MADANI
Jurnal Politik dan Sosial Kemasyarakatan
Vol 16 No 1 (2024) : Februari 2024
(P-ISSN 2085 - 143X) (E-ISSN 2620 - 8857)

Readiness Digital Mengatasi *Cyber War*: Studi Kasus tentang *Cyber War* Indonesia dan Australia

Herlina[1], Yeby Ma'asan Mayrudin[2], Ahmad Sholikin[3]

[1,2] Program Studi Ilmu Pemerintahan, Universitas Sultan Ageng Tirtayasa, [3] Prodi Ilmu Politik dan Ilmu Pemerintahan, Universitas Islam Darul 'Ulum

6670210012@untirta.ac.id[1] yeby@untirta.ac.id[2] ahmad.sholikin@unisda.ac.id[3]

Received: 04 Agustus 2024; Revised: 30 September 2024; Accepted: 15 Oktober2024; Published: Desember 2024; Available online: Desember 2024

Abstract

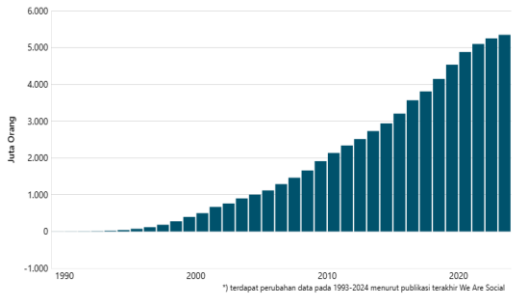
This paper aims to examine the issue of digital readiness in overcoming cyber war between Indonesia and Australia. The existence of cyber conflict has given rise to an evaluation for the government to continue to improve the security system. The wiretapping carried out by the Australian government was a presumptuous act and the Indonesian government and the public condemned the act. The wiretapping action triggered a cyber war between Indonesia and Australia. This research method uses a qualitative Creswell case study approach that focuses on analyzing a case. The theory used is Game Theory and Cyber Conflict. The results of the study show that the cyber war that occurred between Indonesia and Australia can be concluded: First, the conflict that occurred involved government and community actors. Second, if the cyber war is won by one party will get a little benefit then negotiations are taken to get a lot of benefits. Third, the resolution of the cyber war between Indonesia and Australia is to sign an agreement and re-establish bilateral relations. To strengthen cyber security, qualified digital readiness is needed, so cooperation is needed to create such a thing.

Keywords: Cyber War; Cyber Conflict; Readiness Digital

Pendahuluan

Ketergantungan masyarakat pada dunia digital menganggap ruang maya mudah untuk dikuasai (Ardiyanti, 2014; Bahfiarti et al., 2021; Jarir, 2019; Kilovaty, 2021). Dinamika perkembangan demokrasi dan teknologi informasi era globalisasi menuntut negara untuk bersiap dalam mengatasi berbagai fenomena yang terjadi baik skala lokal, nasional dan internasional (Abbas et al., 2024; Alviani & Gusnita, 2018; Wijaya, 2021). Ketergantungan cenderung mendorong wacana ketakutan karena kompleksitas menjadi sifat teknologi. Diperlukannya kajian yang mendalam mengenai perkembangan teknologi dan dampak yang ditimbulkan pada masa mendatang (Maness & Valeriano, 2016).

Gambar 1. Jumlah Pengguna Internet Global Secara Individu



Sumber: (Annur, 2024)

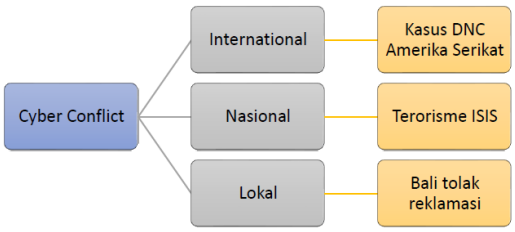
Laporan *We Are Social* mengungkapkan penggunaan internet secara global mencapai angka 5,35 miliar setara dengan 66,2% dari total 8,08 miliar populasi global. Teknologi yang berkembang pesat memberikan dampak positif dan negatif (Sholikin, 2019). Dampak positif yang dirasakan ialah memberikan kemudahan untuk masyarakat, dampak negatif yang dirasakan ialah banyaknya ancaman-ancaman yang ditimbulkan. Dunia maya (*cyber space*) dijadikan sebagai ladang untuk mendapatkan informasi dari kegiatan internet tanpa batas (Suharto & Maria Novita Apriyani, 2021).

Arus globalisasi yang terus berjalan menciptakan teknologi informasi dan komunikasi yang terus mengalami perkembangan. Pertukaran informasi yang cepat menjadikan teknologi informasi dan komunikasi bersifat fundamental . Teknologi informasi dan komunikasi melibatkan beberapa aspek seperti teknologi, rekayasa, dan teknik pengelolaan yang digunakan dalam pengendalian dan pemrosesan informasi serta penggunaannya (Wiryany et al., 2022).

Perkembangan teknologi yang semakin pesat menimbulkan berbagai tantangan konflik, kemungkinan yang paling besar adalah karena adanya faktor ekonomi, pertimbangan politik, termasuk kemampuan kekuasaan pemerintah dan tingkat demokrasi (Apandi, 2020). Konflik yang terjadi di dunia maya masih

cenderung abu-abu seperti serangan siber yang dapat memicu konflik siber (Leszczuk, 2019). Berikut disajikan contoh konflik dalam dunia digital yang terjadi pada tiga ranah yang berbeda:

Gambar 2. Kasus Konflik Siber Berbagai Tingkatan



Sumber: (Peneliti, 2024)

Peretasan terhadap institusi-institusi Amerika menunjukkan bahwa institusi-institusi demokrasi seperti pemilu atau proses pemungutan suara dan partai politik dapat menjadi target serangan siber (Baezner & Robin, 2017). Seperti kasus DNC konflik siber yang terjadi pada pemilu di Amerika Serikat (Wohlfeld & Jasper, 2018) serangan digunakan untuk mempengaruhi jalannya pemilihan presiden AS peretasan ini memberikan guncangan Partai Demokrat pada bulan terakhir kampanye dan berdampak pada stabilitas politik Amerika Serikat.

Konflik siber yang terus-menerus selain perang memengaruhi pandangan negara-negara tersebut terhadap persaingan politik internasional (Liebetrau, 2022; Lindsay, 2021) dalam kebijakan kerja sama yang dibangun (Maness & Valeriano, 2016). Diperlukan sistem keamanan untuk mencegah terjadinya serangan dan konflik siber (Herr et al., 2021) karena negara yang memiliki *cyber security* yang jauh lebih canggih dapat dengan mudah mengontrol seluruh informasi rahasia dengan tujuan mengganggu keseimbangan dan merugikan negara lain (Karisma & Burhanuddin, 2023).

