JURNAL KEAMANAN NASIONAL, Vol. IX No. 2 (2023): pp. 299-324
ISSN 2442-7985 (Print) | ISSN 2579-7727 (online)
Available online at: https://ejurnal.ubharajaya.ac.id/index.php/kamnas

Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan

Thoughts on the Potential Threat of Cyber War in Indonesia: a Defense Strategy Study

Binar Arfa Darumaya[1], Syamsul Maarif[2], TSL Toruan[3], Yoedhi Swastanto[4]

[1,2,3,4] Program Doktoral Fakultas Strategi Pertahanan Universitas Pertahanan Republik Indonesia

Email: binararfadarumaya@gmail.com

Article Info:

Received: August 11, 2023	Revised: December 8, 2023	Accepted: December 26, 2023

Abstract: *The information technology revolution has changed the threat map into a more complex space. Cyberspace has become an unlimited platform for cyber activities conducted by various domestic, regional, and international actors. While some people in the world utilize advances in information technology for positive activities, others use it to present threats. This research analyses the State's perspective on cyber threats, particularly in the context of cyber warfare, in line with Indonesia's State defense doctrine that classifies threats into three forms: military, non-military, and hybrid. The research method used is qualitative. The research results are expected to provide a clear picture of the nature of the cyber war threat in Indonesia and the government's strategy in dealing with it. Thus, it is expected that there will be synergy between the role of the TNI as the main component of national defense and related ministries/agencies in developing strategies and implementing the national defense system to face the threat of cyber warfare.*

Keywords: *Cyber Warfare Threats, Strategy, National Defense*

Abstrak: *Revolusi teknologi informasi telah mengubah peta ancaman ke dalam ruang yang lebih kompleks. Ruang siber menjadi wadah tak terbatas bagi aktivitas siber yang dilakukan oleh berbagai faktor di tingkat domestik, regional, dan internasional. Meskipun sebagian masyarakat dunia memanfaatkan kemajuan teknologi informasi untuk aktivitas positif, sebagian lainnya*

memanfaatkannya untuk menyajikan ancaman. Penelitian ini menganalisis perspektif Negara terhadap ancaman siber, khususnya dalam konteks perang siber, sejalan dengan doktrin pertahanan Negara Indonesia yang mengklasifikasikan ancaman menjadi tiga bentuk: militer, non-militer, dan hibrida. Metode penelitian yang digunakan adalah kualitatif. Hasil penelitian diharapkan memberikan gambaran yang jelas tentang hakikat ancaman perang siber di Indonesia dan strategi pemerintah dalam menghadapinya. Dengan demikian, diharapkan adanya sinergi antara peran TNI sebagai komponen utama pertahanan nasional dan kementerian/ lembaga terkait dalam mengembangkan strategi serta melaksanakan sistem pertahanan nasional menghadapi ancaman perang siber.

Kata Kunci: *Ancaman Perang Siber, Strategi, Pertahanan Nasional*

Pendahuluan

Ruang siber telah menjadi domain perang kelima di samping domain darat, laut, udara, dan angkasa. Fenomena ini merupakan dampak dari perkembangan aktivitas siber yang terjadi secara cepat dan mampu mengambil alih sebagian besar aktivitas yang biasa dilakukan oleh manusia. Kondisi ini pada satu sisi menunjukkan kemajuan peradaban namun di sisi lain juga menimbulkan kompleksitas ancaman yang tidak terbendung. Bahkan saat ini, ruang siber menjadi media favorit bagi sebagian besar aktor baik aktor Negara (*state actor*) maupun aktor non Negara (*non state actor*) untuk melancarkan serangan yang dapat mengganggu stabilitas nasional suatu negara.

