Journal of International Relations, Volume 5, Nomor 4, 2019, hal 764-771
Online di http://ejournal-s1.undip.ac.id/index.php/jihi

Analisis Persepsi Keamanan Nasional India Terhadap Serangan Siber dari Pakistan 2008-2017

Ratna Ayu Paramitha Pratiwi
Departemen Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Diponegoro
Jalan Prof. H. Soedharto, SH, Tembalang, Semarang, Kotak Pos 1269
Website: http//www.fisip.undip.ac.id Email: fisip@undip.ac.id

ABSTRACT

The conflict between India and Pakistan has occurred before independent both of those countries, then continued until they involved in complex pattern of conflict. The development of information and communication technology has influenced on developments leading to cyber conflicts. This conflict makes the perception of India's national security needs to be revised again. In this study, writer discusses Indian cyber security after the Pakistani cyber attack, and looks at India's actions in the cyber attack. This research uses a qualitative method using descriptive. Using Barry Buzan's security theory where individuals and states can be subject and object of reference. The results showed that cyber attacks from Pakistan led to India's critical infrastructure (CI), the existential threats in this case not physical but as cyber. The perception of cyber threats from Pakistan regarded India as confrontation to deal with conflict. Based on this perception has a significant influence of act the of Indian cyber security. Then the writer also looks at Indian national security measures involving non-state actors involved in cyber conflicts with Pakistan.

Keywords: *Perception, Indian Cyber Security, Pakistani Cyber Attack, National Security.*

PENDAHULUAN

Terjadinya suatu konflik diharapkan berakhir dengan perdamaian. Johan Galtung membagi perdamaian menjadi dua yaitu perdamaian negatif dan perdamaian positif. Perdamaian negatif ditandai dengan ketidakhadiran kekerasan sedangkan perdamaian positif ditandai dengan kehadiran harmonis baik disengaja atau tidak dari beberapa aspek (GPI 2018). Menurut IEP (*International for Economic and Peace*) terdapat delapan aspek yang menentukan perdamaian positif yakni pemerintahan yang berfungsi dengan baik, penguatan kondisi ekonomi, keadilan distribusi sumber daya, kebebasan arus informasi, tingkat korupsi rendah, penerimaan hak-hak asasi, tingkat pendidikan, dan hubungan yang baik antar tetangga (GPI 2018).

Global Peace Index (GPI) 2016 menyebutkan wilayah regional Asia Selatan termasuk wilayah tidak damai dengan nilai rata-rata 2,4. Data tersebut, mengindikasikan konflik masih terjadi walaupun perang antara negara berkurang. Konflik kontemporer bisa terjadi dengan negara tetangga. Terdapat tiga indikator mengenai hubungan yang baik antar tetangga, yaitu permusuhan terhadap orang asing dengan mengukur sikap sosial masyarakat terhadap orang asing dan properti pribadi, jumlah kunjungan orang asing, dan integrasi regional dengan mengukur sejauh mana integrasi berbasis perdagangan suatu negara dengan negara lain (GPI 2018). Kencenderungan antar negara tetangga terlibat konflik dapat

disebabkan oleh beberapa faktor antara lain, faktor sejarah, geografis, geopolitik, agama, politik, keamanan, dan persaingan pengaruh. Terjadi fluktuasi konflik antar tetangga dari tahun 2008 hingga 2014 (GPI 2018). Namun, kecenderungan konflik antar negara tetangga di dunia semakin mengingkat sejak tahun 2015. Pada tahun 2016 nilai Pakistan pada *good neighbourhood country* 4.63, sedangkan India 2.97. Penilaian terdiri dari 1 sampai 5 dengan nilai 1 berarti semakin baik hubungannya dan nilai 5 semakin buruk.