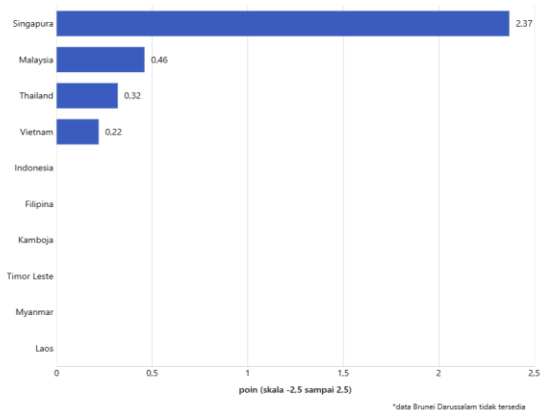
Pemicu konflik di dunia maya yang terjadi di Indonesia cukup beragam mulai dari *cyber war, cyber crime, cyber attack*, *cyber politics*, konflik media sosial hingga *hatespeech* (Bina, 2021; Indrawan, 2019; Muhammad & Yusup, 2019; Suharto & Maria Novita Apriyani, 2021). Meledaknya jumlah pengguna sosial media dapat memicu konflik virtual menjadi konflik dunia nyata (Alviani & Gusnita, 2018). Hal ini disebabkan peran media baru mengubah tatanan sosial masyarakat (Puspianto, 2022), media baru juga menyebabkan terjadinya radikalisme karena kemudahan akses informasi yang dimiliki (Sholikin, 2024).

Kemudahan informasi yang dapat diakses membuat kelompok ekstremisme semakin efektif membuat konten radikal dengan mudah dan masif (Himatul Ula Aulia, 2018; Mupida &

Mustolehudin, 2020) seperti yang dilakukan oleh kelompok ISIS untuk menarik masyarakat tergabung dalam kelompok tersebut. Dibentuklah lembaga negara untuk mengatasi permasalahan siber, seperti BSSN (Badan Siber dan Sandi Negara) dan ciptakannya regulasi untuk menangani konflik siber yang terjadi di Indonesia (Chotimah, 2019; Permanasari, 2017).

Konflik dari dunia maya juga berdampak pada pemberitaan palsu (*hoax*) (Legionosuko & Harnowo, 2017; Masril & Lubis, 2020; Razak & Sumanti, 2023; Wirawan et al., 2022) yang berdampak aksi demonstrasi di dunia nyata. Di Indonesia banyak gerakan disuarakan dalam media sosial (aktivitas medsos), sebab media juga berperan sebagai mediator dalam konflik antara masyarakat dan pemerintah (Setiadarma & Priambodo, 2023). Konflik yang ditimbulkan dalam dunia digital khususnya menggunakan media sosial perlu dilakukan manajemen konflik yang tepat.

Gambar 3. Indeks Kesiapan Digital di Negara Asia Tenggara



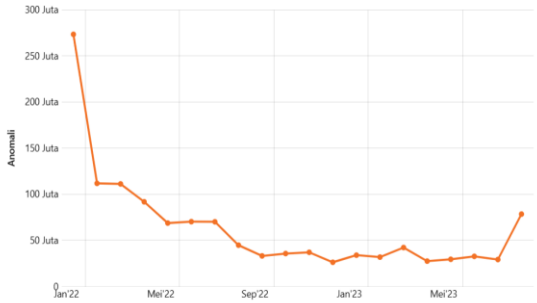
Sumber: (Muhamad, 2021)

Berdasarkan data di atas tingkat kesiapan digital di negara Asia Tenggara memperoleh hasil, Singapura (2,37 poin), Malaysia (0,46 poin), Thailand (0,32 poin), Vietnam (0,22 poin), Indonesia (-0,06 poin), Filipina (-0,25 poin), Kamboja (-0,38 poin), Timor Leste (-0,80 poin), Myanmar (-0,85 poin) dan Laos (-0,89 poin). Jika sebuah negara mendapatkan skor 1 dapat dikatakan negara tersebut memiliki kesiapan digital satu standar deviasi di atas rata-rata global. Jika negara memiliki skor -1 dapat dikatakan negara tersebut satu standar deviasi di bawah rata-rata (Muhamad, 2021).

Studi *Digital Readiness Index* untuk mengukur kesiapan digital di 146 negara yang dilakukan oleh perusahaan teknologi asal Amerika Serikat bernama Cicso. Studi dilakukan untuk mengukur kesiapan digital dengan 7 indikator, yakni mengukur tingkat kebutuhan dasar masyarakat, investasi sektor teknologi baik pemerintah atau swasta, bisnis yang mudah dijalankan, sumber daya manusia yang berkualitas, *start-up* atau iklim usaha rintisan, mengukur teknologi digital yang diadopsi, dan mengukur kondisi infrastruktur negara. Ketujuh indikator tersebut dirumuskan melalui skor dengan skala -2,5 sampai 2,5 dengan kesimpulan semakin tinggi skor

yang dimiliki semakin baik pula kesiapan digital, begitu pun sebaliknya (Muhamad, 2021).

Gambar 4. Jumlah Serangan Siber dari Anomali Trafik



Sumber: (Leoni Susanto, 2024)

Badan Siber dan Sandi Negara (BSSN) mencatat yang terhitung sejak Januari sampai September 2022 kasus serangan siber yang terjadi di Indonesia mencapai 875 juta serangan yang di identifikasi dari *traffic* anomali, dengan data keseluruhan tahun 2022 anomali *traffic* mencapai 973 juta. Dan untuk periode Januari sampai Agustus 2023 tercatat lebih dari 305 juta anomali *traffic* yang terjadi (Leoni Susanto, 2024). Untuk menghadapi tantangan konflik dunia maya, diciptakan strategi sistem keamanan untuk meminimalkan ancaman-ancaman yang mungkin menimbulkan efek negatif dari perkembangan teknologi untuk memberikan keuntungan kepada orang tertentu. Upaya yang dilakukan untuk mengurangi ancaman dunia maya dengan membangun lembaga intelijen dan lembaga siber, memisahkan antara serangan siber dengan konflik siber yang bersifat militer dan pembangunan sistem keamanan yang kuat (Karisma & Burhanuddin, 2023).

Ancaman keamanan siber mengacu pada kemungkinan tindakan kriminal atau serangan yang mencoba mengakses data secara sah, mengganggu operasi digital atau informasi kerusakan. Ancaman dunia maya dapat muncul dengan berbagai cara dan berbagai hal seperti, mata-mata perusahaan, *hacker*, kelompok teroris, organisasi kriminal hingga karyawan yang tidak puas dengan perusahaan (Sholikin, 2021). Penyerangan dunia maya ini dapat menggunakan data sensitif milik individu atau perusahaan untuk mencuri informasi atau mendapatkan akses ke rekening keuangan mereka. Itu sebabnya peran profesional dalam keamanan siber sangat dibutuhkan untuk menjaga data pribadi tetap terlindungi (Rakam et al., 2023).

Pakar dalam bidang keamanan dan sejarawan perang pada masa sebelumnya berpendapat bahwa perang yang akan terjadi selanjutnya bukan terjadi secara tradisional akan tetapi secara virtual dalam dunia siber (Rossdiana & Fahrisa, 2023). Haris mengatakan mereka yang mampu menjawab tantangan siber akan menjadi

pemegang masa depan pada era Revolusi Industri 4.0 atau era Disrupsi. Pemerintah Indonesia juga merencanakan kesiapan digital untuk transformasi kehidupan baik pemerintah, pelaku bisnis, maupun masyarakat (Rahmawati, 2019).

Kesiapan siber (*cyber readiness*) mengacu pada kemampuan suatu negara untuk bertindak melawan serangan siber. Menurut Kuehl (dalam (Makridis & Smeets, 2019) *Cyber Readiness* berbeda dengan *Cyber Power* karena *cyber readiness* menekankan pada kemampuan pertahanan, sedangkan *cyber power* berfokus pada kemampuan defensif (pertahanan) dan ofensif (provokasi). Betz dan Stevens mengatakan mungkin orang-orang mempertanyakan apakah pembahasan *readiness* antar negara merupakan hal yang sia-sia? Karena dunia maya sering dikatakan sebagai ruang tanpa batas (Makridis & Smeets, 2019). Berpedoman pada permasalahan yang terlah diuraikan, maka dalam penelitian ini penulis akan mengkaji dan memformulasikan rumusan masalah yakni "Bagaimana *digital readiness* Indonesia dalam mengatasi kasus *cyber war* Indonesia dan Australia?"

