CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol. 13 No. 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

PAHALGAM 2025 DAN PERANG DIGITAL: ESKALASI *SOFT WAR* DALAM KONFLIK INDIA-PAKISTAN

Tita Andraena
Universitas Hasanuddin, Makassar, Sulawesi Selatan, Indonesia

Email: titaandraena@gmail.com

ABSTRACT

This research examines the dynamics of cyber conflict between India and Pakistan after the 2025 Pahalgam attack. The event became an important moment in the escalation of digital warfare, characterized by the rise of disinformation, attacks on cyber infrastructure, and the struggle for narratives in digital space. Using the theories of asymmetric warfare, soft power, and regional security complex, this study shows that cyberspace has become a strategic terrain in the struggle for power and influence. The involvement of both state and non-state actors extends the impact of the conflict to the regional sphere, deepening the crisis of trust and destabilizing South Asia. The study concludes that digital security requires an approach that goes beyond technical protection, through regional cooperation and digital diplomacy that is responsive to non-traditional challenges.

Keywords: *Cyberwarfare, India, Pakistan, Disinformation, Regional Security.*

ABSTRAK

Penelitian ini mengulas dinamika konflik siber antara India dan Pakistan setelah serangan Pahalgam 2025. Peristiwa tersebut menjadi momen penting dalam meningkatnya perang digital, ditandai oleh maraknya disinformasi, serangan pada infrastruktur siber, serta perebutan narasi di ruang digital. Dengan menggunakan teori *asymmetric warfare*, *soft power*, dan *regional security complex*, studi ini menunjukkan bahwa ruang siber telah menjadi medan strategis dalam perebutan kekuasaan dan pengaruh. Keterlibatan aktor negara dan non-negara memperluas dampak konflik ke ranah regional, memperdalam krisis kepercayaan dan mengganggu stabilitas Asia Selatan. Studi ini menyimpulkan bahwa keamanan digital memerlukan pendekatan yang lebih dari sekadar proteksi teknis, yakni melalui kerja sama kawasan dan diplomasi digital yang responsif terhadap tantangan non-tradisional.

Kata kunci: Perang Siber, India, Pakistan, Disinformasi, Keamanan Regional

Article history
Received: Mei 2025
Reviewed: Mei 2025
Published: Mei 2025

Plagirism checker no 336
Doi : prefix doi :
10.8734/causa.v1i2.365
Copyright : author
Publish by : causa

PENDAHULUAN

Di era pascakebenaran dan revolusi digital, kekuatan negara dalam konflik tidak lagi ditentukan oleh jumlah tentara atau persenjataan, melainkan oleh kemampuan mengendalikan informasi dan menguasai dunia siber. Serangan Pahalgam 2025 menjadi titik krusial yang menunjukkan bagaimana dua negara dengan sejarah rivalitas panjang India dan Pakistan telah menggeser medan pertikaiannya ke wilayah digital. Serangan tersebut tak hanya berdampak pada aspek keamanan fisik, tetapi juga memicu penyebaran disinformasi, propaganda daring, dan tekanan psikologis lintas negara. Kejadian ini mempertegas bahwa *cyberwarfare* kini

Jurnal Hukum dan Kewarganegaraan
Vol. 13 No. 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

menjadi dimensi penting dalam dinamika hubungan internasional, terutama di kawasan rentan konflik seperti Asia Selatan (Baek, D. S. 2025).

Hubungan India dan Pakistan, yang telah lama dipenuhi ketegangan akibat sengketa wilayah, identitas, serta rivalitas militer dan politik, mengalami pergeseran bentuk konflik sejak keduanya menjadi negara bersenjata nuklir. Konfrontasi langsung semakin dihindari dan digantikan oleh perang asimetris seperti serangan siber serta kampanye digital. Dunia maya kini menjadi ruang strategis untuk mempertahankan pengaruh, menyebarkan narasi politik, dan menggoyahkan stabilitas dalam negeri pihak lawan. Berbagai aktor, mulai dari negara, kelompok hacktivis, hingga media partisan, berperan aktif dalam menciptakan lanskap digital yang penuh ketegangan dan ancaman non-tradisional (Awan, M. A., et al. 2025).

Konflik ini tidak lagi hanya menyasar data atau sistem keamanan, tetapi juga menyasar kebenaran itu sendiri. Kemajuan teknologi seperti *deepfake* dan *bot* sosial memperkuat penggunaan informasi sebagai senjata utama. Di tengah ketegangan pasca-serangan Pahalgam, kedua negara saling menyalahkan atas insiden digital tersebut sambil menyebarkan narasi yang saling bertolak belakang melalui media nasional dan global. Dalam konteks ini, muncul urgensi akan strategi "*Truth Defence"* untuk menjaga integritas informasi sekaligus mencegah penyebaran misinformasi yang dapat memperburuk konflik dan memicu eskalasi yang tidak diinginkan (Government ET Blog, 2025).

