©2023 Indonesian Journal of International Relations
Vol. 7, No. 1, pp. 140-164.
DOI: 10.32787/ijir.v7i1.408

STRATEGI KEAMANAN SIBER PEMERINTAH INDIA DARI PERSPEKTIF KAUTILYA: SERANGAN SIBER MUMBAI 2020

Renatha Ayu Rossdiana
Magister Hubungan Internasional, Universitas Airlangga, Surabaya, Indonesia
renatha.ayu.rossdiana-2021@fisip.unair.ac.id

Titing Reza Fahrisa
Magister Hubungan Internasional, Universitas Airlangga, Surabaya, Indonesia
titing.reza.fahrisa-2021@fisip.unair.ac.id

INFO ARTIKEL

Article History

Received

1 September 2022

Revised

20 February 2023

Accepted

10 March 2023

Kata kunci:

India; Kautilya; keamanan siber; serangan siber Mumbai.

Keywords:

India; Kautilya; cybersecurity; Mumbai cyber-attack.

Abstract

This paper aims to elaborate on the Indian Government's cybersecurity strategy from Kautilya's perspective by taking the example of the Mumbai cyberattack case in 2020. By using the classic Kautilya war strategy concept which is relevant to be applied in the contemporary era and beyond conditions of physical war and written with a qualitative research methodology. The research results show that the 2020 Mumbai cyberattacks affected India's national security in economic security, national defense and foreign relations. Weak cyber defenses cause India to suffer socio-economic losses. Therefore, the Government of India seeks to strengthen cyber resources, from the economic, defense and foreign relations perspective, by taking a defensive position to maintain good relations with other countries and implementing cyber diplomacy both bilaterally and multilaterally as a cyber security strategy.

Abstrak

Tulisan ini bertujuan untuk mengelaborasi strategi keamanan siber Pemerintah India dalam perspektif Kautilya dengan mengambil contoh kasus serangan siber Mumbai tahun 2020. Dengan menggunakan konsep strategi perang klasik Kautilya yang relevan diterapkan di era kontemporer dan di luar kondisi perang fisik dan ditulis dengan metodologi penelitian kualitatif. Hasil penelitian menunjukkan bahwa serangan siber Mumbai 2020 memengaruhi keamanan nasional India dalam keamanan ekonomi, pertahanan negara dan hubungan luar negeri. Pertahanan siber yang lemah menyebabkan India menderita kerugian sosio ekonomi. Oleh karena itu, Pemerintah India mengupayakan penguatan sumber daya siber, dari sisi ekonomi, pertahanan dan hubungan luar negeri, dengan mengambil posisi defensif untuk menjaga hubungan baik dengan negara lain dan menerapkan diplomasi siber baik bilateral maupun multilateral sebagai strategi keamanan siber

ISSN: 2548-4109 electronic
ISSN: 2657-165X printed

PENDAHULUAN

Kebutuhan terhadap keamanan siber (*cybersecurity*) semakin relevan dan krusial di era globalisasi terutama dalam kaitannya dengan keamanan nasional. Revolusi telekomunikasi dan teknologi menyediakan berbagai peluang perkembangan ekonomi namun juga mempunyai resiko tinggi ancaman peretasan serius, kejahatan siber terorganisir, ekstrimisme siber hingga isu kesejahteraan siber (Shad, 2019). Walaupun begitu, dengan perkembangan *machine learning* saat ini juga merupakan salah satu peluang dalam menyediakan solusi untuk mampu mendeteksi ancaman serangan siber dan isu keamanan siber pada umumnya (Handa, Sharma, & Shukla, 2019)

Empat bulan pasca ketegangan antara India dan Tiongkok di perbatasan Ladakh Himalaya, seluruh Mumbai dalam keadaan pemadaman listrik yang diakibatkan hilangnya kekuatan sumber listrik pada 12 Oktober 2020. India mengalami serangan siber di Mumbai yang menyebabkan 20 juta penduduk Mumbai mengalami hambatan dalam beraktivitas mulai dari jam 10 pagi selama dua jam yang diakibatkan oleh hilangnya daya pembangkit listrik (Ipdefenseforum.com, 2021). Hal ini mengakibatkan berhentinya jaringan kereta, tutupnya pasar saham, dan rumah sakit mengandalkan daya generator untuk menjaga ventilator tetap berjalan.

Pemadaman ini hanya terjadi dua jam namun memberikan kerugian di berbagai sektor yang cukup masif (Ipdefenseforum.com, 2021). Sebagian besar orang India beralih kepada sistem digital dengan 51 persen dari mereka lebih memilih saluran perbankan *online* dan 26 persen di antaranya mengakses layanan melalui situs jaringan (*website*) bank dan menggunakan layanan *mobile banking* (Acharya & Joshi, 2020). Dengan pertumbuhan digitalisasi yang luar biasa di bank, dampak terjadinya serangan siber cukup signifikan walau tidak ada valuasi pasti untuk jumlahnya.

Dari sisi politik, kejadian ini di satu sisi bisa dilihat sebagai pesan dari Tiongkok agar tentara India mundur terkait konfrontasi di perbatasan. Di sisi lain, kondisi ini juga membuka mata India bahwa keamanan siber bukan merupakan hal yang bisa dinegosiasikan lagi dan India seharusnya segera mempunyai hukum dan perangkat siber yang mumpuni. Namun, sehubungan dengan sensitivitas isu ini terlebih ada indikasi hubungan dengan Tiongkok, tidak ada penjelasan yang cukup detail mengenai peristiwa ini baik dari lembaga pemerintah India maupun entitas lainnya. Meskipun begitu, serangan ini mendapat perhatian dari

pemerintah India yang merasa India terancam dan mengkasifikasikannya sebagai *cyber terrorism*. Oleh karena itu, Pemerintah India perlu segera membenahi sistem keamanan infrastruktur kritis seperti instalasi air dan listrik. Perangkat hukum pun perlu dievaluasi seiring dengan semakin bervariasi dan masifnya serangan siber (Vedant, 2020).

India merupakan salah satu negara tercepat dalam pertumbuhan pasar teknologi digital. Saat ini terdapat sejumlah 1,15 miliar pengguna telepon dan lebih dari 700 juta merupakan pengguna internet aktif di India. Penggunaan media sosial yang intensif juga merupakan potensi tinggi serangan siber dengan tingkat keberhasilan tinggi dalam meretas data pribadi (Kunwar & Sharma, 2016). Pemerintah juga menganjurkan warga negara untuk tidak menggunakan uang tunai dalam melakukan pembayaran (Ardhana, Kumar, & Ardhana, 2017). Efek demonetisasi membuat perdagangan memasuki era baru pasar finansial. Kondisi ini membuat posisi India sebagai negara target yang rentan mengalami kejahatan siber (Economic Times, 2022). Selain itu, peningkatan penggunaan *Internet of Things* (IoT) juga menimbulkan resiko tinggi munculnya serangan siber walaupun telah dilengkapi dengan penggunaan *deep learning* dalam mendeteksi potensi resiko serangan siber (Gopalakrishnan et al., 2020). Hingga tahun 2017, India menduduki peringkat keempat tekait peretasan keamanan daring (Choudhary, Choudhary, & Salve, 2018). Jumlah data yang paling banyak diretas yaitu India sejumlah 33.000 data dan India merupakan negara target serangan siber

Para analis mengenai keamanan dan sejarawan perang sebelumnya menyebutkan bahwa perang dunia selanjutnya bukan terjadi secara tradisional namun secara virtual dalam dunia siber. Sanger & Schmall (2021) mengemukakan bahwa keamanan siber perlu dikembangkan untuk melindungi berbagai infrastruktur penting. Perang siber di era kontemporer merupakan opsi saat ini dengan dampak yang dihasilkan lebih minim namun memungkinkan sebuah negara mempunyai posisi strategis dan menghasilkan efek psikologis. Soewardi (2013) menyebut perang siber menjadi arena pertempuran baru yang semakin mengukuhkan kemampuan sebuah negara dalam penguasaan teknologi di satu sisi dan kapabilitas pertahanan negara dalam mengamankan negaranya di sisi lain. Terkait India, Samuel (2014) melihat strategi keamanan siber yang dikembangkan oleh India tidak berbeda jauh dengan strategi

perang konvensional India yang terfokus di ranah regional utamanya dalam persaingannya dengan Pakistan. Di sisi lain, secara internal, Akash (2021) melihat pada pentingnya keterlibatan aktor di berbagai level dalam membuat pengembangan strategi keamanan siber India yang efektif. Relia (2021) juga berargumen bahwa komitmen pemerintah India semakin intensif dalam keamanan siber dan melibatkan entitas bisnis, sipil dan pemerintah.