TINJAUAN PUSTAKA

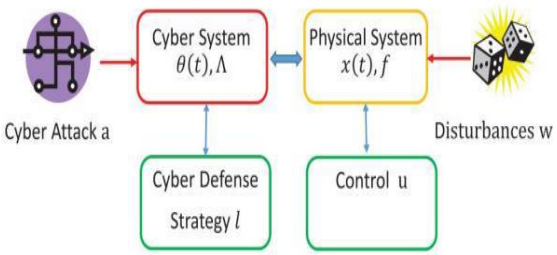
Game Theory

Teori permainan telah digunakan banyak dalam bidang keamanan dan mayoritas berfokus pada keamanan jaringan atau keamanan ekonomi. Penelitian ini menggunakan *game theory* Cuong T. Do dkk melalui kajian yang dilakukan (Anwar et al., 2020) Do dkk menggunakan *game theory* untuk mempelajari skenario pengambilan keputusan strategis untuk melawan ancaman yang disebabkan peningkatan kekhawatiran terhadap keamanan siber. Menurut Do dkk terdapat beberapa alasan yang menjadikan *game theory* lebih baik digunakan terhadap keamanan siber dan privasi, di antaranya:

1) Tindakan yang tepat waktu, karena tidak adanya insentif bagi para peserta, solusi keamanan secara tradisional diadopsi agak lambat.
2) Matematika yang terbukti, mayoritas pendekatan keamanan secara tradisional yang diterapkan pada perangkat reaktif seperti program antivirus atau alat pencegahan seperti *firewall* hanya bergantung pada heuristik.
3) Solusi terdistribusi, pengambilan keputusan dalam solusi keamanan konvensional bersifat terpusat dan tidak terdistribusi (individual).

4) Pertahanan yang andal, strategi keamanan siber yang kuat dapat diandalkan terhadap serangan.

Gambar 5. Interaksi Sistem Siber dan Fisik Mengalami Gangguan



Sumber: (Do et al., 2017)

Sistem fisik berinteraksi dengan sistem *cyber* melalui lapisan komunikasi, yang terdiri dari saluran komunikasi fisik seperti sistem nirkabel dan Internet. Lapisan jaringan dan lapisan komunikasi dianggap sebagai dunia *cyber* dari sistem. Lapisan pengawasan dan manajemen bersama-sama menjadi pemroses pusat sistem yang mengambil keputusan untuk mengendalikan sistem fisik melalui sistem siber. Keputusan biasanya dibuat oleh manusia, dengan demikian lapisan pengawasan dan manajemen sangat terkait dengan tindakan manusia. Sistem berlapis memudahkan untuk memahami mengapa sistem siber dan sistem fisik saling terkait erat dan sangat bergantung (Do et al., 2017).

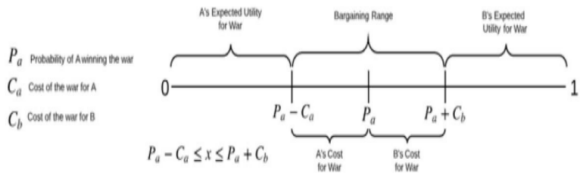
Cyber Conflict

Appelegate dan Stavrou dalam artikelnya (Castro, 2021) memberikan pengembangan taksonomi konflik siber detail yang mampu menggambarkan serangan siber secara rinci. Akan tetapi model yang digunakan tidak mencakup tingkat Hubungan Internasional karena model tersebut tidak menggambarkan atau memprediksi konsekuensi strategis atau bahkan konsekuensi militer yang lebih sempit dari serangan siber. Masih sedikitnya teori konflik siber yang koheren dengan kapasitas deskriptif, prediktif dan perspektif yang memadai. Menciptakan dua paradigma tentang konflik dunia maya (Castro, 2021).

Paradigma pertama, para ahli Hubungan Internasional mengkaji fenomena konflik dunia digital dianalisis dengan konflik tradisional yang muasalnya dari teori konflik. Paradigma kedua, para pakar Keamanan Informasi berfokus pada rincian taktis bagaimana serangan siber dilakukan, namun tidak terlibat dalam Hubungan Internasional. Untuk mengatasi perbedaan tersebut Castro mencoba mengaitkan perbedaan pendapat besar dengan teori matematis formal yang kurang digunakan dalam konflik Dunia Maya. Model matematika langsung digunakan untuk menjelaskan bahwa perang dapat digambarkan sebagai proses negosiasi. Model negosiasi digunakan sebagai dasar untuk mengembangkan konflik siber rasionalis (Castro, 2021).

Penelitian ini menggunakan *Cyber Conflict* kajian Castro (2021) yang menggagas jika telekomunikasi diretas sebagai awal dari perang kinetik, telekomunikasi tersebut akan kehilangan uang, namun seluruh negara menjadi rentan karena kurangnya telekomunikasi ketika perang dimulai. Ketika kita meningkatkan investasi pada keamanan informasi, risiko siber akan menurun. Secara teori, jika kita ingin berinvestasi dalam jumlah yang cukup, kita akan mendekati garis tingkat risiko minimum yang mungkin secara asimtot.

Gambar 7. Model Dasar *Cyber War*



Sumber: (Castro, 2021)

Model dasar merupakan model yang sangat sederhana karena kemungkinan kemenangan negara A sudah diketahui oleh kedua belah pihak yang bersaing dan tidak ada pertimbangan di masa depan, yang ada hanya pertimbangan saat ini. Dalam model ini kita dapat melihat tidak adanya operasi siber yang terjadi karena terdapat rentang tawar-menawar yang jelas. Tindakan yang rasional ketika kedua belah pihak harus bernegosiasi karena memenangkan perang akan memberikan manfaat yang lebih kecil dibanding hasil negosiasi. Namun dalam kehidupan nyata negosiasi dipengaruhi faktor emosional yang tidak dipertimbangkan dalam model ini.

Metode Penelitian

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus. Pendekatan studi kasus digunakan untuk mendapatkan pemahaman secara mendalam mengenai aspek tertentu melalui keyakinan, sikap dan perilaku manusia (Creswell, 2014). Tipe studi kasus instrumental tunggal merupakan salah satu pendekatan yang digunakan dalam penelitian.

Studi kasus instrumental tunggal memfokuskan pada isu atau persoalan, kemudian memilih satu kasus terbatas untuk di ilustrasikan. Kasus *cyber war* yang pernah terjadi antara Indonesia dan Australia menjadi kasus yang diangkat dalam penelitian. Pendekatan studi kasus digunakan dalam penelitian untuk mengungkap kasus yang terjadi khususnya dalam mengeksplorasi *Readiness Digital* Indonesia dalam mengatasi *cyber war*.

Hasil dan Pembahasan

Sejarah dan Perkembangan Teknologi Indonesia

Nenek moyang telah mengenal berbagai macam alat yang digunakan untuk menyampaikan informasi. Kentungan menjadi salah satu alat yang digunakan untuk menyampaikan informasi. Peredaan informasi ditandai dengan nada ketukan yang berbeda, informasi musibah atau informasi waktu memiliki bunyi yang berbeda. Semakin kencang bunyi yang dikeluarkan maka semakin penting sebuah informasi (Nuryanto, 2012).

