.3. Keamanan Siber

Kemajuan teknologi informasi dan telekomunikasi (TIK) tidak menutup kemungkinan dapat mempengaruhi dinamika keamanan internasional, baik keamanan bersifat militeristik maupun non-militeristik. Di dunia yang semakin ketergantungan dan keterhubungan karena dampak globalisasi dan kemajuan TIK, kerentanan pada keamanan akan semakin meluas. Berbagai isu tentang dunia siber seperti serangan siber, hacktivisme, spionase, dan lain-lain menjadi perhatian bagi setiap negara. Selain itu, kecanggihan teknologi juga menciptakan suatu dunia baru

yang harus dipertimbangkan pada studi ilmu hubungan internasional, yaitu dunia maya atau *cyberspace*. Dunia maya/*cyberspace* dewasa ini telah menjadi ruang kontestasi politik seperti kepentingan politik, propaganda, dan lain sebagainya. Maka dari itu, dunia siber tidak hanya menjadi perhatian para ahli teknologi informasi saja, tetapi juga menjadi perhatian bagi para pemerintah negara di seluruh dunia (Barrinha & Renard, 2017).

Konsep keamanan siber menurut Joseph Nye mengacu pada *cyberspace* sebagai subjek utamanya. Nye mengatakan bahwa *cyberspace* merupakan "bumi" dari dunia maya yang di dalamnya terdapat keamanan siber. Selanjutnya, Nye berpendapat bahwa: "*Domain siber adalah lingkungan buatan manusia yang kompleks. Tidak seperti atom, musuh manusia memiliki tujuan dan kecerdasan. Gunung dan lautan sulit untuk dipindahkan, tetapi bagian dari dunia maya dapat dihidupkan dan dimatikan dengan menekan tombol. Lebih murah dan lebih cepat untuk memindahkan elektron melintasi dunia daripada memindahkan kapal besar jarak jauh melalui lautan*."(Nye, 2010)

Keamanan siber dalam konteks studi ilmu hubungan internasional menurut Valeriano dan Maness merupakan teknologi komputerisasi yang kemungkinan berpotensi mengancam keamanan siber dalam hubungan internasional. Pada masa kontemporer, instrumen TIK telah melekat pada setiap aktivitas-aktivitas hubungan internasional, seperti aktivitas kenegaraan, organisasi internasional, perusahaan, hingga pada tingkat individu. Dengan demikian, segala bentuk kejahatan/serangan siber berdampak pada stabilitas keamanan bagi aktor-aktor hubungan internasional (Valeriano & Maness, 2018).

Selain itu, keamanan siber dalam konteks hubungan internasional menurut Myriam Dunn Cavelty mengacu pada lingkungan bioelektrik (*bioelectric environment*) atau *cyberspace*. Cavelty menyatakan bahwa keamanan siber dalam hubungan internasional merupakan *bioelectric environment* yang aman dari serangan, kerusakan, pencurian, dan potensi ancaman lainnya Untuk menciptakan keamanan tersebut negara memainkan peran utama untuk menciptakan serangkaian aktivtas teknis dan non-teknis bagi *bioelectronic environment* dan *cyberspace*. Cavelty dalam bukunya yang berjudul "*Cybersecurity and Threat Politics*" menegaskan bahwa negara sudah seharusnya mempertimbangkan perubahan yang di mana era/peradaban digital mendorong negara untuk memperhatikan keamanan siber beserta ancaman serangan siber. Negara harus merancang strategi-strategi dalam perubahan era digital mulai dari politik, sosial, hingga ekonomi (M. Cavelty, 2007).

Keamanan siber mengandalkan sumber informasi sebagai kekuasaan dalam memperoleh kekuatan siber. Kekuatan siber yang dimaksud yaitu seperti ruang tak terlihat (kasat mata), yang di mana domain operasional yang dirancang oleh pemakaian elektronik untuk memanfaatkan informasi lewat sistem komputer dan aplikasi. Dengan demikian, kekuasaan pada kekuatan siber bergantung pada sumber daya yang menjadi ciri domain dunia maya (Nye, 2010).

Isu keamanan siber tidak serta merta harus ditangani oleh negara saja, tetapi juga pada aspek-aspek lainnya. Di dunia yang semakin terkoneksi satu sama lain, isu keamanan siber menjadi perhatian bagi setiap aktor hubungan internasional. Guna mempelajari, menganalisis, serta mengatasi masalah keamanan siber yang

kompleks, dibutuhkan banyak cabang ilmu lain yang terlibat, seperti ilmu teknologi informasi, politik, ekonomi, hubungan internasional, sosial, keamanan, dan lain sebagainya. Maka dari itu, keamanan siber dapat didefinsikan sebagai keterhubungan aktivitas-aktivitas negara, organisasi internasional, individu, dan aktor HI lainnya dengan teknologi informasi sebagai alat/instrumen dari aktivitas-aktivitas hubungan internasional.

