Jurnal Peperangan Asimetris
Volume 11, Nomor 1, 2025 E-ISSN 2830-0475

Perkembangan Etika dan Moral Pada Dinamika Keamanan Siber Terhadap Perumusan Kebijakan Geopolitik Nasional di Era Digital

Joshua Insetyadi
Universitas Pertahanan, Peperangan Asimetris
Joshuainsetyadi@gmail.com

Abstract

The accelerating dynamics of cybersecurity have created significant ethical and moral complexities that fundamentally challenge the formulation of national geopolitical policy in the digital era. This research aims to analyze how the formulation of national geopolitical policy regarding ethics and morality in defense, and the application of the principle of proportionality in cyber counter-attacks, restricts, legitimizes, or shapes strategic action in response to threats. Employing a qualitative-analytical approach and the conceptual frameworks of Actor-Network Theory (ANT) and Resilience Theory, this study clarifies that cybersecurity has transformed from a purely technical issue into a strategic geopolitical instrument of the state. The main finding indicates the existence of a "policy void" where there is a lack of established national policy to protect state sovereignty through aggressive cyber capabilities. Simultaneously, a nation must adhere to global ethical codes which mandate ensuring human accountability and confirming that such attacks do not cause disproportionate harm to civilians. The implication of this study is the necessity of an adaptive national geopolitical policy framework that clearly integrates digital ethics, providing a moral security foundation for key policymakers in a nation's cyber domain.

Keywords: *Community, Threats, Cyber*

Abstrak

Perkembangan dinamika keamanan siber yang semakin pesat telah menciptakan kompleksitas etika dan moral yang menantang perumusan kebijakan geopolitik nasional di era digital. Penelitian ini bertujuan menganalisis bagaimana perumusan kebijakan geopolitik nasional terhadap etika dan moral dalam pertahanan dan penerapan prinsip proporsionalitas dalam serangan balasan siber yang membatasi, melegitimasi atau membentuk tindakan strategis dalam merespon sebuah ancaman. Penelitian ini menggunakan pendekatan kualitatif-analitis dan kerangka konseptual teori jaringan aktor (ANT) dan Teori Ketahanan (Resilience), studi ini menjelaskan bahwa keamanan siber telah bertransformasi dari isu teknis menjadi

instrumen geopolitik strategis sebuah negara. Hasil yang ditemukan yaitu adanya "kekosongan kebijakan" dimana belum adanya perumusan kebijakan nasional yang diambil untuk melindungi kedaulatan negara melalui kekuatan siber yang agresif. Tetapi pada saat yang sama sebuah negara harus mematuhi kode etik secara global yang mewajibkan untuk menjamin adanya orang yang bertanggung jawab sehingga memastikan serangan tersebut tidak melukai warga sipil secara berlebihan. Implikasi dari penelitian ini adalah perlunya kerangka kebijakan geopolitik nasional yang adaptif yang secara jelas mengintegrasikan etika digital dan memberikan keamanan moral bagi pemangku kebijakan penting di ranah dunia siber suatu negara.

Kata Kunci: Komunitas, Ancaman, Siber

1. Pendahuluan

Perkembangan generasi teknologi modern telah memasuki era society 5.0, dimana revolusi digital telah menyatu dan terintegrasi antara manusia dengan teknologi. Era digital saat ini menjadi dasar utama dalam membentuk pijakan geopolitik suatu negara, dimana ruang siber secara nyata menjadi kekuatan strategis baru yang menggeser kekuatan militer secara konvensional. Pada bidang pertahanan cara pandang ancaman militer konvensional bergeser karena ruang siber telah melampaui batasan-batasan fisik dan menggubah kebijakan suatu negara dalam melihat ancaman baru. Dengan revolusi digital yang semakin modern di suatu negara, maka sebuah pemerintahan akan bergantung pada infrastruktur dan teknologi digital karena kemudahan akses yang mempermudah pekerjaan. Namun dengan perkembangan teknologi yang semakin pesat, terdapat konsekuensi ancaman siber yang meliputi spionase dan sabotase terhadap obyek strategis suatu negara yang dapat menjadi masalah kedaulatan. Negara yang telah menerapkan revolusi digital untuk menjadi bagian utama dalam sebuah sistem, perlu melihat kebijakan geopolitik lebih dalam untuk melihat potensi konflik yang disebabkan kemajuan teknologi. Fenomena ini menciptakan dinamika etika keamanan siber, dimana prinsip-prinsip moral dan perilaku suatu negara harus berevolusi untuk menanggapi kompleksitas

meliputi serangan lintas batas, penangkalan serangan siber dan penggunaan teknologi ofensif dan defensif siber suatu negara. Dengan ketidakjelasan etika dan moral dapat memicu ketakutan bertindak suatu negara sehingga memiliki kerentanan legitimasi tindakan negara untuk membalas suatu ancaman siber didunia nyata.

