PUBLISITAS
Journal of Social Sciences and Politics

Vol. 10 No. 1 Oktober 2023
p-ISSN : 2252-4150
e-ISSN : 2716-3474
Tersedia *online* di http://ejurnal.stisipolcandradimuka.ac.id/index.php/JurnalPublisitas/

Memikirkan Kembali Kebijakan Pertahanan di Era Peperangan Siber

Aris Sarjito
Program Studi Manajemen Pertahanan, Fakultas Manajemen Pertahanan, Universitas Pertahanan Republik Indonesia -Jl. Salemba Raya No. 3, Jakarta 10440
E-mail: arissarjito@gmail.com

ABSTRAK

Evolusi teknologi dan meningkatnya ketergantungan pada internet dan infrastruktur digital telah melahirkan ancaman baru bagi keamanan nasional - perang dunia maya. Tidak seperti perang tradisional, perang dunia maya menghadirkan tantangan unik bagi negara-negara, menjadikannya isu mendesak bagi kebijakan pertahanan negara-negara di seluruh dunia.Tujuan dari penelitian kualitatif ini adalah untuk mengkaji tantangan unik yang ditimbulkan oleh perang dunia maya dan perbedaannya dari bentuk perang tradisional. Penelitian ini akan mengidentifikasi cara-cara di mana kebijakan pertahanan dapat diadaptasi untuk menanggapi ancaman dunia maya secara efektif, dan personel serta keahlian apa yang diperlukan untuk mengatasi tantangan-tantangan ini. Penelitian ini memanfaatkan pengumpulan data sekunder melalui jurnal akademik, laporan pemerintah, dan sumber-sumber terkemuka lainnya untuk memberikan wawasan tentang keadaan keamanan siber dan kebijakan pertahanan saat ini di seluruh dunia. Temuan ini akan menyoroti tantangan unik perang dunia maya, termasuk sifat serangan yang asimetris, kesulitan dalam pemantauan dan atribusi serangan, dan kurangnya norma internasional untuk aktivitas dunia maya. Riset ini menekankan perlunya pemikiran ulang kebijakan pertahanan di era perang siber dan perlunya perubahan paradigma dalam pendekatan terhadap ancaman siber. Penelitian ini merekomendasikan pengembangan strategi pertahanan multidimensi yang komprehensif dengan memanfaatkan teknologi canggih untuk deteksi, pencegahan, dan respons. Temuan ini juga menyoroti kebutuhan untuk berinvestasi pada personel dengan keterampilan teknis dan analitis untuk menduduki posisi penting dalam struktur pertahanan dunia maya.

Kata Kunci: kebijakan pertahanan, pelatihan personel, perang siber

ABSTRACT

The evolution of technology and the increased reliance on the internet and digital infrastructure have given birth to a new threat to national security- cyber warfare. Unlike traditional warfare, cyber warfare poses unique challenges for nations, making it a pressing issue for the defense policies of countries across the globe. The aim of this qualitative research is to examine the unique challenges posed by cyber warfare and how they differ from traditional forms of warfare. The research will identify the ways in which defense policies can be adapted to effectively respond to cyber threats, and what personnel and skill sets are needed to overcome these challenges. The research will also explore methods of developing and training personnel to effectively respond to cyber threats. This research will utilize secondary data collection through academic journals, government reports, and other reputable sources to provide insight into the current state of cybersecurity and defense policies across the globe. The findings will highlight the

unique challenges of cyber warfare, including the asymmetrical nature of the attacks, difficulty in monitoring and attribution of attacks, and the lack of international norms for cyber activities. The research emphasizes the need for rethinking defense policy in the era of cyber warfare and the need for a paradigm shift in the approach toward cyber threats. The research recommends the development of comprehensive, multi-dimensional defense strategies making use of advanced technologies for detection, prevention, and response. The findings also highlight the need for investing in personnel with technical and analytical skillsets to man critical positions in the cyber defense structure.

Keywords: *Cyber Warfare, Defense Policy, Personnel, Skill sets, Training*

1. PENDAHULUAN

Kebijakan pertahanan di era perang siber sangat penting untuk keamanan nasional. Dengan meningkatnya penggunaan teknologi di semua aspek masyarakat, serangan dunia maya telah menjadi ancaman serius yang dapat berdampak buruk bagi negara dan warganya. Kebijakan pertahanan yang kuat diperlukan untuk melindungi infrastruktur kritis, seperti jaringan listrik dan jaringan komunikasi, dari serangan dunia maya yang dapat mengganggu seluruh wilayah dan menyebabkan kerusakan ekonomi [2].

Selain itu, perang dunia maya tidak terbatas pada target pemerintah dan militer, tetapi juga dapat memengaruhi warga sipil, bisnis, dan infrastruktur penting di sektor swasta[19]. Penjahat dunia maya dapat mencuri informasi sensitif dan menggunakannya untuk keuntungan finansial atau untuk memeras individu atau organisasi. Oleh karena itu, diperlukan kebijakan pertahanan yang komprehensif untuk mengatasi sifat beragam ancaman dunia maya.

Selain itu, konsekuensi dari serangan dunia maya yang berhasil dapat menjadi bencana besar, yang menyebabkan hilangnya nyawa dalam kasus yang ekstrim[14]. Oleh karena itu, pemerintah dan organisasi perlu berinvestasi dalam keamanan siber dan terus memperbarui kebijakan pertahanan mereka untuk mengimbangi ancaman yang muncul.

Pernyataan Masalah dan Pertanyaan Penelitian

Meningkatnya prevalensi dan kecanggihan serangan dunia maya menimbulkan ancaman yang signifikan terhadap keamanan nasional, dan pemerintah di seluruh dunia berebut untuk mengembangkan kebijakan pertahanan yang efektif. Amerika Serikat, khususnya, telah berjuang untuk mengimbangi ancaman yang berkembang pesat ini dan telah lengah oleh beberapa serangan dunia maya tingkat tinggi dalam beberapa tahun terakhir, termasuk serangan terhadap Kantor Manajemen Personalia di mana jutaan personel sensitif file dicuri[46]. Perusahaan besar, seperti *Equifax*, juga mengalami pelanggaran data signifikan yang mengakibatkan informasi pribadi jutaan orang Amerika terungkap[13]. Insiden-insiden ini menyoroti perlunya pendekatan baru terhadap kebijakan pertahanan yang mempertimbangkan tantangan unik yang ditimbulkan oleh perang dunia maya.

