ANTISIPASI PERTAHANAN DAN KEAMANAN *CYBERPOLITICS* DENGAN *ARTIFICIAL INTELLIGENCE*

Budi Pramono, Lukman Yudho Prakoso
Universitas Pertahanan RI Kawasan IPSC Sentul
budindonesia@gmail.com, lukman.prakoso@outlook.com

Abstract

Artificial Intelligence has recently come to the fore in the midst of technological advances that have penetrated every area of life, including in the world of politics. Cyberpolitics came to the fore with the events of the 2016 United States presidential election, the competition that occurred between presidential candidates provided a potential threat to defense and security for a country. The purpose of writing this article is to create conceptual ideas for applying AI to anticipate the adverse effects of Cyberpolitics. The method of writing this article uses literature study and William Dunn's policy formulation theory. The results of the discussion show that the formulation carried out is observed through the process of policy issues in which the problem is discussed, through the preparation of the policy formulation team and the pre-policy process which includes the preparation of academic papers. Formulation and determination of policies with policy actors through a public process followed by the process of formulating policies and ending with policy decisions.

Keywords: Artificial Intelligence, Cyberpolitics, driver force, command center

Abstrak

Artificial Intelligence mejadi mengemuka akhir-akhir ini ditengah kemajuan teknologi yang sudah merambah disetiap bidang kehidupan, termasuk di dalam dunia perpolitikan. *Cyberpolitics* menjadi mengemuka seiring peristiwa pemilihan presiden Amerika Serikat 2016, kompetisi yang terjadi antara calon presiden memberikan potensi ancaman pertahanan dan keamanan bagi sebuah negara. Tujuan penulisan artikel ini adalah untuk membuat gagasan konsepsi penerapan AI untuk mengantisipasi dampak buruk dampak dari *Cyberpolitics.* Metode penulisan artikel ini menggunakan studi pustaka dan teori perumusan kebijakan William Dunn. Hasil pembahasan menunjukkan bahwa perumusan yang dilaksanakan diamati melalui proses isu kebijakan yang di dalamnya membahas mengenai masalah, melalui penyiapan tim perumus kebijakan dan proses pra kebijakan yang

didalamnya terdapat pembuatan naskah akademik. Perumusan dan penetapan kebijakan bersama aktor kebijakan melalui proses publik yang dilanjutkan dengan proses merumuskan kebijakan lalu diakhiri dengan penetapan kebijakan.

Kata Kunci: Artificial Itelligence, Cyberpolitics, driver force, command centre

Article History: *Reccived 22 Agust 2022, Revised: 15 September 2022, Accepted: 01 November 2022, Available online 01 Desember 2022*

Pendahuluan

Artificial Intelligence (AI) atau kecerdasan buatan adalah salah satu produk kemajuan teknologi yang diciptakan untuk meniru fungsi kognitif manusia. Basis sistem AI adalah seperti menganalisis data, memahami pola, mengenali lingkungan sekitar hingga membuat keputusan. AI diciptakan untuk memahami dan memberi solusi terhadap suatu masalah dengan lebih cepat dan efektif. Teknologi AI diharapkan mampu menyelesaikan pekerjaan manusia dengan lebih mudah serta memberi hasil yang maksimal dibandingkan jika dikerjakan secara manual oleh manusia.

Kemajuan teknologi semakin pesat dan pemanfaatannya diberbagai bidang termasuk pada bidang politik. Pemelihan presiden Amerika Serikat (AS) pada tahun 2016 adalah sebagai contoh bagaimana penggunakan teknologi *cyber* yang diimplementasikan menjelma menjadi *cyberwar* dalam kontestansi pemilihan presiden, Penggunaan *cyberwar* pada pemilihan presiden tersebut bukan saja mempengaruhi AS tetapi juga dunia, saham-saham di AS dan dunia terkoreksi dengan tajam (Indrastiti, 2016).