Tulisan ini mengangkat rumusan masalah bagaimana strategi keamanan siber Pemerintah India dengan mengambil contoh kasus serangan siber Mumbai tahun 2020. Fokus kajiannya pada implementasi keamanan siber di India dengan berbagai aspeknya seperti kesiapan sumber daya, strategi nasional, hingga kolaborasi antarnegara yang dilakukan India. Pernyataan tulisan ini yaitu Pemerintah India mengupayakan penguatan sumber daya siber, mengambil posisi defensif untuk menjaga hubungan baik dengan negara lain dan menerapkan diplomasi siber baik bilateral maupun multilateral sebagai strategi keamanan. Serangan siber Mumbai 2020 memengaruhi keamanan nasional India dalam keamanan ekonomi, pertahanan negara dan hubungan luar negeri. Pertahanan siber yang lemah menyebabkan India menderita kerugian sosio ekonomi.

Penulis dalam hal ini berupaya untuk melihat secara makro posisi India baik secara internal maupun eksternal dengan menggunakan konsep perang klasik Kautilya yang relevan dengan India kontemporer dari sudut pandang yang berbeda dengan publikasi sebelumnya. Penggunaan konsep strategi perang klasik Kautilya karena secara konsep sangat relevan dengan fenomena kontemporer yang terjadi. Perbedaannya terdapat pada subyek dari konsep tersebut yang telah mengalami pergeseran akibat perkembangan teknologi dan dinamika globalisasi. Sebagai contoh, perang telah meluas areanya tidak hanya pertempuran fisik namun juga perang siber. Selain itu, tulisan ini berkontribusi pada diskusi Hubungan Internasional yang selama ini lebih mengenal Sun Tzu ketika membicarakan strategi perang klasik dan modern. Penulis berusaha untuk mengisi celah secara teoritis dan praktik yang bisa dielaborasi dari konsep peperangan klasik Kautilya di era globalisasi.

KERANGKA ANALISIS

Perspektif Kautilya

Dalam mengelaborasi rumusan pertanyaan, penulis menggunakan konsep

strategi perang klasik Kautilya yang relevan diterapkan di luar kondisi perang fisik pada era kontemporer. Kautilya dikenal juga sebagai Chanakya dan Vishnugupta yang merupakan Guru (mentor) dari Chandragupta, pendiri kerajaan Mauryan (Bisht, 2019). Kautilya merupakan ahli strategi perang. Strategi dan taktik perangnya relevan dengan kondisi kontemporer utamanya dalam hal konsep negara, pertahanan dan hubungan luar negeri (Collins, 2002) sebagai alat untuk mengelaborasi terkait keamanan siber di India. Pertama, terkait konsep negara, pemikiran strategis Kautilya meliputi berbagai elemen negara (praktisi) seperti raja, menteri, negara, benteng, tentara dan aliansi (Singh, 2016). Kautilya berargumen bahwa kemajuan ekonomi suatu negara membuat negara berjalan dengan baik atau dengan kata lain, kesejahteraan negara dan masyarakat tidak akan terjadi jika ekonominya lemah (Prasad, 2018). Posisi Kautilya sangat jelas yaitu pemikirannya untuk membuat negara kaya dan berkuasa dengan menggunakan kekuatan militer untuk melancarkan fungsi negara. Terlihat bahwa Kautilya merupakan seorang realis yang mengerti mengenai penggunaan kekuatan militer untuk menegaskan posisi negaranya dan menjaga kebanggaan nasional (Prabhu & Dwivedi, 2015). Kautilya menyebutkan faktor yang mempengaruhi kemenangan raja yaitu perhatian raja pada kesejahteraan rakyatnya, analisis alam, medan pertempuran, estimasi kekuatan relatif *vijigisu* (penakluk) dan musuh, pertahanan yang baik dan logistik yang memadai, tentara yang terlatih, tentara yang terjamin kesejahteraannya untuk menjaga tetap dalam kekuatan penuh dan penerapan *vijigisu* dalam berbagai jenis perang (Liebig, 2014).

Kedua, terkait pertahanan, dalam kompilasi Arthasastra yang ditulis Kautilya merekomendasikan bahwa sebuah negara harus mendasarkan pertahanannya pada benteng dan tentara (Rangarajan, 1992). Tanpa benteng yang kuat dan tentara yang terlatih, tidak mungkin sebuah negara dapat mempertahankan diri dari serangan musuh. Benteng pertahanan manusia juga merupakan salah satu hal esensial dari elemen pertahanan. Untuk mempertahankan benteng, juga diperlukan elemen lain seperti kendaraan tempur dan senjata (Kumar, Yadav, Sharma, & Singh, 2016). Kautilya menyebutkan faktor yang mempengaruhi kemenangan raja yaitu perhatian raja pada kesejahteraan rakyatnya (Kesejahteraan mendorong pertahanan kerajaan yang

efektif), pertahanan yang baik dan logistik yang memadai, tentara yang terlatih, tentara yang terjamin kesejahteraannya untuk menjaga tetap dalam kekuatan penuh (Shamasastry, 2014).

Ketiga, terkait kebijakan luar negeri, terdapat dua prinsip yang dibahas yaitu konsep Asan dan Yan (Chandrasekaran, 2006). Asan merupakan situasi yang lebih baik jika terdapat keberimbangan kekuatan. Namun, kekuatan itu bukan dipakai dalam tujuan antagonis seperti menyerang atau menyebarkan ancaman pada pihak lawan namun lebih untuk menciptakan hubungan antar negara yang damai dalam konteks kerja sama (Set, 2015). Selain itu, prinsip Yan menyebutkan bahwa invasi hanya berlaku jika pihak yang akan menyerang yakin akan kekuatannya dalam menghadapi pihak lawan (Chandrasekaran, 2006). Namun jika dalam kondisi lemah, sebaiknya tidak mencoba untuk melakukan penyerangan karena akan berdampak pada kekalahan dan kerugian dalam berbagai hal. Selain itu, konsep diplomasi dan membangun aliansi penting mencapai kepentingan politik, ekonomi, dan militer negara itu sendiri utamanya dilakukan oleh pihak yang merasa lemah dengan melakukan kerja sama dengan pihak yang lebih kuat atau setara (Gautam, 2015).

METODE PENELITIAN

Tulisan ini disusun berdasarkan penelitian dengan menggunakan metode kualitatif deskriptif untuk menjelaskan strategi pemerintah India dalam hal keamanan siber dengan menggunakan teori perang klasik yang masih relevan dengan perang non-fisik era kontemporer. Penelitian kualitatif menekankan pada cara menafsirkan, dan memaknai dalam memahami realitas sosial (Neuman, 2018; Mohajan, 2018) dan merupakan proses interaktif untuk peningkatan pemahaman dengan membuat penjelasan signifikan dan interpretatif yang dihasilkan dari fenomena yang dipelajari (Aspers & Corte, 2019; Nassaji, 2015). Data penelitian diperoleh melalui tenik kepustakaan (*library research*) dengan menelaah data sekunder yang didiperoleh dari buku, jurnal dan artikel terkait. Selanjutnya data dianalisis dengan menggunakan kerangka teoretis strategi perang klasik Kautilya dan hasilnya dipaparkan secara dekriptif.