Ancaman perang siber telah berkembang pesat dan mewarnai dinamika lingkungan strategis. Dampak aktivitas siber terhadap kepentingan nasional juga telah diakui oleh *United Nations* (Perserikatan Bangsa-Bangsa/ PBB), sehingga muncul seruan agar Negara membangun pertahanan siber nasional.[1] Berkembangnya ancaman di ruang siber merupakan salah satu dampak dari arus globalisasi yang menimbulkan konsekuensi pada beralihnya aktivitas masyarakat secara manual menuju aktivitas berbasis teknologi informasi dan komunikasi yang saling terhubung. Wacana geopolitik menjadi semakin multidimensional mengingat dunia saat ini telah memasuki fase Revolusi Industri 4.0. Pada tatanan industri baru ini, *Artificial Intelligence* (AI), *Big Data*, *cloud*, *Internet of Things* (IoT), dan teknologi seluler telah mengubah dimensi dunia pada sektor ekonomi, bisnis, politik, budaya hingga kehidupan masyarakat dunia dengan cara yang sangat mendasar.[2]

[1] United Nations, *Cyberconflicts and National Security,* 2021, https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security; accessed Juni 23, 2023.

[2] Kris Wijoyo Soepandji dan Muhammad Farid, "Konsep Bela Negara dalam

Pada dasarnya, perkembangan teknologi informasi dan komunikasi, jaringan internet, dan ruang siber, memiliki urgensi dan menjadi salah satu bagian dari infrastruktur nasional dan global. Akan tetapi, dengan adanya sistem kritikal dan jaringan yang menjalankan berbagai aspek sosial, ekonomi, politik, maupun militer, ruang siber menjadi target yang menarik bagi pihak-pihak tertentu untuk mempengaruhi atau mengganggu keamanan nasional. Fenomena ini tentu menjadi tantangan sekaligus tuntutan bagi Negara-negara untuk memperkuat keamanan mereka dalam ruang siber dan melakukan persiapan secara dini untuk melindungi kepentingan nasional mereka melalui aksi militer jika diperlukan.[3] Karena Negara-negara maju bahkan telah memanfaatkan teknologi di ruang siber untuk mendukung aksi militer yang dilakukan oleh Negara.

Ancaman perang siber menunjukkan persepsi bahwa dunia maya atau ruang siber saat ini menjadi arena baru bagi perang dan serangan antarnegara. Dalam era teknologi informasi ini yang semakin berkemajuan, sistem dan infrastruktur kritis dalam sektor publik dan swasta sangat tergantung pada jaringan internet dan sistem informasi. Sehingga menjadi sangat penting bagi setiap negara untuk melindungi dan mempertahankan aset digital negara. Sebab ancaman siber bergerak tanpa mengenal batas Negara dan waktu. Serangan siber dan aktivitas keamanan siber menjadi bagian dari upaya untuk mencapai keunggulan militer dan diplomasi melalui jaringan dan sistem teknologi informasi. Oleh karena itu, ancaman di ruang siber dapat menimbulkan dampak yang signifikan terhadap asset dan infrastruktur Negara termasuk keamanan nasional dan stabilitas global.

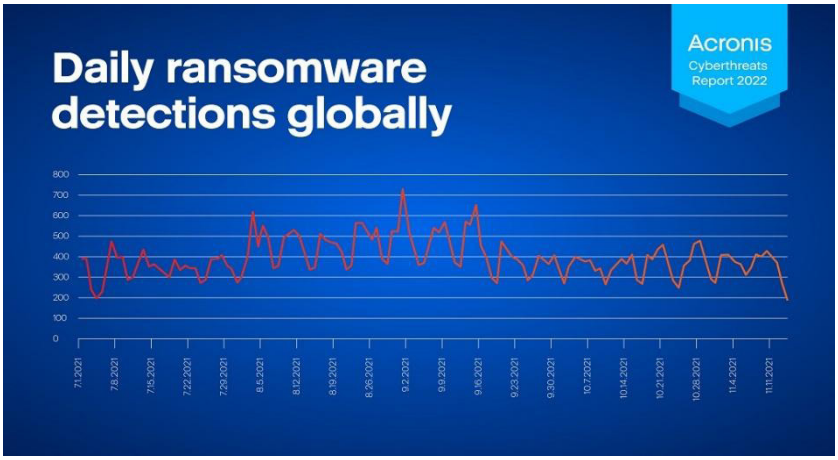
Ruang siber sebagai domain perang baru adalah perwujudan dari perang yang berlangsung melalui jaringan komputer dan sistem informasi, seperti internet. Dalam kondisi ini, actor siber baik negara, organisasi, maupun individu memanfaatkan jaringan komputer dan sistem informasi untuk melakukan serangan. Serangan ini bisa berupa penetrasi sistem, *phishing*, *malware*, dan lainnya yang bertujuan untuk mengakses, merusak, atau mencuri informasi penting. Berdasarkan studi dari para ahli dalam bidang keamanan siber, perang siber memiliki potensi yang sangat besar untuk mempengaruhi stabilitas dan keamanan global, karena jaringan komputer dan sistem informasi sudah menjadi bagian yang tidak