Cyberpolitics di AS tahun 2016 menjelma menjadi cyberwar telah memberikan dampak negative bagi AS dan juga mempengaruhi seluruh dunia, dari peristiwa tersebut penulis melihat bahwa perlu dirumuskan suatu konsep kebijakan yang harus dapat mengantisipasi dampak buruk yang ditimbulkan *cyberpolitcs* yang terjadi di AS, dan peneliti melihat bahwa kebijakan

yang dirumuskan akan efektif dan efisien jika menggunakan teknologi AI.

tulisan ini menggunakan metode studi pustaka dimana menurut M.Nazir dalam bukunya yang berjudul 'Metode Penelitian' mengemukakan bahwa yang dimaksud dengan: "Studi kepustakaan adalah teknik pengumpulan data dengan mengadakan studi penelaahan terhadap buku-buku, literatur-literatur, catatan-catatan, dan laporan-laporan yang ada hubungannya dengan masalah yang dipecahkan (Nazir,1988: 111). Peneliti menelusuri *cyberwar* pada pemilihan presiden AS yang terjadi pada tahun 2016 dan juga literatur tentang pemanfaatan AI.

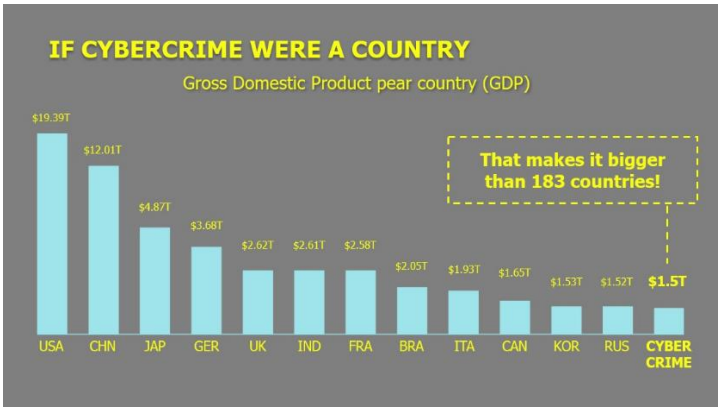
Teori yang digunakan pada tulisan ini dalam merumuskan konsep kebijakan pemanfaatan AI untuk kepentingan pertahanan dan keamanan untuk menghadapi dampak *cyberpolitics* adalah menurut William Dunn, adapun tahap-tahap kebijakan publik menurut William Dunn (1989), Penyusunan Agenda, Formulasi kebijakan, Adopsi/ Legitimasi Kebijakan, Penilaian/ Evaluasi Kebijakan.

Dinamika *cyber* dan *Cyberpolitics*

Cyberpolitics tidak dapat dipisahkan dari dinamika *cyber* yang terjadi baik internal suaru negara maupun dinamika yang berkembang diseluruh dunia. Dunia *cyber* memiliki keunikan tersendiri karena tidak memiliki batas antara negara. Siapapun dapat melakukan akses dari mana saja. Kemajuan teknologi dalam dunia *cyber* dalam satu sisi memberikan dampak yang luar biasa ubtuk dapar mencapai tujuan secara cepat, efektif dan efien. Dunia *cyber* juga memiliki dampak negatif yang juga harus dihadapi karena dapat menimbukan kerugian dan bahaya lain.

Tabel di bawah ini menunjukkan bagaimana *cybercrime* yang terjadi dibeberapa negara.

Tabel 1. Cybercrime di beberapa negara



Sumber: Parama, 2021

Cybercrime menjadi kian tumbuh selama pandemic Covid-19 . Pandemi COVID-19 telah terbukti sangat menguntungkan bagi penjahat karena selama pandemic telah membuka celah lebar dalam struktur keamanan perusahaan kecil dan besar. Pakar keamanan di seluruh dunia telah dengan panik bekerja menambal lubang menganga besar dalam keamanan yang baru-baru ini muncul karena jutaan laptop, tablet, dan ponsel yang sekarang bekerja dari rumah (seringkali, di jaringan yang tidak terlindungi yang tidak berada dibelakang banyak lapisan keamanan). Peningkatan dramatis jutaan perangkat yang tidak terlindungi yang bekerja dari kantor rumahan ini telah menyebabkan peningkatan luar biasa dalam kejahatan dunia maya. Jaringan korporat yang dibentengi oleh system pengamanan, sekarang telah dilubangi dan siap diserang. Pakar keamanan mengetahui hal ini dan begitu juga para penjahat. Rumah sakit, instansi pemerintah dan perusahaan besar semuanya menjadi rentan (PARAMA, 2021).