HASIL DAN PEMBAHASAN

Serangan Siber: Strategi India Di Level Nasional dan Kolaborasi Global

Ada berbagai macam jenis serangan siber mulai dari *stalking*, serangan SQL, *phising,* pelanggaran privasi, dan yang

lainnya. Secara global, serangan siber semakin meningkat pesat dan dibutuhkan pengetahuan yang spesifik terkait keamanan siber untuk dapat mengantisipasinya (Tanwar, Paul, Singh, Joshi, & Rana, 2020). Terdapat dua karakter yang membedakan serangan siber dengan serangan militer konvensional yaitu serangan siber sulit diprediksi secara akurat dan pembuktian kejahatannya merupakan hal yang cukup sulit (Mehta, 2019). Dengan demikian, peperangan di dunia maya menimbulkan tantangan unik bagi keamanan nasional dan kurangnya aturan untuk mengaturnya meningkatkan tantangan ini.

Secara spesifik, tahun 2020 merupakan salah satu tahun yang penting terhadap peningkatan serangan siber ini. Pada tahun 2020, sejak pandemi Covid-19 terjadi, secara global, semua negara mulai mengalihkan berbagai kegiatan kedalam *platform* digital. Transformasi digital ini tentu saja di satu sisi sangat membantu dalam melakukan berbagai transaksi keuangan atau aktivitas. Namun, di sisi lain, transformasi digital yang tidak dilengkapi dengan persiapan, perencanaan dan mitigasi keamanan, sangat berpotensi terjadinya serangan siber yang mampu merusak secara fatal pada sektor-sektor penting dan mampu mengganggu keamanan negara (A. Bahrdwaj & Sapra, 2021).

Pengaruh Serangan Siber Mumbai 2020 pada keamanan Nasional India

Salah satu perusahaan asal Amerika mengidentifikasi asal serangan siber Mumbai 2020 berasal dari Tiongkok yang berupa *malware* untuk melakukan sabotase (Mallick, 2021). Lebih lanjut disebutkan bahwa sabotase ini memiliki keterkaitan dengan RedEcho, kelompok asal Tiongkok dengan aktivitas meyebarkan ancaman siber, yang menanam *malware* pada pembangkit listrik di India. RedEcho diidentifikasi secara sistematis menggunakan teknik intrusi siber teknologi tinggi yang menyebabkan kondisi kritis pada simpul infrastruktur elektronik listrik dan transmisi (Data Security Council of India, 2020). Kelompok RedEcho diperkirakan merupakan bagian unit intelejen militer Tiongkok yang berbasis di Urumqi, timur laut Tiongkok (Kannan, 2021). Serangan Tiongkok tersebut disebut banyak analis tidak akan memicu perang terbuka dengan India, namun lebih ke arah penunjukan kemampuan tangkal serangan siber (*cyber deterrence*) kepada dunia. Hingga saat ini belum ada ketentuan dan hukum mengenai perang siber. Salah satu

dokumen yang menjadi rujukan mengenai perang siber ini yaitu Tallinn Manual yang menyebutkan bahwa serangan siber dapat dikatagorikan sebagai perang atau menjadi bagian dari konflik bersenjata jika menimbulkan kerusakan fisik yang substansial atau menimbulkan jumlah kematian yang signifikan (Kannan, 2021).

Serangan siber Mumbai ini dalam kerangka ide Kautilya dapat dilihat melalui konsep negara, konsep pertahanan dan hubungan luar negeri. Pertama, Kautilya berargumen kesejahteraan negara dan masyarakat tidak akan terjadi jika ekonominya lemah. Serangan siber terhadap infrastruktur vital sangat lazim terjadi karena dampaknya yang masif di berbagai sektor. Kerugian finansial akibat serangan ini belum dipastikan. Namun, sebagai bandingannya, serangan siber terhadap Cosmos Bank di India yang terjadi pada 11 Agustus 2018 selama dua jam saja dapat mengakibatkan kerugian hingga 13.5 juta dolar AS melalui penarikan tunai di 28 negara (Jadhav, 2018). Serangan *malware* ini dilakukan melalui *server* anjungan tunai mandiri di berbagai cabang bank tersebut. Akibat dari matinya listrik di seluruh Mumbai, sektor kesehatan yang saat pandemi sangat bergantung dengan ventilator cukup terancam, begitu pula dengan kerugian finansial di berbagai institusi keuangan.

Setelah serangan siber tersebut, pemerintah India memberi nomor identitas unik 12-digit kepada warga negara India untuk bisa menerima layanan dasar pemerintah. Untuk mendapatkan nomor ini, penduduk India harus melakukan pemindaian sidik jadi, retina dan foto (Nugroho, 2021). Informasi identitas pribadi ini merupakan aset berharga yang berpotensial untuk dicuri. Data dalam dunia siber merupakan ladang emas karena dapat mengekstraksi data pribadi warga negara dan membuat informasi infrastruktur India dapat disalahgunakan. Di India, pembayaran digital diperkirakan akan meningkat hingga sekitar 96 miliar dolar AS pada tahun 2025. Pembayaran *mobile* juga diprediksikan mencapai 3,5 persen dari total pembayaran digital pada tahun 2025. Pada tahun 2021, pengguna total pembayaran *mobile* sejumlah 162 juta dan pada tahun 2015 diperkirakan jumlahnya akan mencapai 800 juta pengguna (Dharmaraj, 2020). Sehingga, solusi atas permasalahan digital akan memengaruhi ketahanan nasional di berbagai bidang terutama ekonomi. Iklim investasi salah satunya sangat dipengaruhi oleh keamanan negara baik dalam artian fisik maupun secara sistem keuangan dan transaksi. Kegagalan dalam penyediaan iklim

investasi dan bisnis yang baik, akan menyebabkan investor kehilangan kepercayaan. Selain itu, perkembangan ekonomi dari maksimalisasi potensi sumber daya manusia (SDM) India terkait digitalisasi transaksi keuangan juga akan terhambat.

Kedua, konsep pertahanan. Dalam Arthasastra merekomendasikan bahwa sebuah negara harus mendasarkan pertahanannya pada benteng dan tentara. Benteng dalam hal ini, berupa perangkat keamanan siber termasuk hukum siber dan sistem TI. Pemerintah India sebelumnya tidak mempunyai perangkat aturan terkait serangan siber dan spionase. Akhirnya pada tahun 2000, pemerintah mengeluarkan regulasi terkait siber dan kebijakan "*The National Cyber Security Policy*" tahun 2013. Lima tahun sejak implementasi kebijakan keamanan siber nasional ini, lanskap keamanan siber India cukup menunjukkan perubahan yang signifikan. Namun, India tetap perlu segera memformulasikan kebijakan keamanan dan kerangka keamanan siber yang lebih komprehensif karena peningkatan jumlah serangan siber dan kompleksitas perkembangan teknologi (Akhiles & Moller, 2020)

Dengan semakin meningkatnya ancaman siber di India, pemerintah India mengeluarkan program "*National Cyber Strategy* 2020". Pada tahun 2020 juga pemerintah memberlakukan pembatasan penggunaan beberapa aplikasi Tiongkok untuk melindung data personal dari pengguna India (IANS, 2020). Hal ini disebabkan Tiongkok diduga menggunakan perusahan seperti Huawei yang bergerak dalam bidang teknologi untuk menjadi alat spionase dalam memperkuat posisi Tiongkok (Febrian, 2020).

Selain menyusun regulasi, pemerintah juga menciptakan ekosistem siber yang aman melalui pembentukan beberapa badan siber seperti National Critical Information Infrastructure Protection Centre (NCIIPC) dengan menerapkan ISO 27032 yang saling berkoordinasi dalam melindungi ekosistem siber India (Pratiwi, 2019). Pemerintah juga membentuk Tim the Indian Computer Emergency Response (CERT-In) yang bertanggung jawab atas insiden serangan siber untuk melindungi infrastruktur penting (D. Bahrdwaj, 2022). Meskipun begitu, banyak kasus serangan siber di India yang bisa terdeteksi dan mampu menghukum pelakunya. Hal ini dikarenakan lemahnya hukum siber di India dan diperlukan sistem yang kompleks untuk bisa menangani

serangan siber ini (S. K. Singh & Rastogi, 2018).