Penelitian ini bertujuan untuk mengkaji bagaimana insiden Pahalgam 2025 menjadi titik balik dalam transformasi konflik India–Pakistan menjadi bentuk digital, serta bagaimana strategi *soft war* kini memainkan peran strategis. Studi ini penting tidak hanya untuk memahami dinamika politik di kawasan Asia Selatan, tetapi juga untuk merumuskan pendekatan keamanan kontemporer yang relevan. Melalui metode kajian pustaka dan teori hubungan internasional, tulisan ini mengeksplorasi bagaimana *cyberwarfare* dijadikan alat untuk membentuk kekuatan dan narasi oleh kedua negara serta dampaknya terhadap stabilitas kawasan.

TINJAUAN LITERATUR

Konflik antara India dan Pakistan telah lama menjadi fokus utama dalam kajian keamanan kawasan Asia Selatan, terlebih sejak kedua negara tersebut memiliki kapabilitas nuklir pada akhir abad ke-20. Namun, dalam dua puluh tahun terakhir, bentuk konflik ini mengalami pergeseran dari konfrontasi militer langsung ke arah perang non-konvensional, termasuk *cyberwarfare*. Salah satu analisis awal mengenai transisi ini ditulis oleh C. Christine Fair dalam karyanya *Fighting to the End: The Pakistan Army's Way of War* (2014), yang menyatakan bahwa Pakistan cenderung menerapkan strategi non-linear dalam menghadapi kekuatan konvensional India, seperti melalui pemanfaatan media digital dan operasi siber. Pendapat ini diperkuat oleh studi Awan dkk. (2025), yang menemukan bahwa serangan siber antara kedua negara meningkat drastis pasca insiden Balakot 2019, dengan pola serangan yang lebih sistematis dan menjadi bagian dari strategi yang matang, bukan sekadar reaksi emosional semata (Awan, M. A., et al. 2025).

Dari perspektif teori hubungan internasional, sejumlah literatur memperkenalkan konsep *asymmetric warfare* dan *soft war* sebagai pendekatan utama dalam memahami dinamika *cyberwarfare* di kawasan Asia Selatan. Nye (2004), dalam bukunya *Soft Power: The Means to Success in World Politics*, menjelaskan bahwa kekuatan lunak melalui budaya, pengaruh, dan informasi dapat menjadi instrumen yang sangat ampuh untuk memengaruhi negara lain tanpa perlu intervensi militer. Dalam kasus India dan Pakistan, kedua negara tidak hanya menargetkan infrastruktur digital lawan melalui serangan siber, tetapi juga menggunakan ruang siber sebagai sarana untuk mempengaruhi opini publik, menyebarkan disinformasi, serta mengikis kepercayaan terhadap institusi negara masing-masing. Awan dkk. juga menyoroti bahwa propaganda siber ini menciptakan tekanan psikologis yang signifikan dalam masyarakat, membuktikan bahwa soft war memiliki dampak strategis yang substansial.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol. 13 No. 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Selain itu, konflik digital antara India dan Pakistan memiliki relevansi kawasan yang lebih luas, sebagaimana dijelaskan dalam teori *regional security complex* oleh Barry Buzan dan Ole Wæver dalam karya mereka *Security: A New Framework for Analysis* (1998). Keduanya berpendapat bahwa konflik bilateral yang berlangsung secara terus-menerus dapat memicu efek berantai terhadap keamanan negara-negara di sekitarnya. Hal ini disebabkan oleh dinamika ancaman yang saling berhubungan dan persepsi ancaman yang tidak dapat sepenuhnya dikendalikan oleh satu negara saja. Dalam konteks serangan Pahalgam 2025, penyebaran disinformasi lintas negara tidak hanya mengganggu keamanan domestik India dan Pakistan, tetapi juga berdampak pada manajemen informasi regional, ketegangan dalam hubungan diplomatik bilateral, hingga konflik di antara komunitas diaspora di negara ketiga seperti Inggris dan Kanada yang menjadi sasaran dari narasi propaganda siber kedua negara (Nye, J. S. 2004).

Oleh karena itu, literatur yang ada menunjukkan bahwa *cyberwarfare* antara India dan Pakistan tidak sekadar representasi dari kemajuan teknologi dalam konflik, tetapi juga menggambarkan transformasi mendasar dalam cara negara menggunakan kekuatan di era digital. Kajian ini memiliki nilai strategis, bukan hanya untuk memahami dinamika keamanan antara India dan Pakistan, tetapi juga sebagai acuan dalam mendefinisikan kembali konsep ancaman dalam hubungan internasional modern. Konflik ini mencerminkan keterkaitan antara *soft power, asymmetric warfare,* dan rivalitas naratif, yang keseluruhannya diperkuat oleh kemajuan infrastruktur teknologi informasi yang semakin rumit dan sulit dikendalikan secara konvensional.