Perkembangan teknologi informasi di masa kini menyebabkan konflik tidak hanya terjadi secara konvensional tetapi melalui siber. Pada awal tahun 2019, pengguna internet dunia terus mengalami peningkatan sebanyak 4,4 milyar pengguna (www.internetworldstats.com, 2019). Banyaknya penguna internet kemudian dijadikan celah oleh kelompok peretas untuk melakukan aktivitas yang berdampak negatif di dunia maya yakni serangan siber seperti kejahatan siber, *hacktivism*, perang siber, terorisme siber dan lainnya. Konflik dunia maya dapat dilakukan antar individu-individu, individu-grup, individu-pemerintah, grup-grup, grup-peremerintah, dan pemerintah-pemerintah. 75 persen rival siber dunia adalah rival dalam wilayah regional dan 93 persen rival siber regional mempunyai masalah isu teritori (Huth and Allee 2009; Ghosn, Palmer and Bremer 2004 dalam Brandon Valeriano dan Ryan C. Maness, 2015). Salah satu konflik konvensional yang berkembang ke arah konflik siber yang melibatkan negara tetangga adalah konflik India-Pakistan yang terjadi sejak tahun 1947 hingga sekarang. India dan Pakistan masuk dalam 10 besar negara yang terdampak serangan siber (Symantec*,* 2019).

Konflik siber antara India dan Pakistan sudah mulai sejak tahun 1997. Pada saat itu terjadi serangan saling retas antara peretas kelompok dari India dan Pakistan. Kelompok peretas India bernama NEO, sedangkan peretas Pakistan bernama PHC (*Pakistan Hackers Club*) yang beranggotakan dua orang Doctor Nuker and Mr_Sweet (Hopper, I. D., 1999) dan Gforce. Peretas India, NEO dan Pakistan, PHC serta Gforce saling serang dengan menggunakan tekhnik *defacement* dengan bentuk *hacktivism*. Fenomena peningkatan serangan siber yang terjadi di India telah mengancam keamanan nasional India. Menteri Komunikasi dan Teknologi Informasi, Ravi Shankar Prasad, mengatakan bahwa sebagian besar serangan berasal dari Pakistan (The Economic Times, 2015).

Berdasarkan pemaparan tersebut, maka penelitian ini bertujuan untuk menganalisis persepsi keamanan nasional India terhadap serangan siber dari Pakistan pada tahun 2008-2017. Menggunakan kerangka pemikiran keamanan Barry Buzan dimana keberadaan ancaman serangan siber akan dipersepsikan oleh subjek, subjek disini bisa berasal dari individu dan Negara serta dapat dilihat tindakan yang diambil.

PEMBAHASAN

Dinamika Konflik India-Pakistan

Konflik India-Pakistan disebabkan oleh beberapa permasalahan antara lain 1) masalah geografis yaitu perebutan wilayah Kashmir, 2) masalah agama yaitu adanya konflik dua agama Hindu dan Islam, 3) masalah keamanan dimana Pakistan merasa terancam dengan India sehingga perlu mempersenjatai diri, dan 4) masalah persaingan pengaruh dimana kedua negara berusaha untuk memberikan pengaruh di kawasan Asia Selatan (Ahmad Mir, 2014). Konflik antara India dan Pakistan telah mengakar kuat karena telah terlibat perang perbatasan sebanyak tiga kali, telah mencapai perang keempat, serta kemungkinan untuk konflik nuklir (Mirza, 2009). Konflik perbatasan pertama terjadi Oktober 1947 ketika anggota suku dari Pakistan datang untuk mendukung Muslim Kashmir yang memberontak keputusan Maharaja Hari Singh yang melakukan penandatanganan aneksasi pada pihak India (Muhammad Iqbal Muhammad Zubair, Shabir Hussain 2018). Konflik kedua terjadi tahun 1965 di wilayah garis batas negara "*the line borders*", Pakistan menyusupkan orangnya melewati teritori Kashmir

milik India dengan tujuannya untuk mempengaruhi warga Kashmir di wilayah itu agar memberontak. Konflik perbatasan ketiga pada 1984, Pasukan India merebut Gletser Siachen, wilayah terpencil dan tak berpenghuni di Karakoram Range yang juga diklaim Pakistan. Konflik perbatasan keempat yakni konflik Kargil terjadi pada Mei-Juli 1999, pemberontak Kashmir bersama dengan tentara Pakistan berusaha menyebrangi garis batas dan merebut pos tentara India grup pakistan menyebrangi "*the line control*" di wilayah Kargil, Kahsmir. Perlombaan persenjataan nuklir dimulai dari pihak Pakistan pada tahun 1972 dan India pada tahun 1974, intensitas ketegangan dengan adanya peningkatan aktivitas pengembangan nuklir terjadi pada 1998 hal ini mengakibatkan naiknya ketegangan di regional Asia Selatan.