Analisis dari para ahli menyebutkan bahwa kemunkinan-kemungkinan yang akan terjadi ke depan adalah sebagai berikut:

1. Kejahatan dunia maya akan meningkat, khususnya di bidang *crypto-malware*.

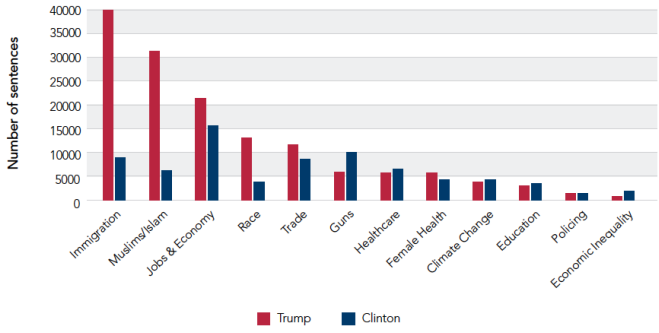
2. Target yang lebih besar dengan kantong yang lebih dalam akan dibidik. Ini kemungkinan akan mencakup sekolah-sekolah besar, perusahaan, rumah sakit dan kantor-kantor pemerintah. Apa pun yang berhubungan dengan bidang medis akan menjadi target utama.
3. Tuntutan tebusan akan naik. Penjahat tahu bahwa data menjadi lebih berharga dan akan mengenakan biaya yang sesuai. Berharap untuk melihat tuntutan jutaan dolar yang harus dibayar (terutama untuk target yang lebih besar seperti lembaga dan instansi pemerintah).
4. Kantor dan perusahaan yang lebih kecil akan digunakan sebagai landasan untuk mencapai target yang lebih tinggi. Penjahat akan menunggu di jaringan target yang lebih kecil dan mengumpulkan informasi tentang klien yang lebih besar yang mungkin mereka hadapi. Perusahaan yang lebih kecil akan menjadi titik masuk ke bisnis yang lebih besar dan lebih menguntungkan.
5. Perangkat lunak sebagai platform layanan akan terus diserang. Jangan salah mengira bahwa Office365 atau G-Suite dilindungi sepenuhnya. Penjahat telah menyusup ke platform ini melalui alat *phishing* dan *crypto-malware* dan telah mengunci klien dari data mereka sendiri.

Crberpolitics dengan mengambil contoh studi kasus pemilihan Presiden Amerika Serikat tahun 2016, menunjukkan suatu kejadian fenomena dalam dunia digital atau dunia *cyber*. Hasil Pemilihan Presiden 2016 akan tercatat sebagai salah satu momen paling tak terlupakan dalam sejarah AS. Terlepas dari sisi spektrum politik mana orang Amerika berada, kemenangan Presiden Trump mengejutkan jutaan warga di seluruh negeri. Baik reaksi positif maupun negatif membanjiri Internet, ketika para sarjana dan pakar politik berusaha memahami bagaimana jajak pendapat yang memprediksi kemenangan Hillary Clinton bisa menjadi sangat salah. Bagi warga yang tidak bersemangat membagikan tanggapan mereka secara *online*, mereka berada di luar diskusi politik yang intens. Itu bukan karena mereka tidak