Strategi India dalam pengembangan siber yaitu "*common but differentiated responsibility"* (CBDR) yang menaruh tanggung jawab keamanan siber pada berbagai aktor yang terlibat termasuk korporasi, pendidikan, pengguna dan pemerintah (Akash, 2021). Strategi nasional keamanan siber india yang masih dalam tahap finalisasi akan mengikutsertakan elemen kedaulatan dan akan menjadi panduan bagi perusahaan dalam ekosistem siber India. Elemen kedaulatan ini akan dimasukkan ke dalam *cyberspace* nasional untuk menciptakan keamanan, ketangguhan, kepercayaan dalam ekosistem siber India untuk meningkatkan kesejahteraan nasional.

Di India, pada tahun 2011 terjadi 1.791 serangan siber yang terdata oleh Pemerintah. Jumlah ini kemudian meningkat pada tahun 2015 mencapai 8.045 kasus (Ardhana et al., 2017) dan berekskalasi secara cepat selama rentang waktu 2015-2020 mencapai 1.158.208.000 kasus (Keelery, 2021). Jumlah serangan siber paling banyak yaitu dari sektor pemerintah disusul sektor perbankan dan finansial dan sektor TI (Anggono, Tarjo, & Riskiyadi, 2021). Oleh karena itu, keamanan siber mutlak dikembangkan sebagai bagian dari perencanaan dan pembangunan nasional.

Meskipun demikian, dengan semakin meningkatnya serangan siber, India masih kekurangan tentara yang dalam dunia siber merupakan para tenaga handal TI. Sumber Daya Manusia (SDM) infrastruktur TI di India yang ada masih belum mampu memenuhi kebutuhan. Data Security Council India menyebutkan bahwa India masih membutuhkan sekitar 1 juta tenaga profesional dalam bidang keamanan siber (Sabharwal, 2022). Muncul tantangan untuk mengatasi gap keahlian siber. Diperkirakan akan ada sekitar 1,5 juta lowongan pekerjaan di bidang keamanan siber pada tahun 2025 di India untuk membangun program yang menjembatani kesenjangan keterampilan dalam keamanan siber ini.

Microsoft telah berinvestasi dalam program 'CyberShikshaa' bersama dengan Dewan Keamanan Data India (DSCI), untuk menciptakan kumpulan profesional keamanan wanita yang terampil di negara tersebut (IANS, 2021). Microsoft juga bermitra erat dengan pemerintah untuk melatih para pemimpin terkait keamanan siber di seluruh entitas pemerintah India. Salah satu elemen yang penting dalam keamanan siber yaitu SDM yang bertanggung jawab langsung di keamanan

siber. Diperlukan keahlian akurasi waktu dan deteksi cepat sebelum serangan siber dilakukan (Dutt, Ahn, & Gonzales, 2012). Keamanan *big data* dan privasi sangat penting untuk mengamankan masyarakat dari kejahatan siber dengan salah satu sektor yang paling rentan dalam serangan siber yaitu sistem perbankan. Saat ini di setiap provinsi di India telah mempunyai *cyber cell* namun banyak penduduk India belum mengetahui keberadaan dan fungsinya (Datta, Panda, Tanwar, & Kaushal, 2020).

Ketiga, terkait kebijakan luar negeri dengan prinsip Asan dan Yan. Investigasi polisi siber Mumbai yang dilakukan pada Oktober 2020 menyebutkan kemungkinan adanya serangan siber dalam infrastruktur elektrik kota yang menyerang penyediaan listrik. Hasil investigasi menyebutkan adanya intrusi *malware* dari Tiongkok pada sistem *power grid* (FreePressJournal, 2021). Walapun begitu, pemerintah India dalam pernyataan resmi menyebutkan bahwa kejadian ini merupakan *human error* karena tidak cukup bukti untuk mengatakan pemerintah Tiongkok merupakan aktor utama di balik serangan ini. Dibandingkan dengan kemampuan siber Tiongkok, India masih harus mengejar banyak ketertinggalan. Tiongkok telah mempersiapkan diri dalam dunia siber selama dua dekade terakhir, sedangkan India masih mencari strategi dan formulasi kebijakan yang tepat (Gill, 2021). Kemampuan serang dan pertahanan siber India tertinggal 20 tahun dibanding Tiongkok. Dibutuhkan Investasi yang cukup besar, infrastruktur yang memadai, kemampuan kriptografi, SDM teknis dan manajerial siber yang andal dan berbagai perangkat yang dikembangkan mandiri untuk menyiapkan kemampuan serang siber tersebut (Naha, 2022). Jika India secara frontal membuat pernyataan yang menyudutkan maka dapat mengancam integritas dan keamanan India atau berpotensi memperburuk hubungan bilateral dengan negara lain.

Pada tahun 2020, India mengeluarkan skema strategi dalam bidang siber yang meliputi keamanan, sinergitas dan penguatan. Banyak aspek yang menjadi pertimbangan termasuk diplomasi siber (*cyber diplomacy*), kapabilitas SDM TI, termasuk perangkat keamanan siber nasional. Komitmen korporasi India dan pemerintah dalam memperbarui praktik keamanan siber di India semakin intensif utamanya dengan peningkatan volume transaksi keuangan digital dan tingkat serangan dunia maya (Relia, 2021). India terus berjuang untuk

menjaga kedaulatan, yurisdiksi, dan privasi dari ancaman yang mengganggu dan anonim yang mendominasi di arena dunia maya. Pemerintah India berusaha untuk menjalankan berbagai macam pelayanan *e-governance* melalui portal dan aplikasi berbasis *web* untuk efektivitas, namun di sisi lain juga sangat beresiko mengalami serangan siber (Sahoo, Behera, & Mohanty, 2018).

Pemerintah dan perusahaan swasta di India masih berusaha menemukan cara untuk menanggulangi kejahatan siber yang terjadi di dunia maya. Diperlukan koordinasi dan kerja sama bukan hanya dalam level nasional tapi juga level global karena terjadi lonjakan besar dalam dunia siber yang tidak mengenal batas negara (Kumar et al., 2016). Diperlukan skenario keamanan siber global karena banyak sektor vital yang berpotensi mengalami serangan siber seperti infrastruktur, privasi warga negara yang tentu akan mengganggu di negara yang bersangkutan tapi juga akan berpengaruh dalam berbagai hal lain di level regional dan global (Mishra, Dhir, & Hooda, 2016)

Dengan digitalisasi yang cepat muncul tantangan risiko yang ditimbulkan oleh teknologi. Serangan siber seringkali menargetkan sektor infrastruktur penting seperti pembangkit nuklir yang menguji kesiapan India dalam keamanan siber. Dari perspektif keamanan nasional, pengamanan infrastruktur informasi penting menjadi prioritas utama, sejalan dengan kebijakan yang telah diadopsi oleh negara digital lain. Saling ketergantungan yang terus tumbuh dari bidang digital, lintas batas, telah memicu munculnya keamanan siber sebagai komponen utama dari strategi keamanan nasional di berbagai negara di seluruh dunia (Parmar, 2017). Hingga saat ini, India tidak memiliki kemampuan untuk memanggil *cache exploitation zero-day* sedangkan peretas menggunakan teknik yang cukup efektif seperti dokumen umpan yang berisi senjata makro yang dapat berubah seiring waktu karena kemampuan mereka berkembang. India kekurangan orang dengan keterampilan teknis tingkat lanjut. Hal-hal yang perlu diperhatikan pemerintah India yaitu kecepatan dalam menyadari bahwa peretasan telah terjadi, kemampuan identifikasi kapasitas serangan siber untuk merusak sistem, ketahanan sistem dan waktu yang dibutuhkan untuk menutup celah (Mallick, 2021).

Salah satu tantangan pembuat kebijakan dalam aturan keamanan siber yaitu keterkaitannya dengan berbagai sektor. Seperti misalnya penggunanan perangkat keras dan perangkat lunak yang berasal dari

luar negeri atau besarnya data pemerintah India yang berada di luar negeri. Ketergantungan terhadap piranti keras Tiongkok juga dapat berbahaya karena berpotensi penetrasi pada infrastruktur penting. Infrastruktur *broadband* India juga saat ini masih sangat tergantung pada Huawei (Tare, 2021). Dibutuhkan integrasi antara keamanan siber dengan agenda nasional untuk dapat membuat inisiatif kebijakan sosio ekonomi yang strategis. India perlu strategi keamanan siber yang dapat menjamin keamanan pemerintah, warga negara dan ekosistem bisnis. Kondisi ini bukan hanya melindungi warga negara dari ancaman siber namun juga meningkatkan kepercayaan investor dalam bidang ekonomi. Dalam jangka panjang, bidang siber juga dapat menciptakan lapangan 1.5 juta lapangan kerja tahun 2025 (Mathur, 2022).