Pernyataan masalah

Meskipun ancaman serangan dunia maya telah dikenali selama beberapa waktu, banyak kebijakan pertahanan masih berfokus terutama pada bentuk peperangan yang lebih tradisional, seperti operasi militer konvensional. Ini telah meninggalkan celah yang signifikan dalam kemampuan kita untuk secara efektif menanggapi ancaman dunia maya, yang dapat dilakukan oleh aktor non-negara, sulit untuk dikaitkan, dan dapat menimbulkan konsekuensi yang menghancurkan. Selain itu, sifat perang dunia maya membutuhkan keahlian dan keahlian yang berbeda dari operasi militer tradisional, yang menyebabkan kekurangan personel yang berkualifikasi [38]. Akibatnya, banyak lembaga pemerintah dan perusahaan swasta berjuang untuk mengembangkan strategi pertahanan yang efektif yang secara memadai mengatasi ancaman yang berkembang ini.

Pentingnya penelitian

Peperangan tidak sama dengan di masa lalu. Itu telah berubah bentuk dan menjadi lebih kompleks dan menantang daripada sebelumnya. Salah satu garis pertahanan baru yang muncul adalah perang siber. Saat ini, perang dunia maya telah menjadi ancaman nyata bagi negara-negara di seluruh dunia, dan penting untuk memikirkan kembali kebijakan pertahanan tradisional mengingat tantangan ini. Ada kebutuhan mendesak untuk mengembangkan pendekatan dan taktik baru untuk mempertahankan diri dari ancaman dunia maya, dan inilah yang membuat studi tentang memikirkan kembali kebijakan pertahanan di era perang dunia maya menjadi sangat penting.

Pentingnya penelitian ini dapat ditunjukkan melalui meningkatnya jumlah serangan siber dan potensi kerusakannya di era digital ini. Dalam sebuah survei terbaru yang dilakukan oleh Center for Strategic and International Studies (CSIS), ditemukan bahwa biaya kejahatan dunia maya tahunan telah mencapai $600 miliar USD (2018). Laporan yang sama juga mengungkapkan bahwa organisasi di seluruh dunia kehilangan $11,7 juta USD setiap tahun karena serangan dunia maya. Selain itu, serangan siber berpotensi mengganggu stabilitas keamanan nasional dan menimbulkan kekacauan yang lebih dari sekadar kerugian finansial, seperti peretasan pemilihan Presiden AS tahun 2016 oleh Rusia.

Oleh karena itu, sangat penting untuk menggabungkan langkah-langkah keamanan siber yang kuat dalam kebijakan pertahanan. Sangat penting tidak hanya untuk meningkatkan kemampuan sistem pertahanan yang ada terhadap serangan dunia maya tetapi juga untuk mempromosikan literasi dunia maya di antara personel yang terlibat dalam perencanaan pertahanan. Departemen Pertahanan AS menekankan perlunya "pendekatan seluruh pemerintah, seluruh masyarakat" untuk melawan meningkatnya ancaman serangan dunia maya [45].

Kesimpulannya, studi ini penting karena memberikan penilaian komprehensif tentang tantangan yang dihadapi negara-negara dalam mempertahankan diri dari ancaman siber. Temuannya dapat memandu pembuat kebijakan dalam

merancang kebijakan dan strategi pertahanan yang efektif untuk melawan serangan dunia maya, sehingga pada akhirnya menjaga keamanan dan stabilitas nasional.

2. TINJAUAN PUSTAKA

Fenomena perang dunia maya telah mendapat perhatian yang signifikan dalam beberapa tahun terakhir karena meningkatnya ketergantungan pemerintah, organisasi militer, bisnis, dan individu pada teknologi informasi. Perang dunia maya dapat didefinisikan sebagai "penggunaan teknologi komputer untuk mengacaukan, merusak, atau menghancurkan sistem atau jaringan komputer untuk tujuan politik atau militer" [28]. Ancaman yang ditimbulkan oleh perang dunia maya bermacam-macam, mulai dari gangguan hingga infrastruktur penting hingga pencurian informasi sensitif. Akibatnya, banyak pemerintah dan organisasi internasional menyadari perlunya langkah-langkah keamanan siber yang kuat untuk melindungi dari serangan siber.

Perang dunia maya dapat mengambil banyak bentuk, termasuk serangan denial-of-service, penyisipan malware, dan pembajakan server [3]. Demikian pula, Lewis (2014) berpendapat bahwa perang dunia maya ditandai dengan taktik siluman dan penipuannya [27].

Terlepas dari upaya untuk mendefinisikan perang dunia maya ini, masih ada perdebatan mengenai apakah itu merupakan bentuk peperangan baru yang fundamental atau apakah itu hanyalah perpanjangan dari operasi militer tradisional. Misalnya, Rid (2013) berpendapat bahwa meskipun baru [40], perang dunia maya tidak mewakili jenis konflik yang baru secara fundamental, karena tujuan dan strateginya pada dasarnya sama dengan perang konvensional. Sebaliknya, sarjana lain berpendapat bahwa kekhasan perang dunia maya – seperti kemudahan serangan dapat dilakukan secara anonim dan dari lokasi terpencil – membedakannya dari perang tradisional dan memerlukan pendekatan pertahanan yang berbeda [18].

Mengingat perdebatan ini, jelas bahwa pembuat kebijakan dan ahli pertahanan perlu memikirkan dengan hati-hati tentang tanggapan yang tepat terhadap ancaman perang dunia maya. Sementara kemampuan militer tradisional mungkin masih memiliki peran, ada pengakuan yang berkembang bahwa pertahanan dunia maya membutuhkan serangkaian keterampilan, teknologi, dan personel yang berbeda. Dengan demikian, pemikiran ulang kebijakan pertahanan diperlukan untuk secara efektif dan komprehensif mengatasi ancaman yang ditimbulkan oleh perang dunia maya.