memiliki suara pendapat, tetapi karena mereka tidak memiliki alat digital untuk melakukannya. Lebih dari 40 juta orang Amerika diperkirakan tidak memiliki akses ke Internet pada tahun 2016, menghalangi mereka untuk tidak hanya terlibat dalam diskusi politik online, tetapi juga dari melamar pekerjaan, mendapatkan pendidikan, mendapatkan akses ke layanan dasar pemerintah, dan tetap mendapat informasi. *Cyberpolitics* implementasinya juga harus memperhatikan dampak sosial dari kesenjangan digital, yang merupakan perbedaan yang ada antara "memiliki" versus "tidak" orang dengan akses ke Internet. Dalam upaya untuk mempelajari kesenjangan digital di AS secara khusus, tesis ini akan fokus pada membandingkan tingkat akses Internet dengan hasil pemungutan suara Pemilihan Presiden 2008, 2012, dan 2016 oleh country AS (Storli, 2018).

Cyberpolitics pada pemilihan Presiden Amerika Serikat bisa menjadi gambaran bagaimana pemanfaatan teknolgy cyber digunakan semaksimal mungkin dalam dunia politik. Tabel di bawah ini menunjukkan bagaimana aktivitas *cyberpolitics* terkait konten perdebatan poltik dengan berbagai tema dilakukan oleh masyarakat Amerika Serikat:

Tabel 2. *Number of sentences by substantive topic and candidate from media on the open web*

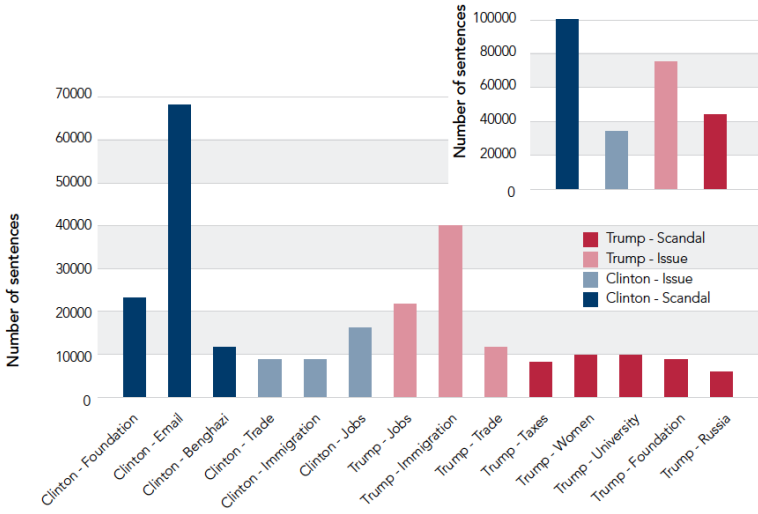


Sumber: (Rob Faris, 2017)

Data tabel di atas menunukkan menganalisis liputan media arus utama dan media sosial tentang pemilihan presiden

Amerika Serikat 2016. Doumentasi data di atas menunjukkan bahwa sebagian besar liputan media arus utama negatif untuk kedua kandidat, tetapi sebagian besar mengikuti agenda Donald Trump: ketika melaporkan tentang Hillary Clinton, liputan terutama berfokus pada berbagai skandal yang terkait dengan Clinton Foundation dan email. Ketika difokuskan pada Trump, masalah substantif utama, terutama imigrasi, sangat menonjol. Memang, imigrasi muncul sebagai isu sentral dalam kampanye dan menjadi isu yang menentukan untuk kampanye Trump.

Tabel 3. *Number of sentences by topic and candidate from May 1, 2015, to November 7, 2016*



Sumber: (Rob Faris, 2017)

Data menunjukkan bahwa struktur dan komposisi media di kanan dan kiri sangat berbeda. Media terkemuka di kanan dan kiri berakar pada tradisi dan praktik jurnalistik yang berbeda. Di sisi konservatif, lebih banyak perhatian diberikan kepada media yang pro-Trump dan sangat partisan. Di sisi liberal, sebaliknya, pusat gravitasi sebagian besar terdiri dari organisasi media lama yang mendalami tradisi dan praktik jurnalisme objektif.