KERANGKA TEORI & METODOLOGI

1. Kerangka Teori

Untuk memahami dinamika *cyberwarfare* India–Pakistan pasca serangan Pahalgam 2025, kajian ini menggunakan kombinasi tiga pendekatan teori dalam studi hubungan internasional dan keamanan, yakni *asymmetric warfare, soft power/soft war,* serta *regional security complex theory*. Pertama, konsep *asymmetric warfare* digunakan untuk menjelaskan karakter konflik yang tidak seimbang secara kekuatan militer konvensional, di mana negara atau aktor dengan kelemahan struktural memilih strategi tidak langsung seperti sabotase siber dan serangan informasi. Dalam konteks ini, Pakistan dianggap menggunakan instrumen digital untuk menantang dominasi konvensional India tanpa memicu konfrontasi langsung. Serangan siber, propaganda daring, dan manipulasi naratif menjadi bagian dari strategi perang tidak simetris yang relatif murah, fleksibel, dan sulit dilacak.

Kedua, kerangka *soft power* dan *soft war* dari Joseph Nye digunakan untuk membaca bagaimana konflik ini bertransformasi menjadi perang pengaruh, di mana narasi, opini publik, dan legitimasi informasi menjadi senjata utama. *Soft war* dalam kasus ini muncul dalam bentuk perang simbolik dan informasi seperti framing serangan, kampanye balasan di media sosial, serta upaya merusak reputasi negara lawan. Tujuan akhirnya bukan hanya kemenangan di medan pertempuran digital, tetapi dominasi dalam persepsi global dan kepercayaan publik domestik.

Ketiga, teori *regional security complex* (Buzan & Wæver) digunakan untuk memahami dampak struktural dari konflik ini terhadap stabilitas kawasan Asia Selatan. Dalam teori ini, konflik bilateral seperti India–Pakistan tidak berdiri sendiri, tetapi memiliki dampak keamanan berantai terhadap negara-negara sekitar karena keterikatan geostrategis dan sejarah. Penyebaran disinformasi, eskalasi naratif, dan potensi kerusakan sistem digital lintas batas membuat konflik ini tidak lagi terbatas secara teritorial, melainkan menjadi konflik sistemik yang berisiko mengguncang keamanan kawasan secara lebih luas.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol. 13 No. 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

2. Metodologi

Penelitian ini menggunakan pendekatan kualitatif-deskriptif dengan metode studi kepustakaan *(library research)*. Seluruh data diperoleh dari sumber-sumber sekunder seperti jurnal akademik, buku teori hubungan internasional, laporan kajian strategis, serta artikel berita yang kredibel dan aktual. Pemilihan metode ini bertujuan untuk menggali pemahaman konseptual tentang fenomena perang siber India–Pakistan, khususnya pasca-serangan Pahalgam 2025, dalam kaitannya dengan strategi *soft war* dan dinamika keamanan regional.

Data dianalisis menggunakan analisis tematik, yaitu dengan mengelompokkan temuan ke dalam tema-tema utama seperti strategi digital, disinformasi, dan respons negara. Tema-tema ini kemudian dibaca dan ditafsirkan menggunakan teori hubungan internasional yang telah dijelaskan pada bagian sebelumnya. Dengan pendekatan ini, penelitian ini diharapkan mampu menghasilkan kajian yang tajam secara teoritis namun tetap relevan terhadap isu strategis kontemporer.

HASIL PEMBAHASAN

1. Kronologi Serangan Pahalgam 2025

Serangan terhadap konvoi pasukan keamanan India di Pahalgam, Kashmir, pada Mei 2025 menandai babak baru yang krusial dalam persaingan antara India dan Pakistan. Insiden ini menewaskan lebih dari 10 anggota pasukan dan memicu respons tegas dari pihak India, baik melalui pernyataan politik yang keras maupun peningkatan pengamanan di wilayah perbatasan. Akan tetapi, aspek yang paling mencolok dari insiden ini adalah perluasan konflik ke ranah digital, ditandai dengan aksi kelompok peretas pro-Pakistan yang segera meluncurkan kampanye defacement terhadap situs-situs militer India, sementara pihak India merespons dengan operasi digital terkoordinasi yang menargetkan media Pakistan serta situs lembaga pemerintahan mereka (Awan, M. A., et al. 2025).

Kejadian ini dengan cepat menjadi simbol dari meningkatnya intensitas perang digital di antara kedua negara, menunjukkan bahwa konflik tidak lagi terbatas pada ruang fisik saja, melainkan juga telah meluas ke dunia maya. Media sosial berubah menjadi medan pertempuran informasi, ditandai dengan penyebaran propaganda, manipulasi video, serta serangan bot terhadap akun-akun resmi pemerintah. Dalam kurun waktu kurang dari satu hari, narasi mengenai pelaku dan korban menjadi kabur karena arus disinformasi yang menyebar sangat cepat dan masif.