Perkembangan etika dalam bertindak di ruang siber memunculkan dilema moral yang mempengaruhi cara berfikir dan bertindak suatu negara dalam merumuskan kebijakan geopolitiknya. Terdapat dilema utama untuk mencari siapa aktor dibalik serangan siber tersebut, diduga penyerangan berasal dari aktor State atau aktor non negara yang didukung pihak lain (*state-sponsored hacking*). Lalu dilema kedua Prinsip Proprsionalitas dari Hukum Humaniter Internasional dari domain siber. Peperangan dibidang siber sampai saat ini masih sulit untuk mengukur penyebab kerugiansipil jika melakukan serangan siber balasan, hal ini berbeda dari peperangan konvensional yang telah memiliki aturan sebelum berperang. Dilema-dilema diatas menyebabkan pentingnya perumusan kebijakan untuk menjelaskan sejauh mana negara dapat membenarkan operasi keamanan siber dalam bertahan atau menyerang dengan skala besar. Ketidakpastian etika ini memaksa para pengambil kebijakan geopolitik untuk melakukan secara abu-abu antara melindungi kedaulatan negara dan menjaga komitmen di ranah domestik maupun internasional.

Mengingat kompleksitas ruang siber, penelitian ini memiliki tujuan untuk menganalisis hubungan antara dinamika etika keamanan siber dan Perumusan Kebijakan Geopolitik Nasional. Dengan mengetahui etika bertindak di ruang siber dan dilema yang muncul ditingkat strategis, penelitian ini akan mengidentifikasi bagaimana moralitas berperan dalam mengatur, membenarkan atau membentuk tanggapan suatu negara terhadap ancaman di era digital. Penelitian ini diharapkan dapat memberikan kerangka konseptual bagi pembuat kebijakan untuk lebih melihat strategi geopolitik nasional dari keamanan siber.

2. Tinjauan Pustaka.

a. **Landasan Teori**

1) Teori Ketahanan dari Karl E Weick dan Kathleen M. Sutcliffe. Dalam buku yang berjudul Managing the unexpected (2001) secara implisit teori ini menawarkan sudut pandang yang berlawanan dengan model keamanan siber tradisional yang berfokus pada pencegahan. Keduanya berpandangan bahwa dalam lingkungan yang kompleks dan penuh resiko pentingnya memiliki kemampuan organisasi untuk mengantisipasi dan beradaptasi secara efektif terhadap kejadian tak terduga dalam hal ini serangan siber. Melalui teori ini konteks bidang pertahanan yang kompleks khususnya dibidang siber sangat relevan.

2) Teori Jaringan Aktor dari Bruno Latour, Michel Callon dan John Law. Dalam bukunya yang berjudul *Reassembling the Social: An Introduction to Actor-Network-Theory* (2005) menyatakan bahwa dalam situasi apa pun di ruang siber, kekuatan dan pengaruh bukan hanya dimiliki oleh manusia (peretas,analis atau pembuat kebijakan) tetapi juga oleh aktor non manusia. Aktor non manusia ini mencangkup teknologi digital seperti Malware, AI dan firewall. Dalam konteks siber, teori ANT relevan karena dalam dunia digital tidak bisa memisahkan peran manusia dan teknologi, keduanya adalah aktor yang sama penting dalam menentukan hasi (output), baik dalam melancarkan serangan maupun dalam membangun pertahanan.

b. Penelitian terdahulu. Penelitian berjudul *"Geopolitik cyber security: Strategi menghadapi ancaman siber terhadap keamanan informasi pada era digital"* oleh Soraya Bilqis (2025) bertujuan menunjukan berbagai strategi yang digunakan untuk menyelesaikan persoalan serangan siber. Strategi ini dilakukan untuk meminimalisir berbagai bentuk serangan dan cara

menghadapi serangan di masa depan khususnya negara Indonesia yang berada diurutan kedua dalam konteks ancaman siber. Pendekatan ini menggunakan pendekatan deskriptip kualitatif dengan fokus pada analisis literatur, karakteristik, metafora, deskripsi suatu hal. Pendekatan kualitatif untuk mendapatkan pemahaman mengenai strategi dalam menghadapi ancaman siber terhadap keamanan informasi, sedangkan pendekatan deskriptif digunakan untuk memberikan gambaran yang detail mengenai hal yang di teliti. Pengumpulan data dipilih yang paling relevan dengan tujuan penelitian. Data yang sesuai dengan tujuan penelitian berfokus pada strategi dalam menghadapi ancaman siber dan keamanan informasi diera digital.