Kelompok peretas Pakistan kebanyakan menyerang *critical infrastructures* (CI) India. Infrastrukur kritis berupa sistem vital bagi suatu negara sehingga ketidakmampuan atau kehancurannya akan berdampak buruk pada keamanan nasional dapat berupa jaringan internet yang menjadi perangkat beberapa sektor tersebut (Kuerbis, Brenden 2007). Perkembangan Teknologi Melalui Dunia Maya Membuat Informasi tidak hanya dilakukan secara tradisional tetapi juga secara modern dengan jaringan system informasi online. Oleh karena itu berkembang menjadi infrastruktur informasi kritis atau *critical information infrastructures* (CII) dimana saling berhubungan dengan infrasturktur kritis dan informasi infrastruktur. Terdapat tiga belas sektor CI India, yakni: pertanian dan makanan, perbankan dan keuangan, telekomunikasi, industri manufaktur kritis, industri pertahanan, pelayanan darurat, energi, kesehatan, teknologi informasi, monumen dan ikon nasional, pengiriman, transportasi, persediaan air (Abhishek Singh, Narain, M.P.Gupta, Amitabh Ojha, 2014).

Tabel 1. Matrix Ancaman Infrastruktur

Alat	*Target*	
	Fisik	Siber
Fisik	Memutuskan kabel telekomunikasi dengan *backhoe* Menghancurkan server dengan *hammer* Mengebom jaringan listrik	Penggunaan pulsa elektromagnetik dan senjata frekuensi radio untuk mengacaukan komponen elektronik
Siber	Meretas ke dalam sistem SCADA yang mengontrol pembuangan kotoran kota *'Spoofing'* sistem kontrol lalu lintas udara untuk menjatuhkan pesawat.	Meretas ke dalam jaringan pemerintah yang kritis. *Trojan horse* di jaringan switch publik

Sumber: Devost et al. 1997, OCIPEP 2003 dalam Cavelty 2008.

Tabel 1 memperlihatkan bahwa ancaman infrastruktur India dapat kategorikan pada kurva kanan bawah. Penggunaan alat siber dengan target siber dapat dicontohkan dengan adanya peretasan pada CI India oleh karena itu sifat ancaman kebanyakan tidak terlihat secara nyata. Motivasi peretasan yang digunakan yakni *hacktivism*, kejahatan siber, perang siber, dan *cyber espionage*. Contoh *hacktivism* terjadi pada perusahaan telekomunikasi BSNL pada 2011, peretas berhasil mendapat 10.000 informasi pengguna termasuk nama, alamat email, lokasi, nomor telepon, serta berhasil meretas halaman internal BSNL yang berisi perincian kerja internal VPN (Anupam Saxena, 2011). Kerugian yang timbulkan akibat serangan siber di India pada kasus *cyber crime*, berdasarkan Statistik kejahatan siber tahunan yang dirilis oleh Norton melaporkan bahwa India memperoleh kerugian senilai 8 miliar Dollar pada 2011 sedangkan jumlah rata-rata tahunan kejahatan cyber diperkirakan mencapai 42 juta INR (Chabbra, 2014). kasus cyber espionase tahun 2016 yang dilakukan oleh pemerintah Pakistan berdampak pada pembocoran data negara India kepada media atau pemerintah Pakistan untuk tujuan politik. *Cyber warfare*, merupakan konflik yang terjadi

dimana terdapat dua kelompok peretas dari kedua negara melakukan *tit for tat* (serangan tersebut terjadi saling serang yang berasal dari balas dendam) seperti, kasus *cyber warfare* tahun 2008 dimana peretas dari kedua Negara saling meretas.