Fenomena tersebut mencerminkan kecenderungan global di mana konflik bersenjata kontemporer hampir selalu dibarengi oleh pertempuran naratif di ruang digital, yang jika tidak dikendalikan, dapat menciptakan tekanan sosial dan psikologis yang sama merusaknya dengan serangan militer tradisional. Dalam konteks Pahalgam, pertarungan narasi tidak hanya menyangkut soal pihak yang dipersalahkan, tetapi juga siapa yang mampu mendominasi persepsi publik, baik di tingkat nasional maupun internasional.

2. Strategi Digital Kedua Negara

India dan Pakistan menunjukkan perbedaan mendasar dalam pendekatan mereka terhadap pengelolaan kekuatan siber, yang mencerminkan karakteristik struktur keamanan nasional masing-masing negara. Di pihak India, pengelolaan kekuatan siber dilakukan secara institusional dan terpusat, dengan fokus utama pada penguatan kapasitas pertahanan digital negara melalui lembaga-lembaga resmi.

Dua lembaga utama yang memainkan peran sentral adalah *National Critical Information Infrastructure Protection Centre* (NCIIPC) dan *Defence Cyber Agency*, yang keduanya beroperasi di bawah koordinasi Kementerian Pertahanan India. Strategi India ini menekankan pentingnya perlindungan terhadap infrastruktur digital vital negara, terutama sistem komando dan kontrol militer, jaringan komunikasi, serta sektor energi dan transportasi yang terintegrasi

secara digital. Pendekatan ini menandakan adanya orientasi jangka panjang untuk membangun pertahanan siber yang stabil, terorganisir, dan dapat dipertanggungjawabkan secara hierarkis (Baek, D. S. 2025).

Sebaliknya, Pakistan mengadopsi strategi yang lebih luwes dan tidak terlalu terpusat, dengan memadukan peran aktor negara dan non-negara dalam operasi-operasi sibernya. Salah satu aktor negara yang paling sering dikaitkan dengan kegiatan ini adalah *Inter-Services Intelligence* (ISI), yang secara historis memiliki kapasitas tinggi dalam operasi intelijen dan pengumpulan informasi. Selain itu, banyak laporan juga menyebutkan keterlibatan kelompok peretas independen yang berpihak pada kepentingan Pakistan dalam melancarkan serangan terhadap situs-situs pemerintah India (Baek, D. S. 2025).

Dengan membentuk jaringan digital yang lebih informal dan tersebar, Pakistan memiliki ruang manuver yang lebih besar untuk menyangkal keterlibatan langsung negara dalam berbagai insiden peretasan. Namun, fleksibilitas ini juga membawa risiko serius, terutama karena sulitnya mengendalikan aktor-aktor non-negara yang dapat bertindak di luar koordinasi atau bahkan tanpa persetujuan otoritas resmi, sehingga berpotensi memperburuk eskalasi konflik siber secara tidak terduga (Ahmad, S., & Jahangir, J. 2023).

Ketika insiden Pahalgam 2025 terjadi, respons digital dari India dilakukan secara sistematis dan terorganisir, mencerminkan karakter terpusat dari kebijakan sibernya. Serangan balasan India diarahkan pada berbagai aset digital milik pemerintah dan media Pakistan, dengan tujuan utama menunjukkan kapasitas pertahanan dan kemampuan ofensif India di ranah siber. Serangan ini tidak hanya bertujuan untuk membalas secara teknis, tetapi juga memiliki nilai simbolik dan strategis, yakni memperkuat posisi India sebagai negara yang mampu melakukan deterrence digital secara efektif. Di sisi lain, Pakistan tetap bertumpu pada metode yang lebih taktis dan cepat, dengan memanfaatkan kekuatan media sosial untuk menyebarkan narasi alternatif dan menggiring opini publik melalui kampanye yang mudah viral. Strategi ini mencerminkan kecenderungan Pakistan untuk menggunakan perang siber sebagai alat dalam pertempuran persepsi, terutama dalam konteks eskalasi jangka pendek (Ahmad, S., & Jahangir, J. 2023).

3. Disinformasi, Truth Defense, dan Narasi Dominasi

Dalam insiden serangan di Pahalgam, disinformasi tidak lagi berperan sebagai konsekuensi pasif dari konflik, melainkan telah bertransformasi menjadi instrumen strategis yang disengaja. Kelompok-kelompok yang berafiliasi dengan kedua belah pihak terlibat aktif dalam menyebarkan konten yang telah dimodifikasi, seperti video yang dimanipulasi secara digital, serta narasi emosional yang sarat bias dan bertujuan mendiskreditkan lawan. Tujuan utama dari serangan ini bukanlah penghancuran infrastruktur fisik, melainkan perusakan reputasi dan kredibilitas, baik di tingkat domestik maupun dalam arena internasional (Government ET Blog, 2025).