Kesimpulannya, perang dunia maya adalah fenomena yang relatif baru yang mengancam akan mengganggu mode perang dan keamanan tradisional. Meskipun masih ada perdebatan tentang apa sebenarnya yang dimaksud dengan perang dunia maya, jelas bahwa pemerintah dan organisasi harus mengambil langkah-langkah untuk melindungi dari potensi ancamannya. Dengan demikian, pemikiran ulang kebijakan pertahanan – termasuk pengembangan teknologi dan personel baru untuk melawan serangan dunia

maya – diperlukan untuk melindungi dari ancaman yang muncul ini.

Saat dunia bergerak menuju digitalisasi dengan kemajuan di bidang teknologi, ada aspek perang paralel yang terkait dengan dunia maya. Sifat konflik telah berevolusi dan meluas menjadi apa yang sekarang dikenal sebagai perang siber. Melalui penelitian ini, evolusi perang siber akan dieksplorasi untuk memahami dampak dan transformasi perang konvensional di era digital. Ini adalah topik penting untuk mengeksplorasi kemungkinan risiko dan konsekuensi yang mungkin ditimbulkan oleh perang dunia maya di era saat ini.

Landasan internet memberi para pemimpin militer banyak peluang untuk mengembangkan kemampuan siber ofensif dan defensif. Salah satu laporan dari National Research Council berjudul "Computers at risk" meramalkan bahwa perang dunia maya akan menjadi topik penting di masa depan peperangan, karena jaringan ini rentan terhadap serangan berbahaya dari dunia luar [35].

Seiring kemajuan teknologi, semakin banyak negara mulai mengembangkan kemampuan siber ofensif dan defensif. Dalam dekade terakhir, kemampuan dunia maya aktor negara telah matang. Ini terbukti dengan meningkatnya jumlah serangan yang disponsori negara yang telah kita saksikan selama dekade terakhir. Pada tahun 2010, Stuxnet, sebuah worm komputer yang diyakini dibuat oleh AS dan Israel, digunakan untuk menargetkan fasilitas nuklir Iran [47]. Demikian pula, pada tahun 2014, peretas Rusia menargetkan jaringan listrik Ukraina, menghasilkan serangan dunia maya terbesar dalam sejarah [31].

Pemerintah menjadi semakin bergantung pada dunia maya untuk melakukan kegiatan sehari-hari mereka. Mengingat hal ini, kebutuhan untuk mengamankan ruang ini dan bertahan dari serangan telah menjadi kebutuhan. Di AS, Departemen Pertahanan telah membentuk Komando Siber untuk mengoordinasikan operasi siber. *Cyber Command* bertanggung jawab atas pengembangan strategi pertahanan dunia maya, kemampuan serangan dunia maya, triase serangan dunia maya, dan menanggapi insiden [45].

Kesimpulannya, perang dunia maya adalah ancaman yang muncul terhadap keamanan nasional dengan potensi kerusakan yang signifikan terhadap infrastruktur dan ekonomi. Negara-negara telah menyaksikan serangan dunia maya yang disponsori negara yang diyakini berasal dari negara-negara saingan. Evolusi peperangan telah dipengaruhi oleh kebangkitan dunia maya, dan kebutuhan untuk mengamankan ruang ini telah menjadi kebutuhan. Ketika pemerintah terus mengembangkan kemampuan dunia maya mereka, kebutuhan untuk memikirkan kembali kebijakan pertahanan nasional untuk mencerminkan lanskap ancaman yang terus berkembang menjadi semakin penting.

Munculnya perang siber sebagai domain baru peperangan telah mendorong para peneliti dan pembuat kebijakan untuk memikirkan kembali kebijakan pertahanan di era ancaman siber modern. Tinjauan literatur dari studi saat ini mengungkapkan pentingnya

perang dunia maya sebagai salah satu ancaman paling signifikan terhadap keamanan nasional di abad ke-21. Perang dunia maya mengacu pada penggunaan teknologi informasi untuk melakukan serangan terhadap sistem komputer, jaringan, dan infrastruktur kritis. Makalah ini menyajikan sintesis studi yang berfokus pada keadaan perang dunia maya saat ini dan tantangan yang terkait dengan perlindungan terhadap ancaman dunia maya.

Salah satu tantangan paling signifikan dalam konteks perang dunia maya adalah sulitnya mengidentifikasi sumber serangan. Sebagaimana dicatat oleh Brenner (2009), atribusi lebih sulit di dunia maya, membuatnya lebih menantang untuk bertahan dari serangan dunia maya[5]. Dengan meningkatnya penggunaan teknologi canggih, penyerang dunia maya dapat menutupi identitas dan lokasi mereka, sehingga sulit untuk melacak dan meminta pertanggungjawaban mereka atas tindakan mereka. Hal ini menunjukkan perlunya mengembangkan kemampuan pertahanan siber yang lebih kuat yang dapat menggagalkan ancaman siber secara efektif.

Tantangan lain terkait perang siber adalah meningkatnya kecanggihan serangan siber. Sebagaimana dicatat oleh Bollen (2011), penyerang dunia maya terus berinovasi dan mengembangkan taktik baru untuk menghindari mekanisme pertahanan dunia maya yang ada [4]. Penggunaan kecerdasan buatan dan algoritme pembelajaran mesin dalam serangan siber, misalnya, menimbulkan tantangan baru dalam konteks keamanan siber. Ini menyoroti kebutuhan untuk mengembangkan mekanisme pertahanan baru yang dapat mengidentifikasi dan merespons ancaman dunia maya yang muncul secara lebih efektif.

Perspektif kebijakan pertahanan, literatur mengungkapkan bahwa mekanisme pertahanan saat ini tidak memadai untuk mengatasi sifat ancaman dunia maya yang terus berkembang. Sebagaimana dicatat oleh Komisi Keamanan Siber untuk Kepresidenan ke-44 (2008), kerangka kebijakan pertahanan saat ini sudah usang dan perlu diperbarui untuk mengatasi sifat serangan siber yang terus berkembang. Hal ini menunjukkan perlunya memikirkan kembali kebijakan pertahanan dalam konteks perang siber [9].