3. Metodologi.

Penelitian ini menggunakan pendekatan kualitatif dengan rancangan metodologis yang disusun secara sistematis dan terarah untuk mencapai tujuan studi yang telah ditentukan. Pendekatan kualitatif dipilih karena berfokus pada eksplorasi data non-numerik melalui teknik wawancara mendalam, observasi partisipatif, serta analisis terhadap dokumen dan teks yang relevan. Penulisan jurnal ini disusun menggunakan metode kepustakaan (library research). Library research ini dilakukan dengan mengumpulkan berbagai referensi bacaan yang relevan dengan permasalahan yang diteliti, kemudian dilakukan pemahaman cara teliti dan careful sehingga mendapatkan sebuah temuan-temuan penelitian (Zed, 2003: 3). Penulis melakukan literature study secara mendalam untuk mendukung penelitian ini.

4. Pembahasan.

4.1 Geopolitik Dalam Keamanan Siber.

Geopolitik dapat didefinisikan sebagai kajian yang menganalisis pengaruh faktor-faktor geografis termasuk lokasi, sumber daya alam, topografi dan batas wilayah internasional antar negara. Menurut Saul Cohen, geopolitik adalah studi tentang interaksi antara kekuatan politik dan ruang geografis,

dimana geografis tidak hanya dilihat secara statis tetapi dapat dilihat juga dari lingkup dinamis yang dipengaruhi juga oleh aspek teknologi. Dalam hal ini geopolitik suatu negara yang dimaksud adalah suatu kekuatan dinamika politik sebuah negara yang tidak hanya melihat kondisi wilayah, namun juga terdapat faktor-faktor pendukung lainnya untuk memajukan kepentingan nasional yang dapat menentukan nasib regional maupun internasional. Melihat dinamika perkembangan teknologi dan ruang siber yang semakin maju, hal tersebut mempengaruhi lanskap geopolitik dan membuka persaingan antar negara yang menyerang keamanan informasi. Menurut ahli geopolitik Nicholas Spykman, tujuan utama kebijakan luar negeri adalah keamanan nasional, yang dicapai melalui penguasaan wilayah-wilayah strategis. Dalam konteks modern, hal ini meluas ke ruang siber, di mana kekuatan pertahanan kini harus merumuskan strategi yang mengintegrasikan geografis tradisional dengan keamanan siber untuk memastikan kemampuan *deterrence* dan *resilience* nasional.

Geopolitik diranah keamanan siber telah mengesampingan konsep peperangan tradisional yang berfokus sebelumnya hanya di teritorial darat, laut dan udara bahwa pertarungan antar negara saat ini sudah terjadi dalam dunia digital. Saat ini keamanan siber telah berevolusi menjadi senjata digital yang dapat menyerang dan bertahan, karena teknologi ini adalah cara ampuh dengan cepat dan efisien untuk memberikan pengaruh dan memberikan daya kejut yang jauh lebih dasyat. Kunci keberhasilan keamanan siber adalah siapa negara yang terlebih dahulu mahir dalam menggunakan sebuah kode atau bahasa pemprograman untuk memiliki keunggulan strategis di ruang siber pada era digital. Dengan adanya persaingan tersebut menciptakan model baru peperangan yang tidak hanya dilakukan melalui kontak fisik diwilayah teritorial yang bergeser ke wilayah teritorial digital sebuah negara. Oleh karena itu bagi sebuah negara, menjaga keamanan siber sama pentingnya dengan

menjaga wilayah teritorial fisiknya, sebab ancaman digital kini menjadi penentu utama status dan posisi mereka dalam politik global.