Diplomasi Siber India

Munculnya keamanan siber sebagai area utama yang menjadi perhatian negara dapat digunakan untuk strategi pertahanan negara (Johnson, 2015). Keamanan siber telah menjadi elemen penting dari kebijakan luar negeri karena relevansinya dengan keamanan nasional, keselamatan publik, dan pembangunan ekonomi. Mengembangkan kesepakatan internasional tentang bagaimana negara harus berperilaku di dunia maya dan bagaimana mencapai internet yang stabil dan terbuka akan menjadi semakin penting. Dalam hal ini, meskipun diplomasi siber adalah bidang yang berbeda dengan aspek keamanan dunia digital, namun tetap dianggap sebagai komponen diplomasi digital (S. Singh, 2018). Diplomasi digital tidak bisa berdiri sendiri, karena praktik diplomasi di ranah digital rentan terhadap ancaman siber. Perlu melakukan analisis risiko atas potensi ancaman atau serangan dunia maya dan mengembangkan langkah-langkah keamanan siber untuk mencegah kekacauan siber.

Tantangan yang dihadapi pemerintah India adalah memastikan bahwa infrastruktur internet yang diterapkan stabil dan aman, namun tidak hanya masalah keamanan nasional tetapi juga kebutuhan dan kepekaan bisnis. Prioritas kebijakan siber domestik India menekankan pada perlindungan transformasi digital melawan ancaman siber dan pembentukan regulasi dengan menjalankan negosisasi multilateral dalam hal tata kelola internet dan keamanan siber (Ebert, Saslow, & Wetzling, 2020). Dalam spektrum kapabilitas *cyber warfare*, India berada di *tier-3* dengan berdasar pada

indikator kekuatan digital ekonomi, kematangan sistem pintar dan fungsi keamanan, dan integrasi siber dengan operasi militer (Tech, 2021). India aktif dalam diplomasi siber namun belum menjadi salah satu pemimpin dalam norma-norma global. India lebih memilih untuk membuat pengaturan praktis yang produktif dan menjalin kerja sama dengan mitra regional dan global. Penyelerasan antara program global dengan kebijakan dalam negeri merupakan salah satu kunci pengembangan kekuatan siber India (Choudary, 2022).

India memiliki kemampuan intelijen siber dan siber ofensif, tetapi India lebih fokus secara regional, terutama di Pakistan. Untuk mengantisipasi kelemahan siber, India melakukan diplomasi siber bilateral mulai dari negara *tier 1* hingga *tier 3* yaitu Jepang, Korea Selatan, Amerika, Inggris, Perancis dan Uni Eropa. Luaran kerja sama ini berupa program pelatihan, kerja sama *smart system*, penelitian, pengembangan dan pembiayaan proyek siber bersama (Samuel, 2014). Dalam jangka dekat, tujuan keamanan siber India yaitu membangun kapasitas dan menyediakan keamanan siber dalam negeri dan membangun kerja sama internasional baik bilateral maupun multilateral. Sedangkan isu siber jangka panjang India meliputi restrukturisasi tata kelola internet, pengembangan norma digital dan konvensi untuk mengantisipasi intrusi siber dan segala konsekuensinya.

Dengan Kebijakan Keamanan Siber Nasional (2020-2025), India memiliki kesempatan untuk menyelaraskan kebijakan domestiknya dengan aspirasi globalnya. Pada tahun 2011, India mengajukan proposal untuk Komite Kebijakan Terkait Internet (CIRP) yang terdiri dari 50 negara. India merupakan salah satu negara anggota yang mendukung resolusi UNGA yang menghasilkan pembentukan Open-Ended Working Group (OEWG) dan UN-GGE (2019-2021). India juga merupakan anggota United Nations Group of Governmental Experts (UN-GGE) dan belum berkontribusi secara formal pada proses OEWG. Di bidang multilateral, India tetap berada di luar Jalur Osaka untuk Tata Kelola Data dan Konvensi Budapest tentang Kejahatan Dunia Maya (Mehta, 2019).

Sebagai bagian dari masyarakat siber, India juga harus terlibat dalam the Oxford Process on International Law Protection in Cyberspace. Proses Oxford merupakan inisiatif yang diselenggarakan di bawah naungan Universitas Oxford yang dimulai pada Mei 2020 yang secara reguler mengidentifikasi tugas keamanan siber negara di bawah hukum internasional (Sud,

2021). Proses Oxford melibatkan berbagai kalangan mulai dari pemerintah, industri, dan masyarakat sipil. Keamanan siber adalah masalah multi-pemangku kepentingan sehingga perlu mengakomodir berbagai perspektif.

Pada 2015, India telah memulai dialog tentang keamanan siber dengan Amerika Serikat, Inggris, Jerman, Uni Eropa, Prancis, Korea Selatan, Rusia, Jepang, dan Australia dengan pandangan telah dipertukarkan tentang kebijakan keamanan siber nasional, berbagi informasi penting, penelitian dan pengembangan peningkatan kapasitas dan masalah lain (Johnson, 2015). Pemerintah India berfokus pada diplomasi siber yang merupakan area yang berkembang dan membutuhkan pengetahuan yang rumit tentang teknologi, hukum, politik, dan aspek terkait lain.

India berpendapat bahwa penyalahgunaan TI dan media sosial dapat menciptakan ketegangan sosial dan ancaman. Inggris telah berupaya membentuk debat internasional tentang norma dunia siber melalui Konferensi London 2011, konferensi Hungaria 2012, Seoul 2013, Belanda 2015, dan India 2017. Dikenal sebagai "*London Process*," konferensi ini berusaha untuk mensosialisasikan ide-ide tentang: norma-norma dunia maya, berdasarkan hukum internasional yang ada; Internet yang bebas dan terbuka, diatur oleh model *multistakeholder*; dan peningkatan kapasitas itu diperlukan untuk menciptakan iklim daring yang aman. Tahun 2016, India mengajukan proposal kepada Sekretaris Jenderal PBB tentang pembentukan badan baru di dalam lembaga-lembaga multilateral yang mendorong diskusi tentang stabilitas dunia maya. India mengadvokasi norma dunia digital, langkah membangun kepercayaan, dan kapasitas upaya membangunnya.

Sejumlah negara telah mulai memasukkan isu-isu dunia maya ke dalam dialog formal antar pemerintah, baik sebagai satu topik di antara banyak topik dalam pembicaraan keamanan reguler atau dalam jalur terpisah yang berdiri sendiri. Selain itu, lembaga *think tank* telah membentuk dialog *track 1.5* dari *track 2* untuk mendorong dialog tentang masalah dunia digital. Pada tahun 2016, India dan Amerika Serikat menyetujui dokumen kerangka kerja hubungan bilateral dalam dunia digital mulai dari upaya penegakan hukum terhadap kejahatan dunia maya hingga pertukaran praktik terbaik keamanan dunia maya, serta sebagai mempromosikan norma-norma dunia

maya tertentu yang direkomendasikan oleh GGE PBB dan G20. New Delhi dan Washington juga telah secara eksplisit setuju untuk "mengembangkan pemahaman bersama tentang stabilitas dunia maya internasional, dan aktivitas destabilisasi." Kerangka tersebut berlaku selama lima tahun (GCSC, 2018).