Situasi ini menimbulkan urgensi akan pentingnya penerapan konsep *truth defense,* yakni suatu mekanisme yang dikembangkan oleh negara untuk melindungi masyarakat dari arus informasi yang menyesatkan. *Truth defense* bukan sekadar aktivitas jurnalistik atau penyampaian klarifikasi satu arah, melainkan merupakan pendekatan komprehensif yang melibatkan sinergi antara media pemerintah, institusi keamanan, dan kerjasama dengan perusahaan teknologi guna membatasi persebaran konten yang belum terverifikasi (Ashraf, M. N., & Kayani, S. A. 2023).

Dalam kerangka teori *soft power,* penguasaan terhadap narasi dan persepsi dipandang sebagai bentuk kekuatan kontemporer. Sebagaimana dijelaskan oleh Nye, kekuatan ini memungkinkan suatu negara mencapai tujuan strategis tanpa harus menggunakan kekerasan, melainkan melalui pembentukan kerangka pikir yang kemudian diadopsi oleh publik. Dalam konteks ini, disinformasi bisa dimanfaatkan sebagai senjata *soft power* yang bersifat ofensif,

sedangkan truth defense hadir sebagai alat *soft power* yang bersifat defensif. Eskalasi *cyberwarfare* menjadikan keduanya sebagai bagian dari medan perebutan dominasi naratif (Ashraf, M. N., & Kayani, S. A. 2023).

Lebih jauh lagi, melalui pendekatan teori konstruktivisme, disinformasi dipahami sebagai sarana untuk menciptakan realitas sosial yang baru. Negara sebagai aktor tidak hanya berupaya memenangkan perdebatan melalui argumen, tetapi juga berusaha merancang ulang persepsi publik mengenai siapa yang berada di pihak yang benar dan siapa yang patut disalahkan. Dalam konteks konflik antara India dan Pakistan, pembentukan narasi seputar isu seperti separatisme, radikalisme, maupun korban sipil memiliki dampak besar terhadap opini publik internasional, bahkan berpotensi memengaruhi legitimasi dalam forum diplomatik (Ghernaouti-Helie, S. 2013).

Dari perspektif teori keamanan kritis *(critical security studies)*, konsep *truth defense* dilihat sebagai wujud perlawanan terhadap upaya militerisasi informasi. Manipulasi informasi dapat menciptakan ketakutan massal dan membuka jalan bagi kebijakan represif yang membatasi kebebasan sipil. Oleh karena itu, menjaga keakuratan dan integritas informasi merupakan bagian dari usaha mempertahankan hak-hak sipil dan kebebasan berekspresi di tengah krisis. Dalam hal ini, *truth defense* bukan hanya alat negara untuk menjaga stabilitas, tetapi juga menjadi bentuk nyata dari advokasi terhadap keamanan manusia (Ghernaouti-Helie, S. 2013).

4. Dampaknya terhadap Stabilitas Kawasan dan Persepsi Global

Ketegangan *cyberwarfare* yang terus meningkat antara India dan Pakistan memiliki potensi besar untuk memperburuk hubungan diplomatik di kawasan Asia Selatan secara keseluruhan. Persaingan digital ini tidak lagi menjadi masalah bilateral semata, melainkan telah menimbulkan kecemasan luas di kalangan negara-negara tetangga seperti Nepal, Sri Lanka, dan Bangladesh. Kekhawatiran utama yang muncul adalah kemungkinan meluasnya dampak konflik digital ini ke luar batas teritorial kedua negara, baik melalui penyebaran hoaks politik, manipulasi informasi yang menyesatkan, hingga ancaman sabotase terhadap sistem infrastruktur digital milik negara lain di kawasan. Dengan meningkatnya ketergantungan pada teknologi informasi di berbagai aspek kehidupan, dari ekonomi hingga pemerintahan, ancaman siber semacam ini dinilai sangat berbahaya karena berpotensi mengguncang stabilitas internal negara-negara tersebut, meskipun mereka tidak secara langsung terlibat dalam konflik (Mirza, M. N., & Babar, S. I. 2020).

Lebih jauh lagi, dinamika ini menunjukkan bahwa konflik digital tidak dapat dipahami hanya sebagai pertarungan antara dua aktor negara, melainkan telah berkembang menjadi persoalan dengan dimensi regional yang kompleks dan sulit untuk diisolasi. Efek domino yang ditimbulkan oleh serangan siber, baik secara teknis maupun psikologis, memiliki cakupan lintas batas yang mengaburkan garis konvensional antara wilayah konflik dan wilayah aman.

Negara-negara Asia Selatan yang sebelumnya tidak menjadi bagian dari konflik utama, tetap berisiko terdampak melalui gangguan pada jaringan digital regional, penyusupan terhadap data strategis, serta polarisasi opini publik akibat kampanye informasi yang bersifat provokatif dan memecah belah.