2.2.4. Ancaman *Hybrid*

Ancaman keamanan dalam studi ilmu hubungan internasional dibagi menjadi dua yaitu ancaman militeristik (tradisional) dan ancaman non-militeristik (non-tradisional). Namun demikian, munculnya teknologi informasi dan telekomunikasi terutama media sosial dan internet memberikan diskursus baru mengenai isu keamanan dalam konteks hubungan internasional. Berkat kemajuan teknologi informasi dan telekomunikasi, ancaman militeristik dan non-militeristik dapat digabungkan menjadi ancaman *hybrid*. Ancaman *hybrid* sendiri merupakan ancaman yang bersifat fluid atau multibentuk. Ancaman tersebut dapat dikategorikan sebagai ancaman non-tradisional, tetapi dalam prakteknya dapat berimplikasi terhadap ancaman militer. Adanya ancaman *hybrid* ini mengakibatkan kesulitan dalam mencari tahu suatu musuh atau ancaman. Hal ini menjadi perhatian utama bagi negara dan non-negara dalam mengatasi masalah keamanan siber. (Tamarell Vimy et al., 2022)

Ancaman *hybrid* adalah konsep yang sangat relevan dalam dinamika keamanan internasional di masa kontemporer. Ancaman *hybrid* juga dapat diartikan sebagai *hybrid warfare*. *Hybrid warfare* sendiri menggambungkan strategi perang konvensional (penggunaan militer) dan non-konvensional, menyatukan berbagai aspek seperti militer, ekonomi, informasi, politik, teknologi, dan aspek-aspek lainnya. Ancaman *hybrid* beserta bentuk perangnya merupakan hal krusial yang harus dipelajari bagi aktor negara dan non-negara untuk mengembangkan strategi yang efektif.

Ancaman *hybrid* bisa datang dari aktor negara, kelompok teroris, kelompok terorganisir, hingga aktor individu. Tujuan dari operasi ancaman *hybrid* adalah bergantung pada motif para aktor yang terlibat. Hal ini mencakup merubah keputusan politik, mengubah opini publik, mencuri informasi sensitif, mengambil alih sumber daya yang strategis, dan memperoleh keuntungan ekonomi, baik di tingkat nasional maupun tingkat internasional. Peretasan yang dilakukan oleh Nobelium terhadap pemerintah AS/Pentagon, sementara dalang utamanya adalah Rusia merupakan salah satu contoh dari ancaman *hybrid* atau bentuk *hybrid warfare*. (Pahlevi, 2023)

Mengatasi ancaman *hybrid* merupakan topik pembicaraan yang sedang berkembang pesat secara nasional dan internasional. Setiap negara, masyarakat, dan organisasi internasional harus memperhatikan dan memahami ancaman *hybrid*, membangun ketahanan dari ancaman *hybrid*, dan memperoleh kapabilitas untuk melawan ancaman *hybrid*.(Weissmann et al., 2021)

Memahami ancaman di antaranya mengembangkan kesadaraan terhadap kerentanan diri, memahami motif dan cara tindakan negara yang mengoperasi ancaman *hybrid*, dan mengidentifikasi ancaman tersebut. Dalam hal ini, ancaman *hybrid* adalah tindakan terkoordinasi dan tersinkronisasi yang dapat dilakukan dalam berbagai cara dan sektor. Selain itu, membangun ketahanan dari ancaman *hybrid* yaitu meminimalisir potensi keuntungan dari aktor *hybrid warfare*. Terakhir, melawan ancaman *hybrid* yaitu dengan memasuki domain yang belum *familiar*/lazim. Dalam hal ini, penanggulangan terhadap ancaman *hybrid* dilakukan secara langsung serta membangun strategi-strategi pencegahan terhadap potensi ancaman.(Weissmann et al., 2021)

2.3.Hipotesis Penelitian

Berdasarkan pengamatan penulis terkait semua penelitian terdahulu dengan penelitian penulis, penulis dapat memberikan hipotesis/jawaban sementara pada penelitian ini. Terdapat kompleksitas dalam mempelajari, meneliti, dan menganalisis domain keamanan siber beserta ancaman serangan siber dalam studi hubungan internasional. Penulis berasumsi bahwa dibutuhkan pengkajian multidisipliner yang menggabungkan ilmu hubungan internasional dan pengetahuan keamanan siber secara teknis dalam menganalisis studi keamanan siber pada perspektif studi hubungan internasional. Hal tersebut dilakukan karena dengan menggabungkan kedua ilmu tersebut, dapat memberikan sudut pandang yang jauh lebih komprehensif dan kompleks terkait analisis tantangan keamanan siber serta langkah-langkah proaktif untuk mencegah ancaman serangan siber.

Selain itu, kebijakan-kebijakan serta perintah negara terkait keamanan siber merupakan hal krusial dalam mengatasi dan mencegah ancaman serangan siber. Namun demikian, penulis berasumsi bahwa negara tidak bisa berdiri sendiri dalam menghadapi ancaman serangan siber. Penulis berargumen bahwa keselamatan akan serangan siber juga tidak hanya tanggung jawab negara saja, tetapi juga tanggung jawab bagi perusahan-perusahaan industri perangkat lunak seperti SolarWinds. Penulis berasumsi bahwa dibutuhkan transformasi pendekatan dan strategi dalam bagaimana keamanan dinilai dari perusahaan industri perangkat lunak Hal tersebut dilakukan supaya keamanan siber serta keamanan rantai pasokan dunia maya dapat terjamin oleh perusahaan. Dengan demikian, diperlukan kerja sama intensif negara dan aktor non negara lainnnya dalam menghadapi isu keamanan siber beserta ancaman serangan siber.