Pada tahun 2020 dibentuk Indian Cybercrime Co-ordination Centre (I4C) oleh Kementrian Dalam Negeri India yang berfungsi sebagai titik simpul dalam memerangi kejahatan dunia maya dan melakukan berbagai kegiatan termasuk koordinasi semua kegiatan yang terkait dengan pelaksanaan *mutual legal assistance treaties* (MLAT) dengan negara lain terkait kejahatan siber (*cybercrime)* dengan berkonsultasi dengan nodal terkait kewenangan di Kementrian (Mea.gov.in, 2020). Selama tahun 2020 hingga 2021, India melakukan beberapa kerja sama baik bilateral maupun multilateral (Basu, 2022). Dalam kaitannya dengan keamanan informasi dan teknologi, Pemerintah India melalui Kementrian Komunikasi dan Informasi Teknologi mengajukan proposal untuk kelompok kerja India-Irlandia di bidang informasi dan teknologi. Pemerintah India juga menandatangani pernyataan bersama (*joint statement*) tentang kemitraan strategis komprehensif antara Republik India dan Australia. Selain itu, India juga menandatangani nota kerjasama di bidang keamanan siber dengan Jepang.

Dialog Siber India-Uni Eropa Keenam diselenggarakan oleh India secara virtual pada 14 Desember 2020. Kedua belah pihak membahas berbagai bidang kerja sama di ruang siber termasuk hal-hal kontemporer, di antaranya: kerjasama multilateral dan regional tentang stabilitas di dunia maya pada *platform* PBB di GGE, OEWG, atau dalam pengaturan regional termasuk diskusi yang relevan di OSCE dan ARF; diplomasi Cyber UE; kerjasama menangani *cybercrime* dan peningkatan kapasitas didalamnya; isu kontemporer dan pertukaran tentang kebijakan siber; tata kelola internet; teknologi baru yang terkait dengan dunia maya. Kedua belah pihak menegaskan kembali komitmen mereka untuk ruang siber yang terbuka, bebas, aman, stabil, damai dan dapat diakses, memungkinkan pertumbuhan ekonomi dan inovasi. Kedua belah pihak mengakui perlunya mengikuti nilai-nilai dasar seperti supremasi hukum, nilai-nilai demokrasi dan kebebasan fundamental (MEA, 2021). Pada 2021, dilakukan dialog siber bilateral India-Prancis keempat diadakan dalam mode virtual yang membahas berbagai aspek kerja sama

bilateral yang ada di dunia maya, bertukar pandangan tentang perkembangan terkini isu-isu dunia maya di forum bilateral, regional dan multilateral serta menjajaki inisiatif untuk lebih memperdalam kerja sama dunia maya(MEA, 2021). Delegasi membahas berbagai topik keamanan siber, kejahatan siber, dan pembangunan kapasitas.

Dari segi diplomasi siber, India memang telah menjalin banyak kerja sama baik bilateral maupun multilateral dengan berbagai negara dan entitas. Namun, setelah serangan Siber Mumbai 2020, kerja sama dengan berbagai pihak juga semakin meluas dan semakin kongkrit utamanya dengan negara-negara yang juga pernah menjadi target serangan siber yang diindikasikan dilakukan oleh Tiongkok.

SIMPULAN

Perang di era globalisasi bukan lagi semata berada di medan pertempuran melainkan juga dalam dunia siber. Sistem pertahanan kemanan tradisional berupa senjata perang, kendaraan perang bahkan nuklir masih diperlukan untuk pertahanan negara dari kemungkinan perang fisik. Namun, setiap negara seharusnya juga melengkapi sistem pertahan keamanan siber menimbang perkembangan teknologi yang begitu pesat di era globalisasi. Keamanan siber secara nyata mempunyai pengaruh terhadap keamanan nasional India dengan pengguna internet yang masif dan meningkatnya digitalisasi dalam berbagai sektor kehidupan. Walau telah mengalami beberapa serangan siber sebelumnya, namun, serangan siber terhadap infrastruktur vital di Mumbai pada tahun 2020 merupakan peringatan bagi pemerintah India untuk segera mempunyai hukum dan perangkat penananganan kejahatan siber yang mumpuni.

Berdasar ide Kautilya bahwa negara seharusnya mempunyai perekonomian yang kuat untuk dapat mensejahterakan rakyat dan membuat negara maju, keamanan siber jelas menjadi prasyarat untuk pertumbuhan ekonomi di era globalisasi dengan kehidupan sosio ekonomi menjadi terdigitalisasi. Terkait ide defensif Kautilya di dunia siber, musuh lebih sulit untuk diidentifikasi dan data merupakan sumber pertarungan antar aktor di era kontemporer, sistem keamanan siber yang tangguh merupakan benteng terbaik dalam mengamankan data warga negara, pemerintah dan bisnis. Mandatori pula untuk mempunyai sumber daya TI handal, sebagai representasi tentara dalam artian tradisional, dalam membangun sistem

yang tidak mudah dirusak. Ketiga, terkait konsep Asan dan Yan, dengan berbagai keterbatasan kemampuan India dalam dunia siber, pemerintah India masih dalam posisi defensif dengan memperbaiki dan menguatkan seluruh elemen siber. Pemerintah India berupaya untuk mempunyai sistem hukum, sistem keamanan dan sumber daya manusia yang tangguh dalam dunia siber. India tidak melakukan tindakan ofensif dengan berkonfrontasi dengan Tiongkok karena menyadari kemampuan sibernya yang belum sebanding dengan Tiongkok, sehingga, diplomasi dan mencari aliansi merupakan jalan terbaik baik India dalam menghadapi berbagai serangan siber yang ada.

Sebagai penutup, kejahatan dunia maya akan selalu menjadi ancaman yang dapat mengeksploitasi berbagai kerentanan dan meluncurkan serangan siber besar-besaran. Satu-satunya cara untuk menghentikan ancaman ini adalah dengan aktif melakukan identifikasi serangan dan menetralisirnya (Sheth, 2021). Namun, Tindakan ofensif seperti ini hanya bisa dilakukan dengan kapabilitas siber yang kuat. Diperlukan sistem pertahanan siber yang tangguh karena semakin terkoneksinya dunia digital, semakin rentan pula terhadap kejahatan siber yang dampaknya bisa menyebabkan kerugian ekonomi dan terancamnya hak warga negara. Selain itu, kerja sama bilateral dan multilateral dalam bidang siber sangat diperlukan untuk bisa membuat sistem pertahanan siber dan iklim investasi yang lebih baik.

REFERENSI

(GCSC), T. G. C. on the S. of C. (2018). *Briefings from the Research Advisory Group. Briefings To The Global Commission On The Stability Of Cyberspace For The Full Commission Meeting.* New Delhi.

(MEA), M. of E. A. (2021). *Ministry of External Affairs, Annual Report 2020-21*. New Delhi.

(MEA), M. of E. A. (2022). *Annual Report 2021-22*. New Delhi.

Acharya, S., & Joshi, S. (2020). Impact Of Cyber-Attacks On Banking Institutions In India: A Study Of Safety Mechanisms And Preventive Measures. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *17*(6), 4656–4670.

Akash, S. (2021). India's Cybersecurity Strategy: Inclusion of Sovereignty. Retrieved February 8, 2023, from https://www.analyticsinsight.net/indias-cybersecurity-strategy-inclusion-of-sovereignty/

Akhiles, K. ., & Moller, D. P. . (2020). Smart Technologies . Retrieved February 8, 2023, from DOI 10.1007/978-981-13-7139-4 website: https://sci-hub.ru/https://link.springer.com/chapter/10.1007/978-981-13-7139-4_6

Ananda Kumar, V., Pandey, K. K., & Punia, D. K. (2014). Cyber security threats in the power sector: Need for a domain specific regulatory framework in India. Energy Policy, 65, 126–133 | 10.1016/j.enpol.2013.10.025. Retrieved February 8, 2023

Anggono, A., Tarjo, & Riskiyadi, M. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Manajemen Dan Organisasi (JMO)*, *Vo.12*(No.3), 239–251.