Kajian literatur juga menyoroti perlunya kerja sama antar pemangku kepentingan dalam mengatasi tantangan yang terkait dengan perang siber. Sebagaimana dicatat oleh Healey (2010), kerjasama antara pemerintah, sektor swasta, dan masyarakat sipil sangat penting dalam mengembangkan mekanisme pertahanan yang efektif terhadap ancaman dunia maya [21]. Ini menggarisbawahi perlunya pendekatan yang lebih kolaboratif dan terintegrasi untuk mengatasi ancaman dunia maya.

Sebagai kesimpulan, tinjauan literatur menggarisbawahi pentingnya memahami keadaan perang dunia maya saat ini dan tantangan yang terkait dengan mempertahankannya. Tinjauan tersebut menyoroti kebutuhan untuk mengembangkan kemampuan pertahanan siber yang lebih kuat, memikirkan kembali kebijakan pertahanan, dan mendorong kerja sama di antara para pemangku kepentingan untuk mengatasi

ancaman siber yang muncul secara efektif.

Studi tentang Cyber Warfare dan Kebijakan Pertahanan

Perang siber telah menjadi ancaman signifikan bagi keamanan nasional. Saat penyerang dunia maya tumbuh lebih canggih dan gigih, penting bagi pemerintah untuk mengevaluasi kembali kebijakan pertahanan mereka untuk mengurangi kerentanan sistem keamanan dunia maya mereka. Tinjauan literatur ini akan memeriksa studi terbaru tentang perang dunia maya dan kebijakan pertahanan untuk memberikan wawasan tentang keadaan penelitian saat ini tentang masalah ini dan implikasi potensial untuk pengembangan kebijakan di masa depan.

Satu studi baru-baru ini tentang topik perang dunia maya dan kebijakan pertahanan menganalisis hubungan antara operasi dunia maya dan kegiatan militer tradisional. Dalam studi oleh Anderson et al. (2019), penulis berpendapat bahwa "operasi dunia maya hanyalah salah satu cara perang" dan karenanya harus diintegrasikan ke dalam proses perencanaan dan pelaksanaan militer tradisional (hal. 17) [1]. Hal ini menunjukkan bahwa pembuat kebijakan pertahanan perlu memikirkan kembali pendekatan mereka terhadap operasi siber dan memprioritaskan penyertaan pertimbangan keamanan siber dalam proses pengambilan keputusan mereka.

Studi lain oleh Gartzke dan Lindsay (2018) mengeksplorasi hubungan antara faktor ekonomi dan perang dunia maya [17]. Para penulis berpendapat bahwa manfaat ekonomi dari serangan dunia maya sering dilebih-lebihkan, dan perang dunia maya tidak mungkin menjadi strategi dominan bagi aktor negara karena biayanya yang tinggi dan peluang keberhasilan yang rendah. Ini menyoroti pentingnya memahami motivasi dan strategi aktor negara yang terlibat dalam perang dunia maya ketika mengembangkan kebijakan pertahanan. Selain itu, Soo Hoo dkk. (2019) mengkaji efektivitas kerjasama internasional dalam memitigasi ancaman perang siber [42]. Para penulis menemukan bahwa sementara kerja sama internasional diperlukan untuk pertahanan dunia maya, hal itu terhalang oleh konflik kepentingan nasional dan masalah kedaulatan. Hal ini menunjukkan bahwa pembuat kebijakan perlu mengejar pendekatan kolaboratif yang memprioritaskan kepentingan bersama dan mengatasi konflik yang mendasarinya.

Secara keseluruhan, studi ini menunjukkan bahwa kebijakan pertahanan harus berevolusi untuk mengatasi perubahan sifat perang dunia maya. Dimasukkannya pertimbangan keamanan dunia maya dalam perencanaan militer tradisional, memahami motivasi dan strategi aktor negara, dan mempromosikan kerja sama internasional merupakan komponen penting dari strategi pertahanan yang efektif. Ketika masyarakat semakin bergantung pada teknologi digital, penting bagi pembuat kebijakan untuk memprioritaskan pertahanan dunia maya sebagai pertimbangan keamanan nasional.

3. METODE PENELITIAN

Desain penelitian kualitatif adalah pendekatan yang digunakan untuk

menggali dan memahami fenomena yang kompleks. Menurut Creswell (2014), metode ini melibatkan pengumpulan data dengan mengamati dan mewawancarai individu dan menganalisis data untuk mengidentifikasi tema dan pola [11].

Peneliti dapat menggunakan data perang siber yang ada untuk mengidentifikasi tantangan dan peluang kebijakan pertahanan negara di era siber. Kesimpulannya, desain penelitian kualitatif dan metode pengumpulan data sekunder bermanfaat dalam memahami kebijakan pertahanan di era perang siber. Metode-metode ini memberi para peneliti kesempatan untuk mengeksplorasi kompleksitas dan nuansa materi pelajaran. Desain penelitian kualitatif memungkinkan peneliti untuk menyelidiki sikap, keyakinan, dan pengalaman individu dan kelompok sementara pengumpulan data sekunder memberi peneliti berbagai informasi yang dapat digunakan untuk mendukung temuan penelitian.

4. HASIL PENELITIAN DAN PEMBAHASAN

Maraknya perang siber telah menghadirkan tantangan baru dalam ranah kebijakan pertahanan negara. Perang siber adalah bentuk konflik yang melibatkan aksi permusuhan yang dilakukan melalui jaringan komputer [30]. Tantangan unik yang ditimbulkan oleh perang dunia maya berbeda secara signifikan dari bentuk peperangan tradisional.

Salah satu tantangan unik yang ditimbulkan oleh perang dunia maya adalah ambiguitas atribusi. Tidak seperti bentuk peperangan tradisional di mana pihak yang menyerang mudah diidentifikasi, serangan dunia maya dapat dilakukan oleh pelaku anonim. Akibatnya, tindakan pembalasan yang diambil oleh pemerintah berpotensi menargetkan pihak yang salah [37]. Tantangan lainnya adalah pesatnya laju teknologi di ranah siber. Peretas dan aktor jahat lainnya dapat dengan cepat beradaptasi dengan firewall dan tindakan enkripsi baru, menghadirkan tantangan tanpa akhir bagi mereka yang bertanggung jawab untuk bertahan melawan mereka [15].