Sebuah ancaman dapat terjadi secara langsung maupun membutuhkan waktu untuk berdampak (Buzan, 1983). Tidak ada cara yang dapat digunakan untuk menilai risiko dari ancaman-ancaman ini, bergantung tingkat prioritas dan kedekatan yang dimiliki aktor. Dalam serangan siber banyak tidak menjadi ancaman langsung bagi fisik suatu sektor CI akan tetapi menjadi ancaman langsung terhadap sistem jaringan CII karena faktor lemahnya sistem keamanan jaringan sehingga mudah untuk diretas.

Analisis Persepsi Keamanan Nasional Siber India terhadap Serangan Siber Pakistan

Rivalitas India-Pakistan memunculkan permasalahan yang kompleks karena konflik siber tidak hanya pertarungan keamanan kedua negara tetapi juga keterlibatan aktor non negara. Perkembangan teknologi informasi dengan cepat diintegrasikan ke dalam strategi kedua negara; memanfaatkan ruang maya telah menjadi alat yang berguna bagi India dan Pakistan. Cyberspace telah menjadi ruang di mana peretas yang berjiwa patriotik dari kedua belah pihak dapat mengekspresikan perasaan patriotisnya dengan tujuan merendahkan musuh. Bahkan, Cyberspace juga bertindak sebagai sarana untuk Advanced Persistent Threats (APTs), yang merupakan kelompok-kelompok yang memiliki hubungan yang sangat mungkin dengan lembaga-lembaga negara, untuk memata-matai dan mendapatkan informasi tentang lawan mereka (Baezner, 2018).

Politik luar negeri India dan Pakistan dipengaruhi oleh warisan sejarah dan kontradiksi ekonomi, politik dan agama. Permusuhan dan kecurigaan masa lalu dari para pembuat kebijakan India dan Pakistan telah terbiasa melihat masalah hubungan bilateral dari sudut pandang keamanan (Ahmar, Moonis 1984). Secara umum presepsi India terhadap Pakistan ketika dipandang melalui hubungan rivalitas maka Pakistan merupakan ancaman keamanan bagi india khususnya setelah perang Kargil dan meningkatnya kasus terorisme di India (Dixit, 2002). Persepsi beberapa orang India percaya bahwa Pakistan adalah produk kesalahan sejarah atau konspirasi British dan akan segera runtuh karena keadaan ekonomi, politik, sosial dan militer yang tidak menguntungkan. Sedangkan dalam keamanan siber penyerangan aktor non-negara merupakan bentuk perlawanan dari hasil kumpulan permusuhan secara historis yang sudah lama terjadi. India memandang negaranya sebagai korban perang siber strategis melalui provokasi yang disengaja atau melalui eskalasi perang siber yang dimulai penyerang (Relia, 2015).

Untuk melihat presepsi India terhadap ancaman keamanan nasional yang berasal dari serangan siber Pakistan adalah dengan melihat tanggapan terhadap serangan teroris. Pakistan terus mensponsori terorisme sebagai kebijakan negara (Hooda, 2019). Pertimbangan besar terhadap Pakistan India dapat dengan baik memutuskan untuk bereaksi terhadap terorisme yang disponsori Pakistan di Jammu dan Kashmir dengan melakukan serangan siber strategis. Ketidaksabaran India yang meningkat dan respons yang kuat terhadap insiden teror berpotensi meningkatkan situasi yang konfliktual. Provokasi dapat dilakukan bahkan dalam skenario di mana negara yang menyerang secara sadar dan bahkan secara terang-terangan melakukan serangan terhadap yang lain di dunia maya tidak hanya untuk melakukan provokasi tetapi menahan diri dari kekerasan fisik.