Ardhana, V., Kumar, D. D., & Ardhana, D. kumar. (2017). Cyber Crime & Cyber Security : Be Vigilant, Not Victim. *Jai Maa Saraswati Gyandayini*, *vol 3*(Issue-II), 585–597. Retrieved from https://www.researchgate.net/publication/342162794_Cyber_Crime_Cyber_Security_Be_Vigilant_Not_Victim

Aspers, P., & Corte, U. (2019). What is Qualitative in Qualitative Research. *Qualitative Sociology*, *42*, 139–160. Retrieved from https://doi.org/10.1007/s11133-019-9413-7

Bahrdwaj, A., & Sapra, V. (Eds). (2021). Security Incidents & Response Against Cyber Attacks. . Retrieved February 8, 2023, from EAI/Springer Innovations in Communication and Computing | 10.1007/978-3-030-69174-5 website: https://sci-hub.ru/https://link.springer.com/content/pdf/10.1007/978-3-030-69174-5.pdf

Bahrdwaj, D. (2022). A year on, cyber security strategy pending with government | Latest News India - Hindustan Times. Retrieved February 8, 2023, from https://www.hindustantimes.com/india-news/a-year-on-cyber-security-strategy-pending-with-government-101645555771206.html

Basu, A. (2022). *India's International Cyber Operations : Tracing National Doctrine and Capabilities*.

Bisht, M. (2019). Kautilya's Arthashastra: Philosophy of strategy. *Kautilya's Arthashastra: Philosophy of Strategy*, 1–187. https://doi.org/10.4324/9780429329333

Chandrasekaran, P. (2006). Munich Personal RePEc Archive KAUTILYA: Politics, Ethics And Statecraft. Retrieved February 8, 2023, from Harvard University/Harvard Kennedy School website: https://mpra.ub.uni-muenchen.de/9962/

Choudary, L. R. (2022). India's Defence Diplomacy Towards Central Asia : A Critical Appraisal. *Indian Journal of Asian Affairs*, *Vol.35*(No.1), 73–93. Retrieved from https://www.jstor.org/stable/27146668

Choudhary, A. S., Choudhary, P. P., & Salve, S. (2018). A Study on Various Cyber Attacks and A Proposed Intelligent System for Monitoring Such Attacks. *Proceedings of the 3rd International Conference on Inventive Computation Technologies, ICICT 2018*, 612–617. https://doi.org/10.1109/ICICT43934.2018.9034445

Collins, J. M. (2002). Nuclear Warfare Strategies. In *Military Strategy :*

Principles, Practices and Historical Perspectives (pp. 133–144). Washington DC: Potomac Books.

Data Security Council of India. (2020). National Cyber Security Strategy 2020. *Nasscom*, 22. Retrieved from https://www.dsci.in/sites/default/files/documents/resource_centre/National Cyber Security Strategy 2020 DSCI submission.pdf

Datta, P., Panda, S. N., Tanwar, S., & Kaushal, R. K. (2020). A Technical Review Report on Cyber Crimes in India. *2020 International Conference on Emerging Smart Computing and Informatics, ESCI 2020*, 269–275. https://doi.org/10.1109/ESCI48226.2020.9167567

Dharmaraj, S. (2020, September 21). India to create National Cyber Security Strategy 2020 - OpenGov Asia. Retrieved February 8, 2023, from https://opengovasia.com/india-to-create-national-cyber-security-strategy-2020/

Dutt, V., Ahn, Y.-S., & Gonzales, C. (2012). Cyber Situation Awareness. Human Factors: The Journal of the Human Factors and Ergonomics Society, 55(3), 605–618 | 10.1177/0018720812464045. Retrieved February 8, 2023, from Human factors : The Journal of the Human factors and Ergonomics Society, 55(3) website: https://sci-hub.ru/https://journals.sagepub.com/doi/pdf/10.1177/0018720812464045

Ebert, H., Saslow, K., & Wetzling, T. (2020). Cyber Resilience and Diplomacy in India. *Digital Dialogue*, (July). https://doi.org/10.13140/RG.2.2.18187.52004

Economic Times. (2022). Cybersecurity: How is India faring? - The Economic Times. Retrieved February 8, 2023, from https://economictimes.indiatimes.com/industry/services/education/cybersecurity-how-is-india-faring/articleshow/90092428.cms

Febrian, A. (2020). Setelah adu kungfu dengan India, China dituding menyerang Australia. Retrieved February 8, 2023, from https://internasional.kontan.co.id/news/setelah-adu-kungfu-dengan-india-china-dituding-menyerang-australia?page=all

FreePressJournal. (2021). Mumbai: Maharashtra Cyber Cell warns people of keeping cyber security on during weekends. Retrieved February 8, 2023, from https://www.freepressjournal.in/mumbai/mumbai-maharashtra-cyber-cell-warns-people-of-keeping-cyber-security-on-during-weekends

Gautam, P. K. (2015). *Kautilya's Arthasastra : Contemporary Issues and Comparison*. New Delhi: Insititute for Defence Studies and Analyses.

Gill, P. (2021, April 9). The Chinese cyber threat is real — and India's best defence right now is to keep its outage time limited | Business Insider India. Retrieved February 8, 2023, from https://www.businessinsider.in/defense/news/the-chinese-cyber-threat-is-real-and-indias-best-defence-right-now-is-to-keep-its-outage-time-

limited/articleshow/81981886.cms

Gopalakrishnan, T., Ruby, D., Al-Turjman, F., Gupta, D., Pustokhina, I. V., Pustokhin, D. A., & Shankar, K. (2020). Deep learning enabled data offloading with cyber attack detection model in mobile edge computing systems. *IEEE Access*, *8*, 185938–185949. https://doi.org/10.1109/ACCESS.2020.3030726

Gunjan, V. K., Kumar, A., & Avdhanam, S. (2013). A survey of cyber crime in India. *2013 15th International Conference on Advanced Computing Technologies, ICACT 2013*. https://doi.org/10.1109/ICACT.2013.6710503

Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. . Retrieved February 8, 2023, from Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, e1306 | 10.1002/widm.1306:

IANS. (2020). Why India needs a national cybersecurity strategy | The News Minute. Retrieved February 8, 2023, from https://www.thenewsminute.com/article/why-india-needs-national-cybersecurity-strategy-130815

IANS. (2021). India in final stages of clearing national cybersecurity strategy | Business Standard News. Retrieved February 8, 2023, from https://www.business-standard.com/article/current-affairs/india-in-final-stages-of-clearing-national-cybersecurity-strategy-121102700663_1.html

Ipdefenseforum.com. (2021). Mumbai blackout serves as cybersecurity alert for region – Indo-Pacific Defense Forum. Retrieved February 8, 2023, from https://ipdefenseforum.com/2021/04/mumbai-blackout-serves-as-cybersecurity-alert-for-region/

Johnson, T. (2015). Cyber security an important element of foreign policy: Deputy NSA Arvind Gupta | India News,The Indian Express. Retrieved February 8, 2023, from https://indianexpress.com/article/india/india-others/cyber-security-an-important-element-of-foreign-policy-deputy-nsa-arvind-gupta/

Kannan, S. (2021). China continues to pose cyber security threats to India. Retrieved February 8, 2023, from Indiatoday website: https://www.indiatoday.in/india/story/china-continues-to-pose-cyber-security-threats-to-india-1856224-2021-09-23

Keelery, S. (2021). Cyber security in India - statistics & facts. Retrieved February 8, 2023, from https://www.statista.com/topics/8251/cyber-security-in-india/

Kumar, S. R., Yadav, S. A., Sharma, S., & Singh, A. (2016). Recommendations for effective cyber security execution. *2016 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016*, 342–346. https://doi.org/10.1109/ICICCS.2016.7542327

Kunwar, R. S., & Sharma, P. (2016). Social media: A new vector for cyber attack. *Proceedings - 2016 International Conference on Advances in Computing, Communication and Automation, ICACCA 2016*. https://doi.org/10.1109/ICACCA.2016.7578896

Liebig, M. (2014). Kautilya's Arthaśāstra: A Classic Text of Statecraft and an Untapped Political Science Resource. *Heidelberg Papers in South Asian and Comparative Politics, Working Paper No. 74*, pp. 1–17.

Mallick, M. J. P. K. (2021). *Chinese Cyber Exploitation in India's Power Grid - Is there a linkage to Mumbai Power Outage?* (No. Issue Brief No – 01/2021).