Menanggapi ancaman dunia maya secara efektif, kebijakan pertahanan perlu disesuaikan. Salah satu strateginya adalah berinvestasi dalam modernisasi dan inovasi untuk membekali personel keamanan dengan alat terkini untuk mendeteksi dan mencegah serangan [24]. Selain itu, kerja sama yang lebih besar antara militer dan perusahaan teknologi swasta dapat meningkatkan mekanisme pertahanan [30].

Mengembangkan dan melatih personel untuk tanggapan yang efektif terhadap ancaman dunia maya, diperlukan berbagai keahlian. Keahlian teknis tentu saja penting untuk memahami kerentanan khusus dan alat yang diperlukan untuk pencegahan dan tanggapan. Namun, keterampilan yang lebih lembut seperti kemampuan beradaptasi, pemikiran kritis, dan komunikasi juga diperlukan. Personel harus dapat dengan cepat beradaptasi dengan teknologi baru dan tetap mengikuti tren dan ancaman terbaru [15]. Kesimpulannya, perang dunia maya menimbulkan tantangan unik yang membutuhkan adaptasi kebijakan dan

keahlian teknis. Tanggapan pertahanan yang berhasil akan membutuhkan investasi, inovasi, dan kerja sama antara berbagai entitas. Keahlian teknis, kemampuan beradaptasi, dan keterampilan berpikir kritis semuanya akan diperlukan oleh personel yang bertanggung jawab untuk mencegah dan merespons ancaman dunia maya.

Munculnya perang dunia maya telah menimbulkan tantangan unik bagi para pembuat kebijakan pertahanan, khususnya dalam hal cara menanggapi ancaman dunia maya secara efektif. Tidak seperti bentuk peperangan tradisional, serangan dunia maya menimbulkan ancaman signifikan terhadap infrastruktur kritis, ekonomi, sistem politik, dan keamanan nasional dengan mengeksploitasi kerentanan dalam jaringan digital dan sistem informasi. Menurut Rid, T. (2018), serangan ini dapat berdampak luas dan menghancurkan di berbagai sektor, termasuk namun tidak terbatas pada keuangan, kesehatan, utilitas publik, dan pertahanan [40]. Untuk menanggapi tantangan ini, kebijakan pertahanan perlu diadaptasi untuk mengatasi sifat ancaman dunia maya yang terus berkembang. Secara khusus, kebijakan harus menekankan perlindungan infrastruktur kritis dan pengembangan kemampuan untuk pertahanan aktif, yang mencakup pendeteksian dan penetralan ancaman sebelum dapat menyebabkan kerusakan [41]. Tanggapan yang efektif terhadap ancaman dunia maya juga membutuhkan personel yang memiliki keahlian khusus, termasuk keahlian dalam pengkodean, jaringan, enkripsi, dan analisis intelijen dunia maya [10]. Dalam kaitan ini, pelatihan dan pengembangan keterampilan yang berkelanjutan dapat mendukung kesiapan personel pertahanan untuk menghadapi dan memitigasi ancaman siber.

1. Tantangan unik yang ditimbulkan oleh perang dunia maya

Peperangan dunia maya menghadirkan serangkaian tantangan unik yang berbeda secara signifikan dari bentuk peperangan tradisional. Dengan meningkatnya ketergantungan pada teknologi dalam kehidupan kita sehari-hari, ancaman serangan siber menjadi isu yang semakin penting bagi para pembuat kebijakan pertahanan. Penelitian ini akan membahas tantangan unik yang ditimbulkan oleh perang dunia maya dan bagaimana perbedaannya dari bentuk perang tradisional dan akan menggunakan berbagai sumber untuk mendukung argumen yang dibuat.

Salah satu tantangan utama perang dunia maya adalah sulitnya atribusi. Bentuk peperangan tradisional seringkali melibatkan garis identifikasi yang jelas, dengan seragam dan bendera yang dapat dikenali. Sebaliknya, serangan dunia maya dapat diluncurkan dari jarak jauh, terkadang dari lokasi anonim, yang membuat sulit untuk mengidentifikasi penyerang atau lokasinya [7]. Ini menciptakan situasi di mana penyerang berpotensi melakukan serangan tanpa mendapat hukuman, tanpa takut akan pembalasan.

Tantangan besar lainnya yang ditimbulkan oleh perang dunia maya adalah kapasitasnya untuk eskalasi non-linier. Dalam peperangan tradisional, eskalasi cenderung terjadi secara linier, dengan masing-masing pihak

menanggapi tindakan pihak lain dalam urutan yang dapat diperkirakan sebelumnya. Namun, dalam kasus perang dunia maya, eskalasi dapat melonjak dengan cepat dari satu tingkat ke tingkat lainnya, sehingga sulit diprediksi dan dikendalikan [28]. Satu serangan dapat dengan cepat meningkat menjadi gangguan yang meluas atau bahkan kerusakan fisik, seperti yang ditunjukkan oleh serangan worm Stuxnet 2010 terhadap fasilitas nuklir Iran [47]. Ketidakpastian ini mempersulit pembela HAM untuk melakukan respons yang efektif.

Tantangan lain dari perang dunia maya adalah masalah kerusakan tambahan. Dalam perang tradisional, kerusakan tambahan adalah realitas operasi militer yang diakui, dengan penduduk sipil sering menderita kerugian yang tidak diinginkan selama konflik. Dalam kasus perang dunia maya, kerusakan tambahan dapat terjadi dalam bentuk konsekuensi yang tidak diinginkan dari serangan dunia maya, seperti terganggunya infrastruktur kritis atau sistem ekonomi [33]. Potensi konsekuensi yang tidak diinginkan dapat mempersulit penilaian risiko dan manfaat dari peluncuran serangan dunia maya.

Tantangan unik terakhir dari perang dunia maya adalah meningkatnya ancaman kecerdasan buatan. AI dan senjata otonom berpotensi mengubah wajah peperangan, memungkinkan serangan dilakukan secepat kilat dan dengan presisi yang belum pernah terjadi sebelumnya [23]. Hal ini akan membuat sangat sulit bagi pembela manusia untuk mengikutinya dan akan membutuhkan pendekatan baru terhadap kebijakan pertahanan agar tetap efektif.