Internet (*Interconnection-networking*) merupakan sistem global jaringan komputer yang saling menghubungkan antara satu dengan yang lain di seluruh penjuru dunia dengan menggunakan *standart Internet Protocol Suite*. Internet hadir di Indonesia sejak tahun 1990an (Gani, 2020). Dalam era tersebut komputer dianggap sebagai barang mewah, asing dan mahal. Teknologi informasi merupakan gabungan dari perangkat keras (*hardware*) dan perangkat lunak (*software*) (Nuryanto, 2012).

Catatan WHOIS, ARIN dan APNIC (*Who is the responsible owner of the domain name or IP address*, *American Registry for Internet Numbers* dan *Asia Pacific Network Information Centre*), jika *Internet Protocol* (IP) pertama di Indonesia di daftarkan oleh Universitas Indonesia dengan nomor UI-NETLAB (192.41.206/24) pada 24 Juni 1998. Beberapa nama yang berjasa dalam pembangunan internet di Indonesia tahun 1992–1994 ialah sebagai berikut:

Tabel 4. Nama Pendiri Internet Indonesia

No	Nama
1	RMS Ibrahim
2	Suryono Adisoemata
3	Muhammad Ihsan
4	Robby Soebiakto
5	Putu
6	Firman Siregar
7	Adi Indrayanto
8	Omo W. Purbo

Sumber: (Nurbaiti & Alfarisyi, 2023)

Tahun 1994 mulai beroperasi IndoNet yang dipimpin oleh Sanjaya. IndoNet merupakan ISP (*Internet Service Provider*) komersial pertama di Indonesia. Pihak POSTEL (Pos dan Telekomunikasi) belum mengetahui mengenai keuntungan bisnis internet karena masih sedikit sekali pengguna internet di Indonesia. Tahun 1995 menjadi awal pemerintah Indonesia melalui Departemen Pos Telekomunikasi menerbitkan izin untuk ISP yang diberikan kepada IndoNet yang dipimpin Sanjaya dan Radnet yang dipimpin BRM. Roy Rahajasa Yamin (Nurbaiti & Alfarisyi, 2023).

Teknologi informasi mengalami perkembangan yang cukup pesat. Selain perkembangan jenis peralatan teknologi berupa *software* aplikasi pendukung, perkembangan juga ditandai dengan semakin meratanya pengguna teknologi informasi. Saat ini teknologi yang hampir dimiliki seluruh lapisan masyarakat adalah *handphone* dan tidak perlu mendatangi warnet untuk memperoleh internet (Nuryanto, 2012).

Internet merupakan hasil dari kemajuan ilmu pengetahuan dan teknologi buatan manusia. Internet digunakan untuk menghubungkan jaringan komunikasi global yang terbuka dan menghubungkan jaringan yang lainnya. Jaringan-jaringan tersebut terhubung melalui telepon, satelit dan sistem komunikasi lainnya. kemudahan yang dihasilkan melalui internet menjadikannya sebagai media komunikasi (Nurbaiti & Alfarisyi, 2023).

Dominasi komputer pada saat ini dapat mengambil alih pekerjaan manusia dan mengalahkan kemampuan komputasi manusia. Era komputasi saat ini dapat mengontrol peralatan elektronik dari jarak jauh dengan internet, IoT (*Internet of Things*) memungkinkan pengguna mengelola dan mengoptimalkan elektronik dan peralatan listrik yang menggunakan internet. Tantangan yang dimiliki IoT adalah menjembatani kesenjangan antara dunia fisik dan dunia informasi (Adani & Salsabil, 2019).

Sejarah Serangan *Cyber*

Serangan siber pertama di dunia dilakukan oleh seorang mahasiswa pascasarjana Cornell University bernama Robert Tappan Morris pada November 1988. Morris menciptakan program yang melakukan perjalanan dari komputer ke komputer dan menjadi satu jenis serangan siber. Untuk mengetahui seberapa banyak komputer yang dapat terhubung dengan internet. Melalui perjalanannya dari komputer, programnya meminta setiap mesin mengirim sinyal kembali ke server kontrol dan akan terus di hitung (Sulistyo, 2014).

Program yang diciptakan Morris bekerja dengan cukup baik sampai perjalanannya terlalu cepat dan menimbulkan masalah, seperti penyumbatan karena kapasitas komputer tidak bisa menampung program yang berjalan begitu cepat dan besar. Program tersebut dinamakan sebagai *Distributed Denial of Service* atau DDoS, di mana sejumlah besar perangkat yang terhubung internet termasuk komputer, *webcam*, dan gadget pintar lainnya diberitahu untuk mengirimkan

banyak *traffic* ke satu alamat tertentu. Morris juga mendapatkan julukan *worm* (cacing) karena memperlambat kinerja komputer yang terhubung pada jaringan sampai pada titik di mana komputer tidak dapat digunakan.

Selanjutnya pada tahun 1990 perseteruan antara kelompok pro-Rusia dan kelompok pro-Chechnya. Gerakan separatis Chechen dianggap sebagai pelopor dalam penggunaan jaringan internet sebagai alat untuk menyampaikan propaganda, melalui situs *Kavkaz.org* yang beralamat *hosting-ip* di Amerika. Tahun 1999 juga dinyatakan sebagai Sejarah perang internet pertama yang berskala luas, terjadi ketika pesawat NATO melakukan serangan bom terhadap Serbia, kelompok peretas pro-Serbia atau anti-Barat menamakan dirinya sebagai *Black Hand*. Perang internet ini menyerang infrastruktur internet milik *North Atlantic Treaty Organization* (NATO) untuk mengganggu jalannya operasi NATO di Serbia dengan menggunakan *Denial of Service* (DoS) serta virus yang disiapkan pada email (Sulistyo, 2014).

Serangan siber pernah terjadi pada tahun 2000 antara Israel dan palestina. Serangan siber bermula dari penculikan 3 tentara Israel, kelompok pro-Israel melakukan serangan dengan menanamkan *file* lagu kebangsaan dan gambar bendera Israel yang muncul pada halaman muka dari situs resmi milik Hizbullah. Serangan pro-Israel selanjutnya ditargetkan kepada situs resmi militer dan organisasi politik yang dianggap bermusuhan dengan Israel, termasuk Otoritas Nasional Palestina, Hamas dan Iran. Kelompok pro-Palestina melakukan serangan terhadap infrastruktur militer, telekomunikasi, politik, media, universitas, *bank of Israel*, situs *e-commerce*, serta Bursa Efek Tel Aviv (Sulistyo, 2014). Serangan siber terus berkembang sampai sekarang.

Kronologi *cyber war* Indonesia dan Australia

Indonesia pernah mengalami serangan siber pada tahun 2013 oleh Australia. Media Australia mengungkapkan jika *Australian Signal Directorate* (ASD) telah melakukan penyadapan terhadap komunikasi pejabat pemerintah Indonesia, termasuk Presiden Susilo Bambang Yudhoyono. Kasus ini memicu ketegangan diplomatik antara Indonesia dan Australia dan mendorong Indonesia untuk meningkatkan keamanan siber yang berasal dari Indonesia.

Pada bulan November 2013 terdapat sebuah insiden dimana terungkapnya aksi penyadapan yang

dilakukan badan pemerintah Australia tepatnya oleh Departemen Pertahanan. Aksi penyadapan ini diperkuat dengan publikasi media *The Guardian* dan *Australian Broadcasting Corporation* (ABC) *News* yang merupakan dua media besar Australia pada tanggal 18 November 2013, menimbulkan berbagai reaksi keras dari kedua negara. Indonesia merasa tersinggung dan Australia merasa media tersebut membahayakan posisi Australia (Yacobus, 2013).