Disinformasi dan propaganda berakar pada keberpihakan dan lebih lazim di media sosial.. Bentuk disinformasi yang paling jelas paling umum di media sosial dan di pinggiran lanskap media yang paling partisan. Popularitas yang lebih besar di media sosial daripada perhatian dari rekan-rekan media merupakan indikator kuat dari pelaporan yang partisan dan, dalam beberapa kasus, meragukan.

Di antara 100 sumber media teratas berdasarkan tautan atau pembagian media sosial, tujuh sumber, semuanya dari partisan kanan atau kiri partisan, menerima perhatian yang jauh lebih besar di media sosial daripada tautan dari outlet media lainnya. Situs-situs ini tidak semuanya terlibat dalam pelaporan yang menyesatkan atau salah, tetapi mereka jelas sangat partisan. Di grup ini, Gateway Pundit berada di kelasnya sendiri, yang dikenal karena "menerbitkan kebohongan dan menyebarkan hoax."

Popularitas yang tidak proporsional di Facebook adalah indikator kuat dari media yang sangat partisan dan tidak dapat diandalkan. Seperangkat situs web yang berbeda menerima perhatian yang tidak proporsional dari Facebook dibandingkan dengan Twitter dan tautan media. Dari daftar media yang paling menonjol, 13 situs masuk dalam kategori ini. Banyak dari situs-situs ini dikutip oleh sumber-sumber independen dan pelaporan media sebagai nenek moyang dari pelaporan yang tidak akurat jika tidak terang-terangan salah. Baik dalam bentuk maupun substansi, sebagian besar situs ini dengan tepat digambarkan sebagai clickbait politik. Sekali lagi, ini tidak menyiratkan kesetaraan di seluruh situs ini. Mengakhiri *The Fed* sering disebut sebagai contoh prototipikal dari sumber media yang menerbitkan cerita palsu. *The Onion* adalah *outlier* dalam kelompok ini, karena secara eksplisit satir dan ironis, daripada, seperti halnya dengan yang lain, terlibat dalam pelaporan yang sangat partisan dan meragukan tanpa ironi eksplisit..

Kerentanan asimetris: Kanan dan kiri menjadi sasaran manipulasi media dengan cara yang berbeda. Ekosistem media

sayap kanan yang lebih terisolasi rentan terhadap propaganda jaringan dan disinformasi yang berkelanjutan, terutama klaim negatif yang menyesatkan tentang Hillary Clinton. Mekanisme akuntabilitas media tradisional-misalnya, situs pengecekan fakta, kelompok pengawas media, dan kritik lintas media tampaknya hanya memiliki sedikit pengaruh pada lingkup media konservatif yang picik. Klaim yang ditujukan untuk konsumsi "internal" dalam ekosistem media sayap kanan lebih ekstrem, kurang koheren secara internal, dan lebih menarik bagi "gaya paranoid" politik Amerika daripada klaim yang dimaksudkan untuk memengaruhi pelaporan media arus utama.

Komitmen institusional terhadap ketidakberpihakan sumber-sumber media pada inti perhatian di sebelah kiri berarti bahwa sumber-sumber yang hiperpartisan dan tidak dapat diandalkan di sebelah kiri tidak menerima penguatan yang sama seperti yang dilakukan oleh situs-situs yang setara di sebelah kanan.

Praktik jurnalistik standar yang sama ini berhasil dimanipulasi oleh media dan aktivis hak untuk menyuntikkan narasi anti-Clinton ke dalam narasi media arus utama. Contoh utama adalah penggunaan email Komite Nasional Demokrat yang bocor dan email ketua kampanyenya John Podesta, yang dirilis melalui Wikileaks, dan serangkaian cerita berkelanjutan yang ditulis seputar tuduhan penjajakan pengaruh berbasis email. Contoh lain adalah rilis buku dan film Clinton Cash bersama dengan kampanye berkelanjutan yang mengikutinya, menjadikan Clinton Foundation sebagai kisah utama pasca-konvensi. Dengan mengembangkan narasi dan dokumentasi yang masuk akal yang rentan terhadap liputan negatif, sejajar dengan garis narasi yang lebih paranoid yang ditujukan untuk konsumsi internal dalam ekosistem media sayap kanan, dan dengan "bekerja sebagai referensi," menuntut liputan arus utama dari cerita anti-Clinton, sayap kanan media memainkan peran kunci dalam menetapkan agenda mainstream, media kiri-

tengah. Kami mendokumentasikan dinamika ini di bagian studi kasus Yayasan Clinton dari laporan ini.