Dalam konteks perspektif global, insiden seperti serangan di Pahalgam dan ketegangan siber yang menyusul setelahnya telah menyoroti tantangan serius yang dihadapi kawasan Asia Selatan dalam hal kapasitas menjaga stabilitas digital dan kredibilitas informasi. Komunitas internasional mulai mempertanyakan sejauh mana negara-negara di kawasan ini mampu membangun mekanisme keamanan siber yang kuat, terkoordinasi, dan transparan. Kekhawatiran berkembang bahwa kawasan ini berisiko berubah menjadi "zona abu-abu" dalam pertarungan digital antar negara-negara besar dunia, di mana berbagai serangan siber dapat

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol. 13 No. 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

terjadi tanpa kejelasan pelaku, akuntabilitas, atau batas etika yang jelas (Mirza, M. N., & Babar, S. I. 2020).

Jika kondisi ini terus berlanjut tanpa adanya pendekatan regional yang kolaboratif, dampaknya dapat meluas ke berbagai sektor penting. Potensi terganggunya kerja sama internasional di bidang teknologi, pertahanan, dan informasi menjadi nyata, karena kepercayaan antarnegara terganggu akibat kekhawatiran terhadap spionase digital. Selain itu, iklim investasi asing juga bisa terdampak secara negatif, mengingat perusahaan-perusahaan global akan menilai Asia Selatan sebagai wilayah berisiko tinggi dari segi keamanan digital. Di sisi lain, komunikasi transnasional, baik antar institusi pemerintahan, perusahaan, maupun masyarakat sipil, juga bisa mengalami gangguan serius apabila tidak ada sistem perlindungan siber yang mumpuni (Ashraf, M. N., & Kayani, S. A. 2023).

5. Peran Aktor Negara dan Non-Negara

Cyberwarfare dewasa ini tidak lagi terbatas sebagai alat milik negara, melainkan juga dijalankan oleh berbagai aktor non-negara seperti kelompok hacktivist, organisasi yang menganut ideologi tertentu, serta komunitas digital dengan afiliasi politik atau nasionalisme yang kuat. Dalam konteks konflik antara India dan Pakistan, keterlibatan aktor-aktor ini menjadi semakin mencolok. Kedua negara tampaknya memberikan ruang gerak baik secara eksplisit maupun implisit bagi kelompok-kelompok semacam ini untuk melancarkan serangan digital sebagai bagian dari bentuk *proxy war* di ranah siber. Fenomena ini menguatkan pandangan dalam teori *proxy war*, yang menjelaskan bahwa negara dapat memanfaatkan entitas non-negara sebagai perpanjangan tangan dari kebijakan luar negeri mereka, terutama ketika ingin menghindari keterlibatan langsung yang berisiko secara diplomatik (Ghernaouti-Helie, S. 2013).

Aktor-aktor non-negara seperti *"Team Pak Cyber Force"* dari Pakistan maupun *"Indian Cyber Troops"* dari India merupakan contoh nyata bagaimana kelompok digital partisan terlibat aktif dalam meningkatkan eskalasi konflik. Aksi mereka meliputi *defacing* situs web milik institusi penting, doxing terhadap tokoh-tokoh publik dari negara lawan, hingga penyebaran narasi provokatif melalui *platform* media sosial yang tertutup dan sulit dilacak. Meskipun mereka beroperasi di luar struktur resmi kenegaraan, narasi dan tujuan yang mereka bawa sering kali secara tidak langsung sejalan dengan kepentingan geopolitik negara asalnya. Keberadaan mereka memperluas medan pertempuran ke dalam domain sosial digital, menciptakan ruang konflik yang melibatkan masyarakat sipil secara langsung sebagai audiens maupun sasaran (Government ET Blog, 2025).

Jika dilihat melalui lensa teori realisme struktural, keberadaan aktor-aktor non-negara dalam *cyberwarfare* tetap menunjukkan adanya struktur kekuasaan global yang berpengaruh dalam menentukan arah konflik. Negara, dalam teori ini, tetap menjadi entitas utama yang memiliki kapasitas dominan dalam mengelola dan memanfaatkan kekuatan, termasuk kekuatan digital. Bahkan di ruang maya yang tampaknya terbuka dan tidak terikat geografis, negara-negara besar tetap memegang kendali melalui infrastruktur digital, kebijakan keamanan, dan teknologi canggih. Dalam hal ini, negara seperti India yang memiliki sistem teknologi informasi dan pertahanan siber yang mapan, memiliki keunggulan dalam mengatur serta memanfaatkan partisipasi aktor non-negara untuk tujuan strategis dan diplomatiknya (Zahoor, R., & Razi, N. 2020).