Perspektif Ketahanan," *Jurnal Hukum dan Pembangunan*, (2018): 442.

[3] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About it,*. (New York: Ecco, 2011).

terpisahkan dari kehidupan sehari-hari dan memainkan peran penting dalam banyak aspek, seperti militer, ekonomi, dan sosial.[4]

Acronis Cyber Threats Report 2022 mengacu pada pemeriksaan data serangan dan ancaman yang dikumpulkan oleh jaringan global perusahaan Acronis CPOC, memantau tren ancaman siber sebagaimana gambar berikut:[5]

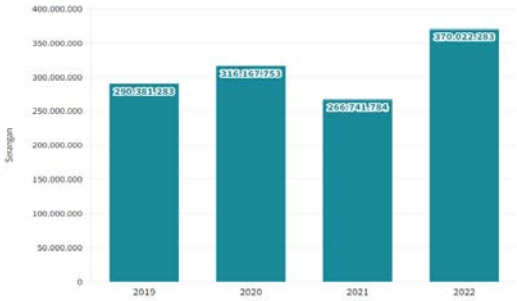


Di Indonesia, Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak 370,02 juta serangan siber terjadi pada tahun 2022. Dilihat dari sektornya, serangan ini paling banyak menyasar sektor administrasi pemerintahan yaitu mencapai 284,09 juta kasus. Pada sektor energi dan SDM, jumlah serangan siber mencapai 2,38 juta serangan. Sektor keuangan mengalami sebanyak 5,72 juta serangan siber, dan sektor kesehatan mengalami sebanyak 850.21 serangan siber. Tren ancaman ini terjadi secara fluktuatif sejak empat tahun terakhir, dapat dilihat melalui gambar berikut:[6]

[4] Shantanu Bhattacharya, Avinash Kumar Agarwal, T. Rajagopalan, dan Vinay K. Patel, *Nano-Energetic Materials: Energy, Environment, and Sustainability,* (New York: Springer, 2018).

[5] Cahyandaru Kuncorojati, *4 Prediksi Serangan Siber 2022 Menurut Acronis.* Januari 3, 2022, https://www.medcom.id/teknologi/news-teknologi/ob34qdYk-4-prediksi-serangan-siber-2022-menurut-acronis, accessed Juli 5, 2023.

[6] Febriana Sulistya Pratiwi, *BSSN Catat 370,02 Juta Serangan Siber ke Indonesia Pada 2022,* Juni 22 2022, https://dataindonesia.id/internet/detail/bssn-catat-37002-juta-serangan-siber-ke-indonesia-pada-2022



Aktor serangan siber cenderung memanfaatkan celah keamanan dan kerentanan ruang siber targetnya dalam melakukan serangan siber. Serangan siber yang dilakukan pada masa konflik, merupakan bentuk dukungan non-militer terhadap operasi militer yang dilakukan suatu Negara seperti yang pernah dialami Ukraina. Namun, disamping itu terdapat beberapa tujuan lain yang menjadi motivasi actor dalam melakukan serangan siber, di antaranya: a) mengeksploitasi data informasi pihak yang menjadi target serangan; b) melakukan pengecohan terhadap musuh; c) melacak sistem informasi musuh atau menghalangi musuh menggunakan sistem informasi milik mereka sendiri; dan d) merusak sistem informasi musuh.[7]