Perumusan Kebijakan *Cyberpolitics*

Penjelesan dalam pendahuluan menunjukkan fakta bahwa *cyberpolitics* yang terjadi pada peristiwa pemilihan Presiden AS pada tahun 2016 memiliki dampak negatif, baik dari sisi dalam negri AS maupun juga merambah ke negara lain. Untuk itu dipadang perlu untuk mengantisipasi cyberpolitcs di Indonesia dengan memanfaatkan teknologi AI yang diharapkan dapat efektif dan efisien mengadapi segala dampak buruk yang memungkinkan akan terjadi. Adapun Langkah perumusan kebijakan tersebut adalah sebagai berikut:

Penyusunan Agenda

Agenda setting yaitu sebuah fase dan proses yang sangat strategis dalam realitas kebijakan publik. Penyelenggaraan Pilpres AS sebagai fakta bahwa Indonesia harus waspada terhadap bahaya yang mengancam stabilitas pertahanan dan kemanan. Dalam proses agenda seting inilah mempunyai ruang untuk memaknai apa yang dinamakan sebagai masalah publik dan prioritas dalam agenda publik dipertarungkan. Bila sebuah isu sukses mendapatkan status sebagai masalah public seperti urgensi kebijakan untuk mengatur masalah terkait cyberpolitcs, dan mendapatkan prioritas dalam agenda publik, karenanya isu tersebut berhak mendapatkan alokasi sumber daya publik yang diprioritaskan daripada isu lain.

Dalam agenda setting juga sangat penting untuk menentukan suatu isu publik yang akan diangkat dalam suatu agenda pemerintah. Issue kebijakan *(policy issues)* sering dinamakan juga sebagai masalah kebijakan *(policy problem). Policy issues* kebanyakan muncul karena telah terjadi silang pendapat di sela para aktor mengenai arah tindakan yang telah atau akan ditempuh, atau pertentangan pandangan mengenai karakter permasalahan tersebut. Menurut William Dunn (1989), isu kebijakan adalah produk atau fungsi dari demikianlah

keadaanya perdebatan patut tentang ciri utama, rincian, penjelasan maupun penilaian atas suatu masalah tertentu. Namun tidak semua isu dapat masuk menjadi suatu agenda kebijakan.

Policy issues tentang cyberpolitics ini sudah secara faktual terbukti berbahaya untuk stabilitas pertahanan dan kemanan sehingga sangat layak untuk dinaikkan ketaraf formulasi kebijakan.

Formulasi kebijakan cyberpolitics

Policy issues cyberpolitics jika sudah masuk dalam agenda kebijakan kemudian dibahas oleh para pembuat kebijakan. Masalah-masalah *cyberpolitics isuues* tadi diartikan untuk kemudian dicari pemecahan masalah yang terbaik. Pemecahan masalah tersebut berasal dari beragam alternatif atau pilihan kebijakan yang telah tersedia. Sama halnya dengan perjuangan suatu masalah untuk masuk dalam agenda kebijakan, dalam tahap perumusan kebijakan masing-masing alternatif bersaingan untuk dapat dipilih sebagai kebijakan yang diambil untuk memecahkan masalah (Winarno, 2008).

Adopsi/ Legitimasi Kebijakan cyberpolitics

Policy issues cyberpolitics jika sudah malalui tahap formulasi kebijakan, selanjutnya Langkah legimitasi, dengan tujuan legitimasi yaitu untuk memberikan otorisasi pada proses dasar pemerintahan. Bila tindakan legitimasi dalam suatu masyarakat diatur oleh kedaulatan rakyat, warga negara akan mengikuti arahan pemerintah (Winarno, 2008).Namun warga negara harus percaya bahwa tindakan pemerintah yang sah mendukung.