Menurut (Relia, 2015) terdapat dua sudut pandang India terhadap serangan Pakistan yaitu pertama, ketika tantangan keamanan, kekuatan India berada di domain asimetris seperti dunia maya, nuklir dan ruang angkasa yang tidak hanya membutuhkan kemampuan penciptaan dan desain tetapi penggunaan kemampuan itu sendiri. Kedua masalah keamanan siber tidak dapat dikesampingkan India. Ada kebutuhan yang sangat besar untuk melakukan

modernisasi dan revolusi kekuatan militer dan reformasi keamanan internal yang diperlukan untuk mempertahankan masyarakat dan ekonomi India yang semakin kompleks.

Tindakan dalam Persepsi Keamanan India

Persepsi masalah oleh aktor memiliki dampak yang menentukan pada keyakinan dan tindakan mereka (Cavelty, 2008). Serangan siber Pakistan menghasilkan persepsi bahwa tujuan untuk konfrontasi secara langsung dalam *cyberspace*. Konfrontasi dilatarbelakangi oleh patriotisme dan permusuhan antara kedua negara. Dengan kata lain, konfrontasi tersebut merupakan serangan non-fisik untuk memicu penyelesaian sengketa teritorial dan memperoleh pengaruh di Asia Selatan. Kemudian hasil dari penjabaran konseptual tersebut menghasilkan keamanan dapat terjadi dengan melakukan perbaikan pada tindakan yang dilakukan pemerintah India rasional bagi India terhadap serangan Pakistan adalah dengan keamanan yang bersifat defensif. Pertimbangan tersebut dipilih karena keamanan siber Pakistan tidak memberikan dampak kekerasan secara langsung, walaupun India memperoleh kerugian terhadap serangan Pakistan. Keamanan siber defensive dimaksudkan untuk meningkatkan kemampuan Negara untuk menangkal serangan siber dan menciptakan lingkungan internet yang baik bagi masyarakat (Lewis, 2015). Keamanan defensif lebih banyak dalam menciptakan perlindungan sistem internet, dan mengurangi kerusakan dari serangan siber dari negara lain.

Selain itu tindakan pemerintah India dapat dilihat dalam pembuatan Undang-Undang, institusi, serta penyataan resmi pemerintah. Pertama undang-undang, penguatan kerangka regulasi yang tepat dalam pengaturan ekosistem siber yang baik serta memastikan bahwa perlindungan hukum tersedia. India membentuk beberapa badan serta regulasi yang menangani masalah siber. Regulasi yang pertama dengan membuat Undang-undang Informasi Teknologi pada 2000. Kemudian pada 2008 pemerintah India mulai mengamandemen Undang-Undang Informasi Teknologi karena saat itu terjadi peningkatan serangan siber terhadap infrastruktur kritis India. Amandemen bertujuan untuk membuat perubahan revolusioner dalam kerangka hukum siber India yang ada, termasuk penggabungan Electronic Signature yaitu memungkinkan otentikasi catatan elektronik dengan teknik tanda tangan elektronik apa pun (Vikas Asawat, 2010).

Pada 2013 Pemerintah India mengeluarkan Kebijakan Keamanan Siber Nasional dengan visi untuk membangun dunia maya yang aman dan tangguh untuk warga negara, bisnis, dan pemerintah. Misi untuk melindungi informasi dan infrastruktur informasi di dunia maya, membangun kemampuan untuk mencegah dan menanggapi ancaman dunia maya, mengurangi kerentanan dan meminimalkan kerusakan dari insiden dunia maya melalui kombinasi struktur kelembagaan, orang, proses, teknologi, dan kerja sama.

Kedua yakni, institusi dengan membentuk badan NIB ((National Information Board) pada tahun 2002 yang merupakan lembaga dibawah eksekutif. Terdapat dua organisasi yang memengang peranan penting dalam lingkungan keamananan siber India yakni National Technical Research Organisation (NTRO) dan National Critical Information Infrastructure Protection Centre (NCIIPC) (E. Dilipraj, 2015). NCIIPC didirikan tahun 2013 sebagai mekanisme untuk mendapatkan infromasi terhadap ancaman infrastruktur TIK. Sebagai badan yang beroperasi penuh selama 24 jam setiap harinya untuk mengawasi beberapa sektor yakni: Air Traffic Management and civil Aviation, Power grid, NSEI, MTNL, BSNL, Railways, SBI (State Bank of India).