Mathur, A. (2022, March 9). Cybersecurity: How is India faring? - The Economic Times. Retrieved February 8, 2023, from https://economictimes.indiatimes.com/industry/services/education/cybersecurity-how-is-india-faring/articleshow/90092428.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

Mea.gov.in. (2020). MEA | Statements : Press Releases. Retrieved February 8, 2023, from https://www.mea.gov.in/press-releases.htm?dtl/33308/6th_IndiaEU_Cyber_Dialogue

Mehta, P. W. (2019). India's National Cybersecurity Policy Must Acknowledge Modern Realities. Retrieved February 8, 2023, from https://thediplomat.com/2019/12/indias-national-cybersecurity-policy-must-acknowledge-modern-realities/

Mishra, S., Dhir, S., & Hooda, M. (2016). A Study on Cyber Security, Its Issues and Cyber Crime Rates in India. Innovations in Computer Science and Engineering, 249–253 | 10.1007/978-981-10-0419-3_30. Retrieved February 8, 2023, from Innovation in Computer Science and Engineering website: https://sci-hub.ru/https://link.springer.com/chapter/10.1007/978-981-10-0419-3_30

Mohajan, H. (2018). Qualitative Research Metodhology in Social Sciences and Related Subjects. *Journal of Economic Development, Environment and People*, *Vol 7*(Issue 01), 23–48. Retrieved from onlineathttps://mpra.ub.uni-muenchen.de/85654/

Naha, A. (2022). Emerging Cyber Security Threats : India's Concerns and options. *International Journal of Politics and Security (IJPS)*, *Vo.4*(No.1), 170–200. https://doi.org/10.53451/ijps.996755

Nassaji, H. (2015). Qualitative and Descriptive Research : Data Type versus Data Analysis. *Language Teaching Research*, *19(2)*, 129–132. https://doi.org/10.1177/1362168815572747

Neuman, W. L. (2018). *Metodologi Penelitian Sosial : Pendekatan Kualitatif dan Kuantitatif* (Edisi Ketu). Jakarta: PT. Indeks.

Nugroho, A. (2021). NEWS : Hacker China Lancarkan Serangan ke Times of India. Retrieved February 8, 2023, from https://cyberthreat.id/read/12523/Hacker-China-Lancarkan-Serangan-ke-

Times-of-India

Parmar, S. D. (2017). *Cybersecurity in India: An Evolving Concern for National Security Sushma Devi Parmar (Central University of Gujarat)*. 1–14.

Prabhu, K. S. V., & Dwivedi, L. D. (2015). A Brief Comparison on 'Espionage' and the Importance of 'Spies' between Kautilya's The Arthashastra & Sun Tzu's The Art of War. *Mediterranean Journal of Social Sciences*, *6*(6), 544–548. https://doi.org/10.5901/mjss.2015.v6n6s4p544

Prasad, J. (2018). Kautilya's Arthashastra: an intellectual portrait: the classical roots of modern politics in India. *Strategic Analysis*, *42*(4), 451–452. https://doi.org/10.1080/09700161.2018.1482621

Pratiwi, R. A. P. (2019). Analisis Persepsi Keamanan Nasional India Terhadap Serangan Siber dari Pakistan 2008-2017 | Pratiwi | Journal of International Relations. Retrieved February 8, 2023, from Journal of International Relations, Volume 5, Nomor 4 website: https://ejournal3.undip.ac.id/index.php/jihi/article/view/25045/22297

Rangarajan, L. . (1992). *Kautilya : The Arthasastra*. Calcutta: Penguin Books India (P) Ltd.

Relia, C. S. (2021, August 4). India's tryst with a New National Cyber Security Policy: Here's what we need | The Financial Express. Retrieved February 8, 2023, from https://www.financialexpress.com/defence/indias-tryst-with-a-new-national-cyber-security-policy-heres-what-we-need/2304053/

Sabharwal, L. (2022, November 15). Why India needs to update its cyber strategy | Cyber Security Information. Retrieved February 8, 2023, from https://www.mygreatlearning.com/blog/why-india-needs-to-update-its-cyber-security-strategy/

Sahoo, B., Behera, R. N., & Mohanty, S. (2018). International Cyber Attackers Eyeing Eastern India: Odisha - A Case Study. Intelligent Computing, 1328–1339 | 10.1007/978-3-030-01177-2_97. Retrieved February 8, 2023, from Intelligent Computing, 1328–1339 | 10.1007/978-3-030-01177-2_97 website: https://sci-hub.ru/https://link.springer.com/chapter/10.1007/978-3-030-01177-2_97

Samuel, C. (2014, November 1). India's International Cybersecurity Strategy from Cybersecurity: Some Critical Insights and Perspectives on JSTOR. Retrieved February 8, 2023, from https://www.jstor.org/stable/resrep05892.6?searchText=cybersecurity+goals&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Dcybersecurity%2Bgoals%26acc%3Don&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3A6f830a4001f3606ecb8259e100c45f3d

Sanger, D. E., & Schmall, E. (2021, February 28). China Appears to warn India: Push too hard and the lights could go out. Retrieved February 8, 2023, from The New York Times

website: https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html

Set, S. (2015). Ancient Wisdom for the Modern World: Revisiting Kautilya and his Arthashastra in the Third Millennium. *Strategic Analysis*, (39:6), 710–714. https://doi.org/10.1080/09700161.2015.1090685

Shad, M. R. (2019). Cyber Threat Landscape and Readiness Challenge of Pakistan on JSTOR. Retrieved February 8, 2023, from Strategic Studies Vol. 39, No. 1 (Spring) website: https://www.jstor.org/stable/48544285?seq=2

Shamasastry, R. (2014). *kautilya Arthasastra*. CHAUKHAMBHA.

Sheth, H. (2021, March 30). 52% of Indian organisations suffered a successful cybersecurity attack in the last 12 months: Survey - The Hindu BusinessLine. Retrieved February 8, 2023, from https://www.thehindubusinessline.com/news/52-of-indian-organisations-suffered-a-successful-cybersecurity-attack-in-the-last-12-months-survey/article34195953.ece

Singh, S. (2018, December). (PDF) Digital Diplomacy: India's Increasing Digital Footprint. Retrieved February 8, 2023, from https://www.researchgate.net/publication/331772911_Digital_Diplomacy_India%27s_Increasing_Digital_Footprint

Singh, S. K., & Rastogi, N. (2018). Role of Cyber Cell to Handle Cyber Crime within the Public and Private Sector: An Indian Case Study. *Proceedings - 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages, IoT-SIU 2018*. https://doi.org/10.1109/IOT-SIU.2018.8519884

Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang Tangguh Bagi Indonesia. *Media Informasi Ditjen Pothan Kemhan*, 31–35.

Sud, N. (2021, September 28). Cybercrime, Cyberattack, Cybersecurity: For Cybersecurity, India Must Look To International Law - Forbes India Blogs. Retrieved February 8, 2023, from https://www.forbesindia.com/blog/legalese/for-cybersecurity-india-must-look-to-international-law/

Sunny, S., Pavithran, V., & Achuthan, K. (2014). Synthesizing perception based on analysis of cyber attack environments. *Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2014*, 2027–2030. https://doi.org/10.1109/ICACCI.2014.6968639

Tanwar, S., Paul, T., Singh, K., Joshi, M., & Rana, A. (2020). Classification and Imapct of Cyber Threats in India: A review. *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, 129–135. https://doi.org/10.1109/ICRITO48877.2020.9198024

Tare, K. (2021). Chinese cyber attack: Why Maharashtra should worry . Retrieved February 8, 2023, from https://www.indiatoday.in/india-today-insight/story/chinese-cyber-attack-why-maharashtra-should-worry-1774905-2021-03-02

Tech, I. T. (2021). India a third-tier country in cyber warfare capabilities, report says US more powerful than China. Retrieved February 8, 2023, from https://www.indiatoday.in/technology/news/story/india-a-third-tier-country-in-cyber-warfare-capabilities-report-says-us-more-powerful-than-china-1820261-2021-06-28

Vedant, H. (2020). A Review Paper on Cyberattacks in India. *International Research Journal of Modernization in Engineering Technology and Science*, *02*(12), 609–614.