Kesimpulannya, perang dunia maya menimbulkan serangkaian tantangan unik bagi pembuat kebijakan pertahanan. Tantangan-tantangan ini berbeda secara signifikan dari bentuk peperangan tradisional, terutama karena kesulitan atribusi, eskalasi non-linier, kerusakan tambahan, dan meningkatnya ancaman AI. Adalah kewajiban para pembuat kebijakan pertahanan untuk mengembangkan pendekatan dan strategi baru agar dapat mengatasi tantangan-tantangan ini secara efektif.

2. Menyesuaikan kebijakan pertahanan untuk merespons ancaman siber secara efektif

Kebijakan pertahanan merupakan aspek krusial dari keamanan nasional, melindungi negara dari berbagai ancaman, baik yang ada di ranah fisik maupun dunia maya. Namun, dalam beberapa tahun terakhir, ancaman dunia maya menjadi semakin kompleks dan berdampak, meningkatkan kebutuhan akan kebijakan pertahanan untuk beradaptasi dengan lanskap keamanan yang berubah. Esai ini berpendapat bahwa kebijakan pertahanan yang efektif harus menggabungkan pendekatan proaktif dan komprehensif yang membahas spektrum ancaman dunia maya. Untuk memulai, penting untuk memahami sifat ancaman dunia maya. Dalam artikel mereka, Kalathil dan Boas menjelaskan bahwa ancaman dunia maya "berkisar dari ancaman sederhana hingga telepon seluler hingga ancaman yang sangat rumit yang diatur oleh aktor tingkat negara bagian" [25]. Ancaman dunia maya dapat terjadi dalam berbagai

bentuk, antara lain serangan peretasan, malware, dan serangan denial of service (DDoS) terdistribusi. Ancaman ini dapat mengganggu infrastruktur penting, membahayakan data sensitif, dan membahayakan keamanan nasional, di antara konsekuensi lainnya.

Pendekatan seperti ini telah direkomendasikan oleh berbagai ahli [22] [32]. Healey (2010) menjelaskan bahwa pendekatan komprehensif harus mencakup "kerangka kerja manajemen risiko, berbagi informasi dan kolaborasi antara pemerintah dan industri, penerapan produk yang aman, dan berinvestasi dalam keahlian keamanan siber." (hal. 43) Mawn (2015) sependapat, menyatakan bahwa "pendekatan manajemen risiko memungkinkan organisasi untuk memprioritaskan risiko dan mengalokasikan sumber daya yang sesuai."

Dalam analisis mereka tentang efektivitas rencana tanggap insiden, Nissenbaum dan Shacham (2014) merekomendasikan beberapa komponen utama, termasuk protokol pelaporan yang jelas, spesifikasi prosedur eskalasi, dan evaluasi berkelanjutan serta peningkatan rencana [36].

Secara keseluruhan, esai ini berpendapat bahwa kebijakan pertahanan harus beradaptasi untuk menanggapi ancaman dunia maya secara efektif di era perang dunia maya kontemporer. Pendekatan proaktif dan komprehensif yang memperhitungkan spektrum ancaman, ditambah dengan rencana respons insiden yang efektif, dapat membantu memastikan keamanan nasional dalam menghadapi ancaman dunia maya yang terus berkembang.

3. Personel dan keahlian untuk menanggapi ancaman dunia maya

Maraknya ancaman dunia maya telah membawa perubahan signifikan dalam cara peperangan modern dilakukan. Strategi pertahanan tradisional dianggap tidak memadai dalam menghadapi ancaman dunia maya. Konsekuensinya, para pembuat kebijakan dihadapkan pada tantangan untuk memikirkan kembali kebijakan pertahanan untuk mengatasi ancaman yang muncul ini dengan lebih baik. Dalam hal ini, penting untuk mempertimbangkan personel dan rangkaian keterampilan yang diperlukan untuk merespons ancaman dunia maya secara efektif.

Pertama-tama, respons yang efektif terhadap ancaman dunia maya membutuhkan personel dengan pemahaman mendalam tentang sifat ancaman dunia maya dan pengetahuan teknis untuk mengatasinya. Sebagaimana dicatat oleh Park, Song, dan Lee (2021), ancaman dunia maya bersifat dinamis dan membutuhkan kewaspadaan terus-menerus untuk mengidentifikasi dan memitigasinya[39]. Oleh karena itu, personel dengan keahlian keamanan siber, seperti insinyur jaringan, analis ancaman, dan analis malware, sangat penting untuk strategi pertahanan siber yang efektif. Selain itu, personel dengan pengetahuan analisis forensik dapat membantu penyelidikan pascaserangan dan memungkinkan pihak berwenang untuk mengidentifikasi pelaku dan mengambil tindakan yang tepat.

Selain keterampilan teknis, respons yang efektif terhadap ancaman dunia maya membutuhkan personel dengan kemampuan pengambilan keputusan yang

baik, keterampilan komunikasi, dan kualitas kepemimpinan. Seperti yang ditunjukkan oleh Taylor (2020)[43], keputusan yang tepat waktu dan terinformasi dengan baik sangat penting dalam mengurangi risiko yang ditimbulkan oleh ancaman dunia maya. Selain itu, komunikasi yang efektif dengan pemangku kepentingan, baik internal maupun eksternal, dapat membantu mencegah serangan dan mengurangi akibatnya. Kepemimpinan yang kuat juga penting dalam mengatur nada untuk anggota tim lainnya dan memastikan bahwa semua upaya diselaraskan untuk mencapai hasil yang diinginkan.

Pelatihan dan pengembangan personel harus menjadi proses yang berkelanjutan untuk memastikan bahwa mereka mengikuti perubahan sifat ancaman dunia maya. Seperti yang disarankan oleh Kumar et al. (2018) [26], pelatihan ekstensif di berbagai bidang seperti forensik digital, pengujian penetrasi, perburuan ancaman, dan respons insiden dapat membekali personel dengan keterampilan yang diperlukan untuk mengidentifikasi dan mengatasi ancaman dunia maya yang muncul. Selain itu, pelatihan lintas fungsi dapat bermanfaat dalam meningkatkan komunikasi dan kolaborasi di antara tim khusus yang berbeda.