NCIIPC merupakan perlindungan terhadap sistem yang disediakan atau dioperasikan oleh penyedia infrastruktur penting, seperti energi, telekomunikasi, dan departemen air. NCIIPC memastikan bahwa sistem dan jaringan tersebut terlindungi dan tahan terhadap risiko keamanan informasi, risiko keamanan jaringan, risiko keamanan internet, serta risiko

keamanan siber. Ini juga mencakup keamanan Teknologi Informasi dan Komunikasi. Keamanan siber atau keamanan cyberspace telah didefinisikan sebagai pelestarian kerahasiaan, integritas, dan ketersediaan informasi di *cyberspace*.

Pernyataan pemerintah, Menurut Shri Shyam Saran (Relia, 2015) Pemimpin *National Security Advisory* menyatakan '*Cyber attacks on critical civilian infrastructure may have consequences far more significant than damage to military activities are heavily reliant on civilian infrastructure such as the transport network*.' Serangan siber Pakistan bahkan lebih besar dapat mempengaruhi kehidupan masyarakat yang saat ini sangat bergantung pada penggunaan Internet dan teknologi informasi. Untuk mendukung argument tersebut, lebih jauh Pidato Sachin sebagai *Minister of State for Communications and Information Technology* dalam Konferensi Cyberspace di London menyatakan dengan jelas bahwa bahwa:

Ensuring cyber and IT security is hard because networks can be attacked from anywhere in the world, and the motives to attack them may include simply demonstrating technical prowess, casual hacking, political orientation, fraud, crime or an extension of state conflict (IDSA, 2012).

Untuk mengamankan dan menciptakan konfigurasi ekosistem keamanan siber, India saat ini telah menjalankan tindakan yaitu: 1) memengembangkan keterampilan keamanan siber dengan mendorong kurikulum keamanan siber yang diperkenalkan di perguruan tinggi; 2) Kebijakan Penelitian dan Pengembangan (R&D) Keamanan Siber yang telah menjadi pertimbangan aktif pemerintah India; 3) India sedang mengejar diplomasi dunia maya aktif dengan mengadakan dialog keamanan siber dengan beberapa negara dan berpartisipasi dalam beberapa forum internasional termasuk PBB tentang keamanan siber (Samuel dan Sharma, 2016). Setidaknya lebih dari dua tahun India teah menginisiasi dialog keamanan siber dengan beberapa Negara diantaranya yakni Uni Eropa, Malaysia, Singapura, Amerika, Jerman, Korea Selatan, Jepang, Australia, Uni Emirat Arab, dan Mongolia.

Keamanan siber India juga berimplikasi terhadap peningkatan aktivitas siber dalam negeri yang kemudian menjalankan Operasi Hangover. Operasi tersebut bermakna sebagai aktivitas kelompok non-negara yang melakukan tindakan peretasan terhadap Pakistan. Operasi ini merupakan bentuk serangan balasan dari India karena adanya jiwa patriotisme di masyarakat India. Operasi Hangover terdeteksi pertama kali oleh perusahaan keamanan siber asal Norwegia, Norman. Serangan ini dilakukan oleh swasta tidak ada bukti keterlibatan sponsor negara diperkirakan telah berlangsung sejak 2010 (Paganini, Pierluigi, 2013). Dijuluki "Operation Hangover" karena penggunaan kata "hangover" ada dalam string teks yang dimasukkan dalam banyak sampel malware terdeteksi (Kaplan, 2013).

Negara yang terdampak serangan *Operation Hangover*, peringkat pertama bahwa Pakistan menjadi negara teratas yang terkena serangan *operasi Hangover* 71 persen. Disusul oleh India, United Arab Emirates, dan Switzerland dengan masing-masing persentase sebesar 5 persen. Saudi Arabia dan Bangladesh terdampak 4 persen. Amerika dan Spanyol sebesar 2 persen. Inggris Raya dan China hanya sebesar 1 persen. Berdasarkan data tersebut menyimpulkan bahwa Operasi hangover yang dijalankan oleh kelompok non negara yang berasal dari India adalah bertujuan untuk menambah tensi konflik kedua negara, serta sebagai bentuk konfrontasi balasan terhadap serangan siber Pakistan.