Dukungan untuk rezim cenderung berdifusi - cadangan dari sikap patut dan niat patut terhadap tindakan pemerintah yang menolong bagian mentolerir pemerintahan disonansi.Legitimasi dapat diurus melewati manipulasi simbol-simbol tertentu. Di mana melewati proses ini orang berupaya bisa untuk mendukung pemerintah (Winarno, 2008).

Penilaian/ Evaluasi Kebijakan cyberpolitics

Setelah formulasi kebijakan terkait penanganan *cyber-politics* sah atau sudah ada legitimasi, maka kebijakan tersebut sudah bisa dilaksanakan, namun kebijakan ini seringkali mendapat prokontra karena sebagaian orang menganggap bisa menjadi alat pemerintah untuk membatasi kebebasan pendapat, atau rawan digunakan pihak yang berkuasa untuk dijadikan alat politik dalam menghadapi kompetitornya (Nugroho, 2010).

Setelah kebijakan penanganan *cyberpolics* dimplementa-sikan maka tahap selanjutnya adalah tahap evaluasi dimana Secara umum evaluasi kebijakan dapat diceritakan sebagai agenda yang menyangkut estimasi atau penilaian kebijakan yang mencakup substansi, implementasi dan dampak dari kebijakan tentang *cyberpolitics.*

Dalam hal ini, evaluasi dipandang sebagai suatu agenda fungsional. Artinya, evaluasi kebijakan tidak hanya dilakukan pada tahap kesudahan saja, melainkan dilakukan dalam seluruh proses kebijakan. Dengan demikian, evaluasi kebijakan dapat mencakup tahap perumusan masalah-masalah kebijakan, pro-gram-program yang diusulkan untuk menyelesaikan masalah kebijakan, implementasi, maupun tahap dampak kebijakan. (Winarno, 2008).

Penggunaan AI untuk Mengantisipasi Dampak Negatif *Cyberpolitics*

Di Indonesia sendiri, laporan Badan Siber dan Sandi Negara (BSSN) pada 2018 mengungkapkan bahwa Indonesia menda-patkan lebih dari 12,9 juta *cyberattack* setiap tahunnya (Yasmine, 2021) Pada Pilpres AS 2016, bisa dibayangkan bagaimana arus *cyberattack* yang terjadi terkait kontestansi para calon presiden. Hal ini juga bisa saja terjadi di Indonesia, yang bisa mempengaruhi kondisi situasi pertahanan dan kemanan Indonesia. Arus informasi yang begitu masiv tentunya tidak mungkin dihadapi dengan hanya menggunakan metoide konvensional saja, yang mengandalkan manusia, pemilihan

teknologi AI adalah salah satu alternatif terbaik dalam penanganan *cyberpolitics.*

Kurangnya sumber daya manusia serta minimnya sampel terkait jenis dan tipe serangan *cyberattack* membuat proses *screening* menjadi lebih lama. Terlebih, saat ini peretas juga mulai menggunakan teknologi *artificial intelligence* (AI). Misalnya saja, pada serangan berbasis *email phising (spear phishing).* Berita-berita hoax melalui media sosial, yang berpotensi membahayakan persatuan dan kesatuan bangsa, yang memecah belah masyarakat dengan muatan kebencian satu sama lain.

Network Penanganan *Cyberpolitics*

Cyberpolitics sangat dekat dengan Tindakan *cybercrime*, dalam *cyberpolitics* seperti pada peristiwa Pilpres AS 2016, terdapat banyak berita-berita hoax yang mempengaruhi kondisi perekonomian AS dan juga merambat ke negara lainnya, Entitas yang menangani masalah cyber seperti di Indonesia dilaksanakan oleh beberap instituasi diantaranya adalah pihak kepolisian, TNI maupun Badan Siber dan Sandi Negara (BSSN), hamper setiap kementrian dan Lembaga juga memeiliki unit yang menangani masalah cyber. Kasih Prihantoro (2016) megatakan bahwa jaringan kerja ini sangat mempengaruhi efetifitas implementasi sebuah kebijakan sehingga perlu digunakan jaringan yang dapat menjami efektifitas dan efisiensi implementasi sebuah kebijkan.