Namun, perspektif yang ditawarkan oleh teori pluralisme menantang dominasi pandangan negara-sentris. Dalam teori ini, aktor non-negara dipahami memiliki otonomi dan agenda tersendiri yang tidak selalu sejalan dengan kepentingan negara. Artinya, keterlibatan kelompok sipil dalam konflik digital dapat menciptakan lapisan kompleksitas baru, karena tindakan mereka bisa saja bertentangan atau bahkan mengganggu upaya diplomatik antarnegara. Ketika serangan dilakukan oleh entitas sipil tanpa koordinasi atau sepengetahuan

negara, potensi untuk menciptakan kesalahpahaman dan memperburuk ketegangan antar pemerintah menjadi sangat besar. Dalam situasi seperti ini, *cyberwarfare* justru memperlihatkan kerentanannya terhadap intervensi yang tidak terkendali (Mirza, M. N., & Babar, S. I. 2020).

Dari sudut pandang normatif, aktor non-negara dalam dunia siber tidak hanya bisa dilihat sebagai pelaku serangan atau perusuh digital, tetapi juga sebagai pihak yang berperan menjaga etika dan keadilan dalam ruang informasi. Berbagai elemen masyarakat sipil, mulai dari jurnalis independen, *fact-checker,* hingga kelompok masyarakat digital yang peduli pada kebenaran informasi, memainkan peran penting dalam melawan disinformasi dan menjaga integritas wacana publik selama konflik berlangsung. Dengan demikian, penguatan kapasitas dan literasi digital kelompok non-negara sipil menjadi sangat krusial. Mereka berkontribusi dalam membentuk ekosistem informasi yang sehat, serta berfungsi sebagai penyeimbang terhadap dominasi narasi dari negara atau kelompok yang berkonflik. Maka dari itu, dalam dinamika perang siber, aktor non-negara sipil tidak hanya perlu dilindungi, tetapi juga dilibatkan secara strategis dalam kebijakan keamanan informasi nasional (Awan, M. A., et al. 2025).

6. Implikasi Strategis terhadap Stabilitas India-Pakistan dan Kawasan

Konflik siber dewasa ini menegaskan bahwa keamanan nasional tidak lagi dapat dipahami secara sempit dalam kerangka pertahanan militer semata. Strategi keamanan modern harus mencakup aspek informasi sebagai komponen utama, sebab dominasi suatu negara kini sangat dipengaruhi oleh kemampuannya dalam mengelola kekuatan digital serta membangun ketahanan terhadap serangan naratif. Dalam konteks India dan Pakistan, perang digital bukan sekadar alat konfrontasi teknologi, melainkan juga instrumen untuk mempertaruhkan dan menegosiasikan ulang kekuasaan di kawasan Asia Selatan. Dengan demikian, dunia maya menjadi arena persaingan strategis yang memungkinkan kedua negara saling menekan tanpa harus terlibat dalam konflik bersenjata secara langsung (Baek, D. S. 2025).

Meski demikian, strategi perang digital ini bukan tanpa konsekuensi serius. Penggunaan kekuatan siber dalam rivalitas antarnegara berpotensi mempercepat terjadinya krisis politik yang lebih luas, serta menciptakan hambatan serius dalam proses diplomatik. Selain itu, ada bahaya terjadinya miskalkulasi strategis ketika tindakan defensif oleh satu pihak dipandang sebagai provokasi oleh pihak lain. Dalam kerangka teori dilema keamanan, hal ini menciptakan lingkaran aksi-reaksi yang sulit dikendalikan. Pola tersebut terlihat nyata dalam dinamika serangan balasan antara India dan Pakistan, di mana upaya masing-masing pihak untuk meningkatkan pertahanan digital justru memperkeruh eskalasi konflik dan memperlemah stabilitas bilateral (Baek, D. S. 2025).

Dampak jangka panjang dari *cyberwarfare* juga merambah pada aspek yang lebih mendasar, yakni pembangunan kepercayaan antar negara dan masyarakat di kawasan Asia Selatan. Ketika informasi digunakan sebagai senjata, masyarakat mulai meragukan narasi resmi yang disampaikan oleh pemerintah, dan hal ini berdampak langsung pada keefektifan diplomasi regional. Dalam perspektif *regional security complex*, ketegangan antara India dan Pakistan tidak berdampak secara isolatif, melainkan menciptakan resonansi negatif yang dapat mengganggu keseimbangan keamanan secara sistemik di seluruh Asia Selatan. Kerapuhan kepercayaan ini berpotensi menghambat berbagai bentuk kerja sama kawasan, termasuk yang berkaitan dengan isu-isu lintas negara seperti penanggulangan ekstremisme, migrasi, dan perubahan iklim (Baloch, R. 2019).