Pengungkapan ini dilakukan berdasarkan dokumen rahasia yang dibocorkan oleh Edward Snowden, *whistle blower* Amerika Serikat. Sehingga terungkap jika Australia melakukan penyadapan komunikasi di Indonesia. Dalam dokumen tersebut dicantumkan nama-nama pihak yang menjadi sasaran mulai dari presiden SBY, Ibu negara, sampai pejabat tinggi negara lainnya lengkap dengan jenis perangkat telepon genggam yang digunakan.

Gambar 14. Sasaran Penyadapan

	Name/Position	Handset	Generation
1	Susilo Bambang Yudhoyono	Nokia E90-1	3G
2	Kristiani Herawati (First Lady)	Nokia E90-1	3G
3	Boediono (new Vice President)	Blackberry Bold (9000)	3G
4	Yusuf Kalla (former Vice President)	Samsung SGH-Z370	3G
5	Dino Patti Djalal (Foreign Spokesman)	Blackberry Bold (9000)	3G
6	Andi Mallarangeng (Domestic Spokesman)	Nokia E71-1	3G
7	Hatta Rajasa (State Secretary)	Nokia E90-1	3G
8	Sri Mulyani Indrawati (MENKO EKON)	Nokia E90-1	3G
9	Widodo Adi Sucipto (MENKO POLKAM)	Nokia E66-1	3G
10	Sofyan Djalil (Minister – Confidant)	Nokia E90-1	3G

Sumber : (Yacobus, 2013)

Pemerintah Indonesia segera melakukan berbagai langkah untuk merespons aksi penyadapan dengan menuntut keras duta besar Australia untuk menjelaskan laporan mata-mata dari kedutaan besar Jakarta. Indonesia juga menarik duta besar RI untuk Australia yakni Nadjib Riphhat Kesoema untuk konsultasi dan sebagai bentuk protes penyadapan. Penghentian kerja sama bilateral dalam bidang pertukaran informasi, pertukaran intelijen dan latihan bersama juga dihentikan sampai adanya penjelasan resmi dari Canberra.

Kasus yang terjadi juga menimbulkan reaksi dari pada *hacker* Indonesia yang tergabung dalam *Anonymous* Indonesia (AnonIndo). Serangan siber pada sejumlah perusahaan Australia juga di laporkan menjadi target pada tahun 2015. Serangan tersebut berasal dari kelompok *hacker* Indonesia dan diduga memiliki

hubungannya dengan isu politik dan diplomatik antar kedua negara.

Gambar 15. Percakapan *Cyber War* Indonesia dan Australia

Sumber: (Yacobus, 2013)

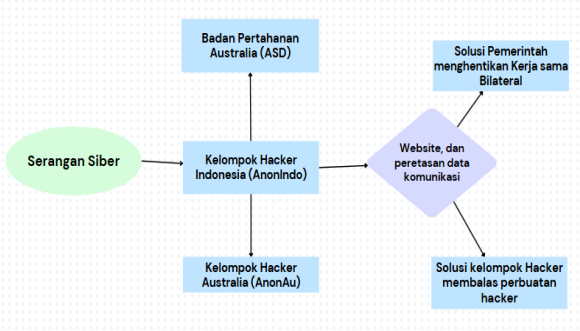
Mulanya AnonIndo melakukan penyerangan terhadap situs-situs Australia dengan total peretasan sebanyak 170 situs. Kelompok *hacker* Australia yang tergabung dalam AnonAU, menganggap maklum kejadian tersebut. Karena sebagai bentuk ketidakpercayaan terhadap pemerintah Australia atas kesempatan yang telah diberikan. Tetapi AnonIndo juga mencoba melakukan peretasan bukan hanya melalui *platform* pemerintah akan tetapi juga menyasar milik masyarakat.

AnonAU berupaya untuk melakukan penyerangan balik dengan meninggalkan pesan jika penyerangan hanya menyasar situs pemerintah bukan milik masyarakat. AnonIndo mengikuti saran yang diberikan kemudian berhasil menyerang situs badan intelijen Australia yang bernama *Australian Security Intelligence Organisation* (ASIO). Namun karena beberapa kelompok AnonIndo masih menyerang situs masyarakat sipil, maka AnonAu mengambil tindakan untuk membalas serangan dengan menyasar pada berbagai kementerian dan infrastruktur kritikal.

Analisis Game Theory Cuong T. Do dkk

Game theory digunakan untuk menganalisis interaksi strategis antara aktor-aktor yang terlibat dalam konflik siber dan mengambil solusi cepat dalam menjalankan permainan. Aktivitas siber yang terjadi antara Indonesia dan Australia melibatkan beberapa aktor yang terdiri dari pemerintah Indonesia, kelompok *hacker* Indonesia atau AnonIndo, pemerintah Australia dan AnonAu. Kepala Badan Intelijen Nasional Marciano Norman tahun 2011-2015 mengungkapkan jika Australia sudah melakukan penyadapan percakapan sejak 2007 sampai 2009.

Gambar 16. Analisis Game Theory



Sumber: (Peneliti, 2024)

Interaksi yang terjadi ialah penyadapan melalui perangkat telepon yang digunakan pejabat. Aksi yang dilakukan oleh aktor ASD kepada Aktor Pemerintah Indonesia. Adapun sasaran terdiri dari Presiden SBY, Ibu Negara Kristiani Herawati, Boediono, Yusuf Kalla, Dino Patti Djalal, Andi Mallarangeng, Hatta Rajasa, Sri Mulyani Indrawati, Widodo Andi Sucipto dan Sofyan Djalil. Solusi yang dilakukan pemerintah untuk menghentikan kerja sama bilateral antara Indonesia dan Australia.

Selanjutnya terjadi interaksi serangan siber yang dilakukan oleh aktor AnonIndo, yang menyerang berbagai *website* masyarakat Australia. Bertujuan untuk mengganggu jaringan siber tersebut sebagai bentuk pembalasan. Karena serangan terus terjadi, AnonAu juga melakukan serangan balasan yang menyasar pada Angkasa Pura, Solo *Airport*, Kementerian Pendidikan dan Garuda *Airways*. Solusi yang dilakukan para kelompok *hacker* dengan saling melakukan peretasan.

Jika kita berfokus pada interaksi pada aktor pemerintahan, menurut Do dkk *game theory* akan memahami bagaimana aktor membuat keputusan dan mengambil tindakan dalam konflik siber yang saling mempengaruhi. Indonesia menuntut penjelasan dari pemerintah Australia, tetapi karena respons yang diberikan Mark Textor seorang ahli strategi dan konsultan *polling* Partai Liberal Australia melakukan cemooh terhadap Presiden SBY, maka SBY menyatakan menghentikan kerja sama dengan Australia.