Menanggapi ancaman dunia maya secara efektif membutuhkan kombinasi keterampilan teknis, kemampuan pengambilan keputusan, komunikasi, dan kualitas kepemimpinan. Pembuat kebijakan yang bertugas memikirkan kembali kebijakan pertahanan di era perang siber harus memprioritaskan pengembangan dan pelatihan personel dengan keterampilan dan atribut yang disebutkan di atas. Pelatihan dan pengembangan berkelanjutan sangat penting untuk mengikuti sifat ancaman dunia maya yang terus berkembang.

5. KESIMPULAN DAN SARAN

KESIMPULAN

Peperangan dunia maya menimbulkan tantangan unik yang sangat berbeda dari bentuk peperangan tradisional. Riset kami menunjukkan bahwa tantangan ini mencakup kecepatan dan skala serangan yang dapat diluncurkan, kesulitan atribusi, dan potensi kerusakan tambahan pada infrastruktur penting. Selain itu, sifat multidimensi perang siber membuatnya sulit untuk dilawan dan memerlukan pemikiran ulang kebijakan pertahanan di era perang siber. Seperti dicatat oleh Gaetz et al. (2020) [16], penting untuk mengembangkan strategi yang memprioritaskan perlindungan infrastruktur kritis dan pencegahan serangan. Selain itu, inovasi dan kemajuan berkelanjutan diperlukan untuk memenuhi sifat ancaman dunia maya yang terus berkembang dan kebutuhan akan mekanisme pencegahan dan respons yang lebih efisien. Oleh karena itu, pembuat kebijakan dan ahli strategi militer harus mengalokasikan sumber daya yang memadai untuk memprioritaskan bidang kebijakan pertahanan yang kritis ini.

Mengatasi ancaman dunia maya memerlukan pendekatan multifaset yang mencakup personel dengan berbagai keahlian. Profesional dengan keahlian dalam keamanan jaringan, forensik

digital, manajemen risiko, dan respons insiden merupakan komponen penting dari strategi pertahanan dunia maya yang efektif [34]. Selain itu, pelatihan dan pengembangan berkelanjutan dari personel ini diperlukan untuk mengikuti lanskap dunia maya yang berkembang pesat[8]. Organisasi harus memprioritaskan dan berinvestasi dalam pendidikan karyawan dan mendorong program pembelajaran seumur hidup untuk memastikan staf mereka mempertahankan pengetahuan dan keterampilan terkini yang diperlukan untuk memerangi ancaman dunia maya secara efektif.

SARAN

Rekomendasi untuk Memikirkan Kembali Kebijakan Pertahanan di Era Peperangan Siber:

1. Peperangan dunia maya menghadirkan tantangan unik seperti kesulitan dalam atribusi, kecepatan dan anonimitas serangan, serta kemampuan untuk menargetkan infrastruktur penting. Oleh karena itu, kebijakan pertahanan perlu diadaptasi untuk mengatasi tantangan ini dan menekankan integrasi langkah-langkah teknis dan kebijakan.
2. Pemerintah harus berupaya mendorong lingkungan kerja sama antara entitas swasta dan badan intelijen untuk membantu mencegah dan menanggapi ancaman dunia maya. Ini termasuk mendorong industri untuk berbagi intelijen ancaman dan praktik terbaik sambil memastikan privasi dan keamanan nasional.
3. Diperlukan tenaga kerja keamanan siber khusus yang dapat merespons ancaman siber secara efektif. Ini membutuhkan investasi dalam pelatihan dan pengembangan personel yang berspesialisasi dalam keamanan siber dan memiliki pemahaman mendalam tentang lanskap ancaman yang berkembang.
4. Kebijakan pertahanan harus mengutamakan pengembangan teknologi baru dan kemitraan strategis untuk mendukung pertahanan terhadap ancaman siber. Ini termasuk berinvestasi dalam alat dan taktik baru untuk mengatasi ancaman dunia maya dan memanfaatkan kemitraan strategis dengan sekutu dan entitas swasta untuk meningkatkan kemampuan keamanan dunia maya.
5. Kolaborasi dan kemitraan dengan entitas internasional penting dalam mengatasi ancaman siber global. Pemerintah harus bekerja sama dengan organisasi internasional untuk mempromosikan kolaborasi dan strategi pertahanan kolektif melawan ancaman keamanan siber.
6. Untuk beradaptasi dengan ancaman dunia maya yang terus berkembang, kebijakan pertahanan harus menekankan pemantauan, analisis, dan evaluasi lanskap keamanan dunia maya secara terus-menerus. Ini termasuk memantau dan mengevaluasi teknologi, kebijakan, dan personel untuk memastikan bahwa kebijakan pertahanan terus diperbarui untuk mengatasi perubahan sifat ancaman dunia maya.

7. Sebagai kesimpulan, terbukti bahwa perang dunia maya menimbulkan tantangan unik yang berbeda dari bentuk peperangan tradisional, dan memerlukan pendekatan berbeda untuk pertahanan yang efektif. Dengan mengadaptasi kebijakan pertahanan untuk mengatasi tantangan unik ini, berinvestasi pada personel dan keahlian, mengembangkan teknologi baru, dan membina kemitraan, adalah mungkin untuk mengembangkan strategi pertahanan yang efektif melawan ancaman dunia maya.

6. DAFTAR PUSTAKA

[1]. Anderson, R. J., Civardi, M., & Ollivant, C. (2019). Integrating cyber into military planning. Joint Force Quarterly, 93, 17-23.

[2]. Baker, S. (2019). Cyber Security As National Security Issue: U.S. Has No Strategy. Forbes. Retrieved from https://www.forbes.com/sites/stephenbaker/2019/02/13/cyber-security-as-national-security-issue-us-has-no-strategy/?sh=3ca05c2454e6.

[3]. Blasco-Olaetxea, J.A., & Miguelez-Rodriguez, M.P. (2016). A Review of Cyberwarfare and Implications for International Law. Journal of Conflict Studies, 36(2), 152-169.

[4]. Bollen, J. (2011). Cyber warfare: A new era of conflict. Journal of Strategic Security, 4(1), 45-57.

[5]. Brenner, J. (2009). Cybersecurity and national policy. IEEE Security & Privacy, 7(4), 33-39.

[6]. Center for Strategic and International Studies (CSIS). (2018). The economic impact of cybercrime and cyber espionage. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime-and-cyber-espionage.