Driver Force Cyberpolitics

Analisis dan pembahasan sebelumnya menunjukkan bahwa ancaman nyata dampak cyberpolitics sangat nyata, dan penggunaan AI sangat urgent untuk dilaksanakan, setelah perlu membangun jaringan yang efektif dan efisien, Kasih Prihantoro (2016) juga mengatakan bahwa diperlukan *driver force* untuk mengendalikan semua aktivitas implementasi sebuah kebijakan,

Entitas yang menangani masalah *cyber* di Indonesia beragam, dalam implementasi penganangan *cyberpolitics* diperlukan satu entitas sebagai *driver force,* sehingga ada satu komando agar penenganan *cyberpolitics* dapat dilaksanakan secara efektif dan efisien. Menghindari Tindakan-tindakan yang tidak perlu yang dapat menimbulkan efek lainnya.

Kesimpulan

Cyberpolitics sebagai salah satu dampak perkembangan teknology *cyber* memiliki dampak positif yang memungkinkan bidang politik dapat terselenggara dengan efektif dan efisien dengan prasyarat bahwa *cyberpolitics* dapat terjamin penyelenggaraannya. Untuk itu dalam mengantisipasi dampak negatifnya perlu segera dirumuskan kebijakan untuk penyelenggaraan dapat dioptimalkan manfaat positifnya agar Indonesia dapat lebih maju.

Rekomendasi dalam artikel ini adalah perumusan kebijakan penanganan *cyberpolitics* harus dibangun melalui network yang efektif dan efisien dan pembentukan *driver force* sebagai pengendali terpusat.

Daftar Rujukan

Budi Winarno (2008), Kebijakan Publik: teori dan Proses. Jakarta: PT Buku Kita. Hlm 33.

Indrastiti, N. (2016). *investasi*. Retrieved from investasi kontan.com:https://investasi.kontan.co.id/news/menghitung-dampak-pemilihan-presiden-as

Kasih Prihantoro Zakariya, Lukman Yudho Prakoso, Ratna Damayanti, A. D. (2019). Public Policy Analysis of Defense Areas and Defense Area Plan In Grati Pasuruan. The 3th Indonesia International Defense Sciense Seminar, 2(Universitas Pertahanan), 483–490.

Moh. Nazir. 1988. Metodologi Penelitian. Jakarta: Ghalia Indonesia.

Nugroho, A. S. (2010). Perlindungan kebebasan berpendapat melalui media internet dalam Undang-Undang No. 11 Tahun 2008 tentang informasi dan transaksi elektronik ditinjau dari perspektif hak asasi manusia. *core.ac.uk*, 1.

PARAMA, P. S. (2021, May 27). Retrieved from softindo.co.id: http://softindo.co.id/cybercrime-in-2021/

Rob Faris, H. R. (2017, August 16). *Publication*. Retrieved from The Berkman Klein Center for Internet & Society at Harvard University: https://cyber.harvard.edu/publications/2017/08/mediacloud

Storli, E. (2018, 5). Digitally United We Stand, Divided We Fall: How Does the Digital Divide Influence the Way Americans Vote? p. 1.

Undang-Undang No. 11 Tahun 2008 tentang informasi dan transaksi elektronik

William Dunn. Pengantar Analisis Kebijakan Publik, 1998, Yogyakarta: Gadjah Mada University Press. Hal: 24

Yasmine, F. (2021). *Advertorial*. Retrieved from INFOKOMPUTER: https://infokomputer.grid.id/read/122745022/semakin-canggih-deteksi-serangan-siber-perlu-bantuan-teknologi-ai?page=all