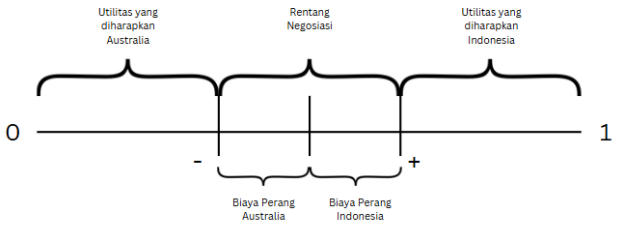
Analisis *Cyber Conflict* Sergio Castro

Appelegate dan Stavrou memberikan pengembangan taksonomi konflik siber detail yang mampu menggambarkan serangan siber secara rinci. Akan tetapi model yang digunakan tidak mencakup tingkat Hubungan Internasional karena model tersebut tidak menggambarkan atau memprediksi konsekuensi strategis atau bahkan konsekuensi militer yang lebih sempit dari serangan siber. Masih sedikitnya teori konflik siber yang koheren dengan kapasitas deskriptif, prediktif dan perspektif yang memadai. Menciptakan dua paradigma tentang konflik dunia maya (Castro, 2021).

Paradigma pertama, para ahli Hubungan Internasional mengkaji fenomena konflik dunia digital dianalisis dengan konflik tradisional yang bermuasal dari teori konflik. Paradigma kedua, para pakar Keamanan Informasi berfokus pada rincian taktis bagaimana

serangan siber dilakukan, namun tidak terlibat dalam Hubungan Internasional. Untuk mengatasi perbedaan tersebut Castro mencoba mengaitkan perbedaan pendapat besar dengan teori matematis formal yang kurang digunakan dalam konflik Dunia Maya. Model matematika langsung digunakan untuk menjelaskan bahwa perang dapat digambarkan sebagai proses negosiasi. Model negosiasi digunakan sebagai dasar untuk mengembangkan konflik siber rasionalis (Castro, 2021).

Gambar 18. Model *Cyber Conflict* Indonesia dan Australia



Sumber: (Peneliti, 2024)

Menganalisis dalam perspektif Sergio Castro mengungkapkan jika kemungkinan kemenangan negara Australia sudah diketahui kedua negara, dikarenakan teknologi keamanan Australia jauh di atas Indonesia. Sehingga tidak adanya pertimbangan atas penyerangan yang dilakukan. Tetapi Indonesia dibantu oleh AnonIndo untuk melakukan penyerangan balik pada pemerintahan Asutralia. Sehingga rentang negosiasi terpampang jelas, tindakan negosiasi digunakan sebagai solusi yang rasional. Sebab memenangkan akan memberikan manfaat sedikit dibandingkan dengan hasil negosiasi. Proses negosiasi dipengaruhi oleh faktor emosional, sebab pada mulanya Mark Textor memberikan respons yang kurang baik bahkan mengejek presiden SBY.

Perdana Menteri Australia Tony Abbot menganggapi kasus penyadapan kepada pemerintah Indonesia dengan melakukan konferensi pers. Tetapi ketika pemerintah Indonesia bertanya maksud dan tujuan dari penyadapan serta menuntut permintaan maaf, PM Tony Abbott justru mengungkapkan jika Australia tidak perlu melakukan permohonan maaf. Sebab penyadapan ataupun serangan siber lainnya lazim terjadi di dunia internasional serta hal demikian merupakan kebutuhan untuk melindungi kepentingan nasional Australia.

Kasus penyadapan ini menjadi kasus serius karena dapat menjadi ancaman untuk kedaulatan dan keamanan negara Indonesia. Kebijakan yang di ambil oleh presiden SBY untuk menghentikan pertukaran informasi dan pelatihan intelijen dengan Australia di hentikan sebagai bentuk protes atas penyadapan tersebut. PM Tony Abbott

merespons hal tersebut dengan membalas surat resmi yang diberikan Presiden SBY, Abott menyatakan jika ingin mengembalikan hubungan kerja sama kedua negara dan berjanji untuk tidak melakukan tindakan yang merugikan Indonesia (Megananda & Sholeh, 2020).

PM Tony Abbott memberikan balasan untuk Presiden SBY yang berisikan beberapa kebijakan luar negeri yang baru sebagai upaya resolusi konflik dan perdamaian. Adapun kebijakannya sebagai berikut:

a. Menugaskan Menteri Luar Negeri Marty Natalegawa untuk membicarakan masalah-masalah sensitif yang berkaitan dengan hubungan bilateral Indonesia-Australia.
b. Presiden SBY kemudian menindaklanjuti dengan melakukan pembahasan protokol dan kode etik kerja sama setelah diadakannya *mutual understanding* dan *mutual agreement* oleh kedua belah pihak.
c. Presiden SBY memastikan *draft* protokol dan kode etik apakah sudah memadai dan sesuai dengan keinginan Indonesia.
d. Pengesahan protokol dan kode etik dilakukan di hadapan kepala pemerintahan kedua negara.
e. Selanjutnya kedua negara melakukan observasi dan evaluasi dalam melakukan protokol dan kode etik tersebut.

Kerja sama yang sempat terjalin, kemudian terhenti karena adanya penyerangan kembali dilanjutkan antara Indonesia dan Australia. Kerja sama tersebut terjalin kembali dengan adanya beberapa protokol dan kode etik yang harus dipatuhi. Dengan adanya aturan tersebut Presiden SBY meyakini jika ke depannya Australia tidak mengulangi kesalahan yang sama dan mulai memperbaiki hubungan antara Indonesia dan Australia. Langkah Ini diambil karena Presiden SBY menjadi pemimpin yang ingin mendapatkan keuntungan ekonomi untuk Indonesia. Sehingga memperluas hubungan kerja sama luar negeri menjadi kebijakan yang diambil oleh Presiden SBY, sebab presiden memiliki otoritas penuh dalam pengambilan keputusan atas kejadian penyadapan tersebut (Salehun & Sulaiman, 2019).

Readiness Digital Mengatasi *Cyber War*

Readiness digital untuk mengatasi *cyber war* diartikan sebagai sejauh mana

kesiapan dan kemampuan Indonesia dalam menghadapi ancaman *cyber war*. Beberapa aspek yang dapat menggambarkan *readiness* digital, antara lain sebagai berikut:

a. Infrastruktur dan kapabilitas pertahanan siber. Ketersediaan dan keandalan infrastruktur teknologi informasi dan komunikasi Indonesia pada tahun 2013 belum mumpuni serta masih dalam tahap transisi. Infrastruktur Telkom IDN sebagai bentuk pengembangan infrastruktur *board* oleh Telkom Group untuk memperkuat akses dan kapasitas infrastruktur dilakukan pada tahun 2015. Penggunaan internet juga belum merata dengan penggunaan 80 juta dari 250 juta jiwa.
b. Regulasi dan kebijakan keamanan siber. Kerangka hukum dan peraturan yang mengatur tentang keamanan siber Indonesia telah memilikinya melalui UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dan PP No. 28 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi elektronik sebagai regulasi dunia siber. Pemerintah Indonesia juga membuat kebijakan untuk melakukan kerja sama luar negeri dalam bidang siber.
c. Kesiapan masyarakat dan sektor swasta. Kemampuan masyarakat dalam merespons dan memulihkan diri dari serangan siber dapat dilihat melalui AnonIndo. Meskipun masih dikatakan sedikit yang memahami dunia siber tahun 2013.
d. Kerja sama Internasional. Meskipun Indonesia dan Australia sempat bersitegang atas kejadian penyadapan, akan tetapi resolusi konflik dapat diatasi dengan menghasilkan kerja sama dalam memperkuat kapabilitas ruang siber. Di bawah kepemimpinan Hinsa Siburian, melalui BSSN Indonesia kembali melakukan MoU dengan Australia pada tanggal 8 September 2021 yang di mana klausul MoU ini agak sedikit berubah dengan ditambahkannya *Cyber and Emerging Cyber Technology Cooperation* yang mana dalam MoU ini masih erat kaitannya dengan *Confidence Building Measure* dan *Capacity Building.*

Di era digital saat ini, kesiapan digital menjadi komponen kritis dalam

pertahanan nasional menghadapi ancaman *cyber war* (Darumaya et al., 2023). Kompleksitas perang siber membutuhkan pendekatan komprehensif yang melibatkan infrastruktur teknologi yang tangguh, sumber daya manusia berkualitas, dan strategi pertahanan yang adaptif. Infrastruktur teknologi merupakan fondasi utama kesiapan digital. Pemerintah dan lembaga strategis perlu mengembangkan sistem keamanan siber berlapis yang mampu mendeteksi, mencegah, dan merespons serangan siber secara cepat dan efektif. Hal ini mencakup pengembangan *firewall* canggih, sistem deteksi intrusi, dan mekanisme pemulihan data yang handal.