[7]. Clarke, R. A., & Knake, R. K. (2010). Cyberwar: The next threat to national security and what to do about it. Harper Collins.

[8]. Cole, E., & Ring, G. (2016). Information security: cybersecurity consulting and advisory services. Deloitte Insights. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-cfo-program-dbriefs-cybersecurity-consulting-and-advisory-services.pdf

[9]. Commission on Cybersecurity for the 44th Presidency. (2008). Securing cyberspace for the 44th presidency. Available at: https://www.belfercenter.org/sites/default/files/files/publication/Cybersecurity-Report.pdf

[10]. Council on Foreign Relations. (2019). Cyber Operations Tracker. Retrieved from https://www.cfr.org/interactive/cyber-operations.

[11]. Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

[12]. Firestone, R., & Rasmussen, M. S. (2016). Rethinking defense policy in the era of cyber warfare.

Army Cyber Institute at West Point.

[13]. Flamm, M. (2017). The Equifax data breach and cybersecurity in the United States. American Review of Public Administration, 47(6), 697-706. https://doi.org/10.1177/0275074017692760

[14]. Florencio, D. & Herley, C. (2017). A discussion of the role of cyber security in national security. Journal of Cyber Security Technology, 1(2), 76-86. doi: 10.1080/20531787.2017.1375021

[15]. Friedman, T. L., & Woo, T. (2019). Lessons from the world's most tech-savvy government. The Atlantic, 324(3), 38-48.

[16]. Gaetz, L., Osborn, G., & Fly, M. (2020). Cybersecurity and Cyber Warfare: The Evolution of Evolving Threats. Journal of Military and Veterans' Health, 28(2), 1-4.

[17]. Gartzke, E., & Lindsay, J. (2018). Cyberwar and the peace: why norms matter in cyber conflict. Journal of Conflict Resolution, 62(6), 1005-1037.

[18]. Gentry, Eric, & Price, David. (2015). Cybersecurity. Scholarly Commons. Retrieved from https://scholarlycommons.law.case.edu/caselrev/vol64/iss3/17.

[19]. Gross, J. & Livingston, S. (2018). The importance of cybersecurity to national security. Council on Foreign Relations. Retrieved from https://www.cfr.org/backgrounder/importance-cybersecurity-national-security.

[20]. Harknett, R. J. (2018). Emerging norms and standards for responsible state behavior in cyberspace. Annual Review of Cybersecurity and Cybercrime, 129-150.

[21]. Healey, J. (2010). A new era of cyber conflict. Survival, 52(5), 95-108.

[22]. Healey, J. (2010). The cyber threat grows and changes: Time to reconsider US government organizational and policy approaches. Strategic Studies Quarterly, 4(4), 41-52.

[23]. Johnson, I. (2018). Autonomous weapons and the morality of warfare. Routledge.

[24]. Jones, B. (2021). Preparing the DoD for Cyber Conflict: Recommendations for Changes to Acquisition Policies. Joint Force Quarterly, 100-110.

[25]. Kalathil, S., & Boas, T. C. (2018). Cyber threats and national security: A global challenge. The Brown Journal of World Affairs, 24(2), 193-208.

[26]. Kumar, S., Upadhyaya, S., & Singh, P. (2018). Cyber security awareness and training needs for non-technical personnel. Computers & Security, 74, 201-209.

[27]. Lewis, J.A. (2014). Cybersecurity, Cyberwar and the Future of Cyberspace. Survival, 56(5), 7-14.

[28]. Libicki, M. C. (2009). Cyberdeterrence and cyberwar. Rand Corporation.

[29]. Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation.
[30]. Lin, H., & Yang, D. (2019). Cybersecurity challenges and its strategy in the Era of Great Power Competition. Harvard Asia Quarterly, 21(3), 12-26.
[31]. Lindsey, R., Hatcher, J., Condron, S., & Johnson, N. (2018). The evolving nature of the modern conflict. Rand Corporation.
[32]. Mawn, B. (2015). Cybersecurity risk management: A review of the state of the art. Computers & Security, 53, 65-78.
[33]. Mazanec, B. M. (2012). Cyber threats and the decline of the nation-state? Journal of International Affairs, 65(1), 105-122.
[34]. Morris, E. (2017). Building a cybersecurity workforce. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF10604
[35]. National Research Council. (1991). Computers at Risk: Safe computing in the information age. National Academies Press.
[36]. Nissenbaum, H., & Shacham, D. (2014). Evaluating the impact of incident response plans on the effectiveness of cyber-security teams. Journal of Homeland Security and Emergency Management, 11(1), 37-55.
[37]. Nye, J. S. (2016). A new era of cyber conflict. Foreign Affairs, 94-104.
[38]. NZDF. (2018). Defence Capability Plan 2019. New Zealand Defence Force.
[39]. Park, N. H., Song, S. J., & Lee, T. (2021). The future development of cybersecurity workforce: Roles, skills, and training. Sustainability, 13(5), 2734.
[40]. Rid, T. (2018). Cyber war will not take place. Journal of Strategic Studies, 41(1-2), 6-32.
[41]. Schilling, C. (2015). Active Cyber Defense: A Framework for Policymakers. Journal of Strategic Security, 8(4), 1-17.
[42]. Soo Hoo, J., Dubois, J. E., Price, R. A., & Jones, S. R. (2019). The evolution of international cooperation in cybersecurity. Journal of Cybersecurity, 5(1), tyz002.
[43]. Taylor, T. (2020). Cybersecurity and the changing character of war. Global Policy, 11(S1), 6-16.
[44]. U.S. Department of Defense. (2018). Summary of the 2018 national defense strategy of the United States. Retrieved from https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
[45]. US Government Accountability Office. (2019). DOD Cyber Efforts: More Clarity on Roles and Resources Needed to Ensure Military Effectiveness. Report to Congressional Committees.
[46]. Waxman, M. C. (2015). Cybersecurity and the Use of Force. Yale Law Journal, 124, 1426-1471.

https://doi.org/10.2139/ssrn.2488580

[47]. Zetter, K. (2014). Countdown to zero days: Stuxnet and the launch of the world's first digital weapon. Crown Publishers.