Ruang siber dapat menjadi sebuah senjata digital yang digunakan sebuah negara karena hal tersebut dapat menjadi instrumen utama yang memberikan pengaruh strategis dalam ranah geopolitik. Senjata yang dimaksud dapat dikategorikan seperti sebuah kode bahasa pemprograman, malware dan ransomware canggih, memiliki teknik esploitasi yang beragam berdasarkan tujuannya. Kategori peperangan siber dapat dikategorikan sebagai senjata ofensif dan defensif. Senjata ofensif mencakup zero day exploit dan penyerang melalui malware yang dirancang untuk merusak sistem target, melumpuhkan infrastruktur vital dan mencuri dokumen penting sebuah negara. Disisi lain senjata defensif dan kemampuan cyber deterrence berfungsi sebagai alat tawar-menawar strategis yang menunjukan kesiapan suatu negara untuk membalas serangan sehingga menyeimbangkan dinamaika kekuasaan global diruang siber. Kepemilikan dan keahlian negara saat ini dalam memakai senjata siber secara efektif membuat sebuah negara dapat lebih unggul bila kemampuan negara tersebut siap dalam kemampuan dibidang siber. Intinya, kemampuan digital saat ini sudah mengganti cara negara berperang dan bernegosiasi antar negara.

4.2 Dinamika Keamanan siber di Indonesia pada Era Digital.

Dinamika keamanan siber di Indonesia sangat kompleks dan beragam, hal ini adalah sebuah ancaman yang melampaui sekedar peretasan individu. Indonesia dengan populasi pengguna internet yang masif dan tingkat literasi keamanan siber yang lemah, membuat celah bagi kelompok *cybercrime* transnasional untuk melakukan kejahatan diruang siber. Kejahatan tersebut dapat dilakukan dengan menargetkan sektor infrastruktur vital melalui *phising* dengan menanamkan *malware* dan *ransomware*. Namun ancaman utama yang

dapat menggangu kedaulatan adalah operasi spionase dan serangan yang disponsori oleh negara (*state-sponsored attacks*) dengan tujuan untuk menyerang basis data digital agar melemahkan sistem pemerintahan di Indonesia. Serangan ini bertujuan untuk mencuri informasi yang bersifat srategis, meretas ekonomi perbankan dan melumpuhkan layanan publik menunjukan bahwa keamanan siber di Indonesia adalah ruang digital yang tidak memiliki kekuatan memadai.

Indonesia telah merespon dinamika ancaman tersebut dengan melakukan kolaborasi dan transformasi antar kelembangaan secara signifikan, hal terutama dengan melakukan pembentukan Badan Siber dan Sandi Negara (BSSN) sebagai otoritas tunggal dibidang keamanan siber. Pembentukan BSSN adalah bukti nyata bahwa Indonesia memiliki pengakuan secara global bahwa keamanan siber harus dilihat sebagai cara peperangan baru pada era saat ini. Terdapat tantangan utama yang terletak pada sinergi dan koordinasi antara BSSN dengan kementerian/lemabaga lain seperti TNI, POLRI, BIN serta sektor swasta yang mengelola infrastruktur digital yang bersifat strategis. Duplikasi wewenang dan perbedaan cara penanganan membuat lambatnya informasi sehingga respon cepat terhadap insiden tidak berjalan semestinya. Oleh karena itu dinamika respon negara Indonesia saat ini berada dalam fase kritis dimana efektivitas pertahanan bergantung pada seberapa baik kerangka kerja dan kordinasi yang efektif untuk mengatasi ego sektoral sehingga kemampuan siber dapat berjalan secara terintegrasi antar lembaga.

Dinamika keamanan siber di Indonesia juga menghadapi dilema regulasi dan etika digital. Dalam hal ini Indonesia meskipun memiliki UU ITE, regulasi tersebut sering dianggap tidak memadai untuk mengatasi isu yang lebih kompleks dalam bidang pertahanan siber yang membutuhkan standar jelas. Dalam bidang penyerangan (*cyber counter attack*) aktor siber negara memiliki beban moral yang harus ditanggung untuk segera merespon dan

melindugi kedaulatan melalui tindakan represif dan agresif dibidang siber. Akor siber dalam hal ini perlu mendapatkan kepastian payung hukum untuk melakukan upaya pencegahan yang kadang bertentangan dengan komitmen terhadap hak privasi dan kebebasan sipil warga negara. Di era transformasi digital saat ini, kebijakan nasional perlu mempertegas dengan melakukan perumusan undang-undang yang dirumuskan secara bersama oleh kementerian dan lembaga agar tindakan yang dilakukan aktor siber menjadi jelas dan tidak berjalan diranah abu-abu. Dengan adanya undang-undang yang jelas maka pengamanan negara akan memberikan etika hukum yang adaptif, transparan dan dapat diterima secara luas. Hal ini dilakukan untuk memastikan bahwa kekuatan siber suatu negara dikerahkan secara terintegrasi dan profesionalitas.