Investasi berkelanjutan dalam teknologi pertahanan siber menjadi kunci untuk melindungi aset-aset digital kritis dari potensi serangan musuh. Aspek sumber daya manusia tidak kalah pentingnya dalam kesiapan digital. Pembentukan pasukan *cyber defense* profesional dengan keahlian tinggi dalam teknologi informasi, keamanan siber, dan intelijen digital menjadi prasyarat mutlak. Pelatihan berkelanjutan, simulasi serangan siber, dan pengembangan kemampuan analitis para personel keamanan siber akan menciptakan pertahanan yang proaktif dan responsif terhadap ancaman yang terus berkembang (Darumaya et al., 2023).

Penutup

Indonesia menjadi negara yang paling rentan terhadap serangan siber ditandai dengan banyaknya kasus serangan siber yang terjadi. Penyebab terjadinya serangan siber karena *readiness* digital Indonesia yang belu mapan dan masih terus di kembangkan. Indonesia pernah mengalami serangan siber pada tahun 2013 yang dilakukan oleh pemerintah Australia melalui penyadapan yang dilakukan melalui *handphone* yang dimiliki beberapa pejabat tinggi. Konflik tersebut memicu aksi serang siber antar dua negara yang dilakukan oleh ANonIndo dan AnonAU, resolusi yang dihasilkan dari konflik tersebut ialah dengan menjalin kerja sama untuk memperkuat serangan siber. Karena siber bukan hal sepele, serangan siber merupakan penyerangan serius yang harus dihadapi pada masa kemajuan teknologi saat ini. Diperlukan kesiapan yang matang dalam menghadapi tantangan teknologi maju.

Referensi

Abbas, W., Ismira, A., & Losi, Z. (2024). Measuring Radicalism in International Relations: an Analysis and Interpretation in West Sulawesi. *Journal of Humanities and Social Sciences Innovation*, *4*(1), 2775–6165.

Adani, F., & Salsabil, S. (2019). INTERNET OF THINGS : *ISU Teknologi STT Mandala*, *14*(2), 92–99.

Alviani, S. R., & Gusnita, C. (2018). Analisis Media Sosial Sebagai Pembentuk Konflik Sosial di Masyarakat Sosial di Masyarakat. *Core Universitas Terbuka*, 221–241.

Annur, C. M. (2024). *Individu Pengguna Internet Global Tembus 5,35 Miliar pada Januari 2024*. Databoks. https://databoks.katadata.co.id/datapublish/2024/02/08/individu-pengguna-internet-global-tembus-535-miliar-pada-januari-2024

Anwar, F., Ul, B., Khan, I., Olanrewaju, R. F., & Pampori, B. R. (2020). A Comprehensive Insight into Game Theory in relevance to Cyber Security. *Indonesian Journal of Electrical Engineering and Informatics*, *8*(1), 189–203. https://doi.org/10.11591/ijeei.v8i1.1810

Apandi. (2020). Pendekatan Resolusi Konflik Dalam Upaya Pencegahan Konflik Regional Pada Era Digitalisasi. *Jurnal Inovasi Ilmu Sosial Dan Politik*, *2*(1), 94. https://doi.org/10.33474/jisop.v2i1.6414

Ardiyanti, H. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Jurnal Politica*, *5*(1), 95–110.

Baezner, M., & Robin, P. (2017). Cyber-conflict between the United States of America and Russia. *CSS Cyberdefense Hotspot Analyses (2)*, *2*.

Bahfiarti, T., Theriady, A. A. Z., Akmalia, D., & Sabir, T. A. (2021). Penggunaan Media Sosial pada Calabai di Sulawesi Selatan. *Jurnal Komunikasi Global*, *10*(2), 197–213. https://doi.org/10.24815/jkg.v10i2.22343

Bina, M. A. H. (2021). Fenomena Hate Speech di Media Sosial dan Konstruk Sosial Masyarakat. *Jurnal Peurawi: Media Kajian Komunikasi Islam*, *4*(1), 92–100.

Castro, S. (2021). Towards the Development of a Rationalist Cyber Conflict Theory. *The Cyber Defense Review*, *4*(1), 125–136.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *10*(2), 113–128. https://doi.org/10.22212/jp.v10i2.1447

Creswell, J. W. (2014). Penelitian Kualitatif & Desain Riset: Mamilih Diantara Lima Pendekatan. In S. Z. Qudsy (Ed.), *Pustaka Belajar* (Edisi 3). SAGE.

Darumaya, B. A., Maarif, S., Toruan, T., & Swastanto, Y. (2023). Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan. *Jurnal Keamanan Nasional*, *IX*(2), 299–324.

Do, C. T., Tran, N. H., Hong, C., Kamhoua, C. A., Kwiat, K. A., Blasch, E., Ren, S., Pissinou, N., & Iyengar, S. S. (2017). Game theory for cyber security and privacy. *ACM Computing Surveys*,

50(2), 30–37. https://doi.org/10.1145/3057268

Gani, A. G. (2020). SEJARAH dan PERKEMBANGAN INTERNET DI INDONESIA Alcianno Ghobadi Gani, ST. *Jurnal Mitra Manajemen*, *5*(2).

Herr, T., Laudrain, A. P. B., & Smeets, M. (2021). Mapping the Known Unknowns of Cybersecurity Education: A Review of Syllabi on Cyber Conflict and Security. *Journal of Political Science Education*, *17*(S1), 503–519. https://doi.org/10.1080/15512169.2020.1729166

Himatul Ula Aulia. (2018). *Potensi Ancaman Global terhadap POTENSI ANCAMAN GLOBAL TERHADAP*. 1–9.

Indrawan, J. (2019). Cyberpolitics Sebagai Perspektif Baru Memahami Politik di Era Siber [Cyberpolitics as A New Perspective in Understanding Politics in The Cyber Era]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *10*(1), 1–16. https://doi.org/10.22212/jp.v10i1.1315

Jarir. (2019). Solusi Konflik Agama Di Media Sosial. *TOLERANSI: Media Ilmiah Komunikasi Umat Beragama*, *10*(2), 106. https://doi.org/10.24014/trs.v10i2.7080

Karisma, I., & Burhanuddin, A. (2023). Signifikansi Perang Siber dalam Konflik Modern Rusia-Ukraina Studi Kasus: Wizard Spider-It Army. *Jurnal Ilmu Sosial Dan Humaniora)*, *1*(Juni), 800–817.

Kilovaty, I. (2021). Cyber Conflict and the Thresholds of war. *University of Arkanas*, 1–38.

Legionosuko, T., & Harnowo, S. (2017). Dinamika fake news atau hoax sebagai sumber konflik horisontal pada pilkada propinsi dki tahun 2017. *Jurnal Prodi Damai Dan Resolusi Konflik*, *3*(3), 111–136.