Menurut Baezner (2018) aktivitas kelompok India banyak didasarkan pada perteas yang memiliki jiwa patriotik sehingga disebut sebagai peretas patriotik. Peretas patriotik India sebagian besar diidentifikasi bertindak untuk membela kepentingan India di dunia maya. Peretas dan peretas patriotik India biasanya menghancurkan situs web di situs web pemerintah Pakistan. Peretas patriotik telah mengklaim serangan ransomware di bandara dan situs web pemerintah Pakistan (Shukla, 2017). Selain itu, tercatat melakukan dua kali cyber

espionage pada tahun 2013. Pertama dengan insiden Telenor Pakistan yang berlangsung 17 Maret 2013. Kedua, insiden tranchulas pada tanggal 1 Februari 2013 hingga 7 Februari 2013 (Valeriano, B., & Maness, R. C 2015). Salah satu kelompok yang teridentifikasi dalam penyerangan terhadap Pakistan adalah Mallu Cyber Soldier (MCS). MCS adalah kelompok peretas patriotik yang menonjol karena besarnya intensitas serangan yang telah dilakukan. MCS adalah sekelompok pakar keamanan cyber India yang bertujuan melindungi situs web India dari serangan cyber negara lain (Baezner, 2018). Grup ini memberi tahu administrator situs web tentang kerentanan dan membantu mereka memulihkan situs web yang rusak. MCS juga menanggapi serangan dunia maya dengan merusak situs-situs Pakistan sebagai balasannya (Baezner, 2018). Anggota kelompok mengklaim bahwa MCS benar-benar independen dan tidak berfungsi untuk negara India.

KESIMPULAN

Konflik India-Pakistan telah mengakar hingga menyebabkan beberapa perubahan pola konsep keamanan antara kedua negara. Seiring dengan peningkatan perangkat teknologi informasi dan komunikasi, konsep keamanan kedua negara juga mengalami perluasan yang tidak hanya berkenaan terhadap isu keamanan tradisional seperti konflik perbatasan, perang, dan perlombaan senjata nuklir tetapi juga meluas hingga ke konsep keamanan siber.

Keamanan siber menjadi penting karena mengingat bahwa tidak ada batas kedaulatan dalam siber, serta konflik yang lebih banyak dipelopori oleh aktor non negara. Dalam isu kontemporer, keamanan India dihadapkan oleh serangan siber dari Pakistan yang berdampak pada infrastruktur kritis serta tensi kedua negara. Jenis serangan siber dari Pakistan yang banyak adalah untuk motivasi *hacktivism, cyber crime, cyber warfare, cyber espionage*. Dengan banyaknya bentuk serangan siber tersebut membuat keamanan nasional India perlu di konseptualisasikan melalui pendekatan keamanan.

Penelitian ini merujuk pada keamanan siber India yang menemukan bahwa keamanan siber India terhadap serangan siber Pakistan dianalisis melalui aktor yang terlibat adalah kelompok militan siber dan India sebagai negara yang merumuskan keamanan sibernya. Perubahan makna keamanan India terhadap serangan siber Pakistan ditinjau melalui persepsi terhadap ancaman terhadap serangan siber Pakistan dapat ditinjau dari hubungan konfliktual kedua negara, ditentukan melalui adanya keyakinan bahwa Pakistan dan kelompok peretas melakukan konfrontasi terhadap siber India sehingga mengancam infratruktur kritis. Perspektif India terhadap ancaman dari Pakistan dipengaruhi karena alasan warisan sejarah dan kontradiksi ekonomi, politik, agama terbawa hingga saat ini.