Oleh sebab itu, sangat penting bagi negara-negara di kawasan ini untuk mulai merancang pendekatan keamanan yang lebih holistik dan adaptif terhadap tantangan era digital. Diplomasi digital harus dikembangkan secara lebih terbuka dan akuntabel, agar dapat membangun dialog yang berbasis pada transparansi dan kolaborasi. Penguatan norma internasional dan pembentukan kerangka hukum siber regional menjadi kebutuhan mendesak guna menetapkan

batas-batas perilaku negara di ruang siber. Selain itu, kerja sama antar negara dalam menghadapi ancaman siber non-tradisional, seperti serangan dari aktor non-negara atau penyebaran disinformasi, perlu ditingkatkan. Hanya dengan membangun arsitektur keamanan kawasan yang responsif terhadap perkembangan teknologi dan ancaman informasi, perdamaian dan stabilitas jangka panjang di Asia Selatan dapat benar-benar terjaga (Shabbir, S., Fatima, H., Malik, S., Khan, A. U., & Zheng, M. 2022).

KESIMPULAN

Konflik India–Pakistan pasca-serangan Pahalgam 2025 memperlihatkan bahwa medan perang modern telah meluas ke ruang digital yang tak berbatas. Setelah serangan fisik di Kashmir, kedua negara langsung terlibat dalam pertarungan siber yang mencakup penyebaran propaganda, disinformasi, dan serangan daring. Perang kini bukan hanya soal kekuatan militer, tapi juga soal pengaruh atas narasi publik, legitimasi politik, dan citra internasional. Aktor non-negara dan platform digital turut memperkuat dinamika ini, menjadikan dunia maya sebagai arena konflik politik, identitas, dan persepsi.

Secara strategis, *cyberwarfare* membuat konflik India–Pakistan semakin asimetris dan sulit dikendalikan. Ketegangan ini mengancam stabilitas Asia Selatan karena disinformasi lintas negara dan keterlibatan aktor informal melemahkan kepercayaan publik serta menghambat kerja sama regional. Maka, tantangan ke depan mencakup penguatan pertahanan digital, pembentukan kerangka kerja sama siber regional, diplomasi digital yang aktif, serta kolaborasi lintas sektor untuk membangun sistem pertahanan informasi yang kuat dan terpercaya.

DAFTAR PUSTAKA

Ahmad, S., & Jahangir, J. (2023). Cyber warfare: Emerging non-traditional threat to Pakistan's security. *Pakistan Horizon,* 76(2), 39–58.

Ashraf, M. N., & Kayani, S. A. (2023). India's cyber warfare capabilities: Repercussions for Pakistan's national security. *NDU Journal*, 37, 34–45. [ISSN: 2073-0926]

Babar, S. I., Mirza, M. N., & Qaisrani, I. H. (2021). Evaluating the nature of cyber warfare between Pakistan and India. *Webology,* 18(6), 6973–6985.

Baloch, R. (2019). Cyber warfare trends, tactics and strategies: Lessons for Pakistan. *Journal of Development Policy Research & Practice,* 1, 23–43.

Baek, D. S. (2025). Cyber warfare in the May 2025 India–Pakistan conflict. *LinkedIn Articles.* Retrieved from https://www.linkedin.com/pulse/cyber-warfare-may-2025-india-pakistan-conflict-david-sehyeon-baek-ygjoc/

Farooq, A., & Ali, A. (2022). India's growing cyber partnerships and challenges for Pakistan. *Margalla Papers*, 26(2), 49–61. [ISSN: 1999-4396]

Ghernaouti-Helie, S. (2013). Cyber power: Crime, conflict and security in cyberspace. Lausanne: *EPFL Press.* [ISBN: 9782940222460]

Imran, M., Murtiza, G., & Akbar, M. S. (2022). The rise of cyber crime in Pakistan: A threat to national security. *Journal of Development and Social Sciences,* 3(4), 631–640. [ISSN: 2788-3571]

Mirza, M. N., & Babar, S. I. (2020). The Indian hybrid warfare strategy: Implications for Pakistan. *Progressive Research Journal of Arts and Humanities* (PRJAH), 2(1), 39–52.

Mustafa, G., Murtaza, Z., & Murtaza, K. (2020). Cyber warfare between Pakistan and India: Implications for the region. Pakistan Languages and Humanities Review, 4(1), 59–71. [ISSN: 2663-9214]

Nye, J. S. (2004). Soft power: The means to success in world politics. *New York: PublicAffairs.* [ISBN: 9781586483067]

Relia, S. (2015). Cyber warfare: Its implications on national security. *New Delhi: Vij Books India.* [ISBN: 9789384464736]

Shabbir, S., Fatima, H., Malik, S., Khan, A. U., & Zheng, M. (2022). Cyber warfare from Pakistan-India: A critical analysis. *International Journal of Special Education,* 37(3), 2452–2458.

Zahoor, R., & Razi, N. (2020). Cyber-crimes and cyber laws of Pakistan: An overview. *Progressive Research Journal of Arts and Humanities,* 2(2), 133–143. [ISSN: 2707-731]