Leoni Susanto. (2024). *Cek Data: Anies Menyinggung 800 Juta Serangan Siber di Indonesia, Seperti Apa Datanya?* Databoks. https://databoks.katadata.co.id/datapublish/2024/01/07/cek-data-anies-menyinggung-800-juta-serangan-siber-di-indonesia-seperti-apa-datanya

Leszczuk, S. (2019). Cyber conflict in the light of article 5 of the North Atlantic treaty. *Історико-Політичні Проблеми Сучасного Світу*, *11*(39), 12–20. https://doi.org/10.31861/mhpi2019.39.12-20

Liebetrau, T. (2022). Cyber conflict short of war: a European strategic vacuum. *European Security*, *31*(4), 497–516. https://doi.org/10.1080/09662839.2022.2031991

Lindsay, J. R. (2021). Cyber conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem. *Intelligence and National Security*, *36*(2), 260–278. https://doi.org/10.1080/02684527.2020.1840746

Makridis, C. A., & Smeets, M. (2019). Determinants of cyber readiness. *Journal of Cyber Policy*, *4*(1), 72–89.

https://doi.org/10.1080/23738871.2019.1604781

Maness, R. C., & Valeriano, B. (2016). The Impact of Cyber Conflict on International Interactions. *Armed Forces and Society*, *42*(2), 301–323. https://doi.org/10.1177/0095327X15572997

Masril, M., & Lubis, F. W. (2020). Analisis Penggunaan Media Sosial dan Penyebaran Hoax Di Kota Medan. *JURNAL SIMBOLIKA: Research and Learning in Communication Study*, *6*(1), 11–22. https://doi.org/10.31289/simbollika.v6i1.2937

Megananda, S., & Sholeh, B. (2020). Hubungan Australia-Indonesia Di Masa Pemerintahan Presiden Susilo Bambang Yudhoyono (Sby). *Global Insight Journal*, *5*(2), 16–34. https://doi.org/10.52447/gij.v5i2.4033

Muhamad, N. (2021). Indeks Kesiapan Digital Asia Tenggara, Skor Indonesia Tergolong Rendah. *Databoks*, *2021*.

Muhammad, & Yusup, M. (2019). Exegetic Cyberwar: Religiious Diactics in New Media. *Esensia*, *20*(2), 171–182.

Mupida, S., & Mustolehudin. (2020). New Media Dan Konflik Ekstrimis Perempuan Indonesia. *Jurnal Bimas Islam*, *13*(2), 345–370. https://doi.org/10.37302/jbi.v13i2.231

Nurbaiti, & Alfarisyi, M. F. (2023). Sejarah Internet di Indonesia. *Jurnal Ilmu Komputer, Ekonomi Dan Manajemen (JIKEM)*, *3*(2), 2336–2344.

Nuryanto, H. (2012). *Sejarah Perkembangan Teknologi Informasi dan Komunikasi*. PT Balai Pustaka.

Permanasari, A. (2017). Bagi Kerangka Hukum Indonesia Tentang Pertahanan Siber. *Jurnal Hukum Pidana Dan Pembangunan Hukum*.

Puspianto, A. (2022). Peran Media Baru Dalam Membentuk Cyber Society. *An-Nida' : Jurnal Komunikasi Dan Penyiaran Islam*, *11*(1), 98–123. https://doi.org/10.61088/annida.v11i1.439

Rahmawati, C. (2019). Tantangan dan ancaman keamanan siber indonesia di era revolusi industri 4.0. *Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO AAU)*, *1*(1), 299–306.

Rakam, R., Imron, C., Purnomo, J., & ... (2023). Cyber Warfare Threats and Analyzing Readiness of the Indonesian Navy in Prioritizing Variables. *Sttal …*, *7*.

Razak, A., & Sumanti, S. T. (2023). Penggunaan Media Sosial Sebagai Media Komunikasi Dalam Penyebaran Informasi Pada Dinas Kominfo Kota Medan. *Communication & Social Media*, *3*(1), 1–6. https://doi.org/10.57251/csm.v3i1.939

Rossdiana, R. A., & Fahrisa, T. R. (2023). Strategi Cybersecurity Pemerintah India Dari Perspektif Kautilya. *Indonesian Journal of International Relations*, *7*(1), 140–164. https://doi.org/10.32787/ijir.v7i1.408

Salehun, L. W., & Sulaiman, Y. (2019). Kebijakan Luar Negeri Indonesia

dan Kepemimpinan Susilo Bambang Yudhoyono: Studi Kasus Spionase Australia. *Jurnal Agregasi : Aksi Reformasi Government Dalam Demokrasi*, *7*(2), 147–162. https://doi.org/10.34010/agregasi.v7i2.2561

Setiadarma, W., & Priambodo, B. (2023). Peran Media Sebagai Kontrol Sosial dalam Mengurai Konflik masyarakat dengan Pemerintah Kota Surabaya. *Jurnal Media Pengabdian Kepada Masyarakat (MPKM)*, *2*(2), 1–4.

Sholikin, A. (2019). Cyberspace: RUANG PUBLIK BARU BAGI AKTIVITAS POLITIK MUHAMMADIYAH (Cyberspace: New Public Space for Muhammadiyah's Political Activities). *Profetik Jurnal Komunikasi*, *12*(2).

Sholikin, A. (2021). Implementation of Green and Clean Policies in Environmental Governance Perspective in Lamongan Regency. *Jurnal Ilmu Administrasi: Media Pengembangan Ilmu Dan Praktek Administrasi*, *18*(1), 104–117.

Sholikin, A. (2024). Implementation of Transparency and Accountability Principles in Extractive Industry Governance in Bojonegoro Regency. *Konferensi Nasional Ilmu Administrasi*, *8*(1), 258–266.

Suharto, M. A., & Maria Novita Apriyani. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. *Risalah Hukum*, *17*, 98–107. https://doi.org/10.30872/risalah.v17i2.705

Sulistyo, A. (2014). Sejarah dan Perkembangan Perang Siber. *Universitas Pertahanan Indonesia*, *3*, 1–6.

Wijaya, S. H. B. (2021). Penyuluhan Literasi Media Tentang Hoax Di Kalangan Generasi Muda Desa Juwok. *Dedikasi: Jurnal Pengabdian Kepada Masyarakat*, *1*(1), 1–10. https://doi.org/10.46368/dpkm.v1i1.300

Wirawan, I. G. M. A. S., Mudana, I. W., Sitompul, L. U., Nur, I., & Purnawibawa, R. A. G. (2022). Demokrasi Digital Di Masa Pandemi Covid-19 (Studi Kasus Pilkada Tahun 2020 Di Kabupaten Jembrana). *Sosioglobal : Jurnal Pemikiran Dan Penelitian Sosiologi*, *6*(1), 62. https://doi.org/10.24198/jsg.v6i1.36839

Wiryany, D., Natasha, S., & Kurniawan, R. (2022). Komunikasi Terhadap Perubahan Sistem. *Jurnal Nomosleca*, *8*(Oktober), 242–252.

Wohlfeld, M., & Jasper, J. (2018). *Cyberattacks and Cyber Conflict : Where is Conflict Resolution ?* 5–17.

Yacobus, D. (2013). Hacker'S Conflict As Non-State Actor in the Tension Between Indonesia – Australia'S Relationship in 2013. *Jurnal Prodi Peperangan Asimetris*, *3*(2), 17–23.