Berdasarkan persepsi keamanan tersebut kemudian melihat bahwa India melakukan tindakan keamanan siber nasional yang bersifat *defensive*. Pertimbangan tersebut dipilih karena keamanan siber Pakistan tidak memberikan dampak kekerasan secara langsung, walaupun India memperoleh kerugian terhadap serangan Pakistan. Selain itu, tindakan India mengeluarkan regulasi Tahun 2000 yang terus mengalami beberapa perubahan hingga menghasilkan regulasi keamanan siber tahun 2013. Selain menyusun regulasi tersebut pemerintah juga mengupayakan penciptaan ekosistem siber yang aman melalui pembentukan beberapa badan yang saling berkoordinasi dalam melindungi ekosistem siber India seperti National Critical Information Infrastructure Protection Centre (NCIIPC) dengan menerapkan ISO 27032. Selain peran negara, kelompok patriotis India atas dasar nasionalisme kemudian melakukan serangan siber balasan yang disebut sebagai *Operasi Hangover*. Operasi offensive tersebut memicu timbulnya siber warfare kedua negara, yang berdampak pada peningkatan tensi yang tidak hanya terjadai di dunia nyata akan tetapi juga di dunia siber.

REFERENSI

Asawat, Vikas. (2010). Information Technology (Amendment) Act, 2008: A New Vision through a New Change.

Baezner, M. (2018). Hotspot Analysis: Regional rivalvy between India-Pakistan: tit-for-tat in cyberspace. Zurich.

Buzan, Barry. (1983). People, State, and Fear The National Security Problem in International Relations. Great Britain: Wheatsheaf Books LTD.

Cavelty, M. D. (2008). *Cyber-Security and Threat Politics US Efforts to Secure the Information Age.* New York: Routledge.

Chhabra, Captain Sanjay. (2014). India's National Cyber Security Policy (NCSP) And Organisation – A Critical Assessment Naval War College Journal.

Cyber attacks on India mostly from Pakistan, China: Government. (2015). Diakses dari <www.economictimes.indiatimes.com/news/defence/cyber-attacks-on-india-mostly-from-pakistan-china-government/articleshow/48392113.cms>

Dixit, J. N. (2002). *India-Pakistan in War & Peace* (1 ed.). New York: Routledge.

Hopper, D. Ian. (1999), 'Kashmir-minded Pakistani 'hacktivists' blitz Web sites', diakses dari <http://edition.cnn.com/TECH/computing/9910/08/pakistani.hack/>.

Institute for Economics & Peace. (2018). Global Peace Index Measuring Peace in a Complex World, Sydney, June 2018.

Kaplan, D. (2013). *Espionage hacking campaign "Operation Hangover" originates in India*. Diakses dari <www.scmagazine.com/home/security-news/espionage-hacking-campaign-operation-hangover-originates-in-india/>

Karatzogianni, A. (2009). *Cyber Conflict and Global Politics.* New York: Routledge.

Mir, Mushtaq Ahmad. (2014). India-Pakistan; the History of Unsolved Conflicts. IOSR Journal of Humanities And Social Science.

Paganini, Pierluigi. (2013). Operation Hangover, the Indian Cyberattack Infrastrusture. Diakses dari <https://securityaffairs.co/wordpress/14550/cyber-crime/operation-hangover-indian-cyberattack-infrastructure.html>

Relia, Sanjeev. (2015). *Cyber Warfare Its Implications on National Security* . New Delhi: Vij Books India Pvt Ltd.

Singh, Abhishek Narain, M. P. Gupta, Amitabh Ojha. (2012). Identifying critical infrastructure sectors and their dependencies: An Indian scenario.

Samuel, Cherian & Munish Sharma. (2016). *Securing Cyberspace: International and Asian Perspectives.* New Delhi: Institute for Defence Studies and Analyses.

Symantec. (2019). *Internet Security Threat Report*. Volume 24: February 2019.

Valeriano, B., & Maness, R. C. (2015). *Cyber War Versus Cyber Realities Cyber Conflict in the International System.* New York: Oxford University Press.

World Internet Usage and Population Statistics. (2019). Diakses dari <www.internetworldstats.com/stats.htm>.