Secara geopolitik, kemanan siber Indonesia sangat dipengaruhi oleh persaingan kekuatan besar terutama antara blok barat dan blok timur hal ini disebabkan ketergantungan teknologi dibidang siber yang masih belum memiliki kemandirian pengembangan teknologi siber. Indonesia sebagai negara non blok di kawasan Asean berusaha menjaga independesi kemampuan siber yang infrastruktur dan perangkat sibernya masih dari produsen asing. Dinamika ini memaksa Indonesia yang akhirnya memiliki kerentanan geopolitik dimana kebijakan pengadaan teknologi dapat menjadi alat pemaksaan oleh negara adidaya. Oleh karena itu Indonesia perlu meningkatkan kemandirian siber melalui pengembangan industri keamanan siber domestik dan memperkuat diplomasi siber di forum regional dan internasional. Tujuan kemandirian ini bukan tanpa sebab yakni untuk membentuk norma perilaku siber yang mendukung kedaulatan nasional sehingga mengurangi resiko yang dapat dimanfaatkan sebagai pintu masuk serangan siber melalui alat-alat asing.

5. Kesimpulan.

Penelitian ini, melalui pendekatan kualitatif-analitis yang didukung oleh Teori Jaringan Aktor (ANT) dan Teori Ketahanan (Resilience), menyimpulkan bahwa dinamika keamanan siber telah bertransformasi menjadi instrumen geopolitik strategis yang setara dengan kekuatan konvensional. Temuan sentralnya adalah adanya "kekosongan kebijakan" (policy void) di tingkat nasional yang disebabkan oleh dilema etika dan moral. Dilema ini menuntut negara untuk mengembangkan kapabilitas siber agresif demi melindungi kedaulatan, tetapi pada saat yang sama harus mematuhi kode etik global dan prinsip proporsionalitas Hukum Humaniter Internasional (HHI), terutama dalam melakukan serangan balasan siber. Ketidakjelasan mengenai akuntabilitas aktor (State vs. state-sponsored) dan kesulitan mengukur kerugian sipil telah menciptakan ketakutan bertindak dan menyebabkan aktor siber bergerak di ranah abu-abu. Implikasi dari studi ini menekankan urgensi untuk merumuskan kerangka kebijakan geopolitik nasional yang adaptif. Kerangka ini harus secara jelas mengintegrasikan etika digital, memberikan keamanan moral bagi pemangku kebijakan, serta menjamin payung hukum yang transparan bagi tindakan siber, guna menyeimbangkan antara kebutuhan pertahanan strategis negara dan komitmen terhadap norma-norma etika global, sekaligus mengatasi tantangan internal seperti koordinasi antarlembaga dan ketergantungan teknologi asing.

6. Ucapan Terima Kasih.

Penulis mengucapkan terima kasih kepada Universitas Pertahanan atas penyediaan lingkungan akademik yang suportif, serta apresiasi tertinggi kepada peninjau external atas bimbingan dan arahan dalam penyelesaian jurnal ini.

Penghargaan khusus juga penulis sampaikan kepada Kaprodi Program Studi Peperangan Asimetris, serta rekan-rekan Prodi Peperangan Asimetris Angkatan Cohort XIV atas dukungan moral, diskusi, dan semangat kebersamaan yang menjadi penguat penulis selama proses penelitian.

DAFTAR PUSTAKA

Zed, M. (2003). Metode Penelitian Kepustakaan. Jakarta: Yayasan Obor Indonesia.

Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. San Francisco: Jossey-Bass.

Rid, Thomas. (2013). *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

Cohen, S. B. (2003). *Geopolitics: The Geography of International Relations* (2nd ed.). Lanham: Rowman & Littlefield Publishers. (Mengacu pada buku Cohen yang membahas definisi geopolitik).

Spykman, N. J. (1942). *America's Strategy in World Politics: The United States and the Balance of Power*. New York: Harcourt, Brace and Company.

Weick, Karl E., & Sutcliffe, Kathleen M**.** (2001). *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. San Francisco: Jossey-Bass.

Bilqis, S. (2025). Geopolitik *cyber security*: Strategi menghadapi ancaman siber terhadap keamanan informasi pada era digital. *Maliki Interdisciplinary Journal*, *3*(6), 2233-2239.

Tallinn Manual. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Edited by Michael N. Schmitt. Cambridge: Cambridge University Press. Kerangka Etika dan Hukum Humaniter Internasional di ruang siber, termasuk Prinsip Proporsionalitas yang dibahas dalam dilema etika.