Pembahasan mengenai ancaman siber di Indonesia menjadi isu yang semakin mendesak dan kompleks, sebab seiring dengan kemajuan teknologi informasi dan ketergantungan masyarakat terhadap internet. Indonesia masih menghadapi beberapa permasalahan yang memperbesar peluang hadirnya ancaman siber. Di antara beberapa masalah tersebut seperti ketidaksiapan dan kurangnya kesadaran pengguna teknologi terhadap keamanan siber, regulasi dan kerangka hukum yang belum sepenuhnya mengakomodir kepentingan keamanan siber dan kurang adaptif, sumber daya manusia keamanan siber yang terbatas, ancaman natural yang berasal dari lingkungan, ketergantungan terhadap teknologi asing, dan lemahnya infrastruktur kritis yang mendukung upaya keamanan siber.[8]

Kompleksitas ancaman siber yang melibatkan berbagai aktor, motif, dan target telah dibahas dalam penelitian yang dilakukan Adi Rio

[7] Muhammad Syaroni Rofii, "Antisipasi Perang Siber: Postur Ketahanan Nasional Indonesia Merespon Ancaman Perang Siber," *Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 1, No. 2*, (2018): 105-114.

[8] Muhammad Prakoso Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)," *Politica, Vol. 13, No. 2*, (2022): 222-238.

Arianto dan Gesti Anggraini pada tahun 2019. Dalam penelitian tersebut dijelaskan terdapat empat aspek kompleksitas ancaman siber yang perlu diamati yaitu landasan geometri politika, pencegahan ekspansi kejahatan siber, penanganan ancaman siber global, dan struktur pertahanan dan keamanan siber nasional.[9] Penelitian ini mengembangkan pendekatan pertahanan dan keamanan siber nasional yang inklusif, melibatkan aspek sipil dan militer untuk mencegah ancaman siber global. Namun, penelitian ini belum merinci pemahaman tentang ancaman siber dan strategi yang diterapkan dalam konteks ancaman siber yang memiliki elemen militer dan non-militer.

Dalam rangka menghadapi ancaman perang siber di masa depan, maka kebijakan pertahanan siber harus dirumuskan secara dini dan bersifat responsif. Sebagaimana yang telah dibahas pada penelitian Maulia Jayantina Islami pada 2017, bahwa hambatan dalam pengimplementasian strategi pertahanan terkait ancaman siber dimana sumber daya manusia, prosedur dan kebijakan pencegahan dan keamanan masih memerlukan koordinasi dengan seluruh pemangku kebijakan bagi kalangan swasta, pemerintah, rakyat, dan lembaga luar negeri.[10] Sehingga pemerintah Indonesia harus terus berinisiatif untuk merancang strategi keamanan siber nasional yang ideal dalam program dan projek jangka pendek maupun panjang.

Dalam konteks globalisasi dan ketergantungan pada teknologi informasi, penelitian ini bertujuan menghadirkan pendekatan inovatif dengan menjelajahi secara komprehensif potensi ancaman perang siber yang mungkin dihadapi oleh Indonesia. Meskipun Indonesia belum secara nyata menghadapi peristiwa perang siber, namun pemerintah tetap perlu menyusun strategi pertahanan siber yang ideal demi menangkal ancaman perang siber di masa mendatang.

Postur pertahanan siber perlu dibentuk secara terpadu mulai dari aktifitas pemantauan, pendeteksian dini, peringatan dini, hingga pengambilan kebijakan dalam rangka menghadapi ancaman perang siber. Untuk itu penelitian ini diarahkan untuk mengeksplorasi strategi pertahanan Indonesia yang efektif dalam rangka menghadapi potensi ancaman perang siber.

---

[9] Adi Rio Arianto dan Gesti Anggraini, "Membangun Pertahanan dan Keamanan Siber Nasional Indonesia Menghadapi Ancaman Siber Global Melalui Indonesia Security Response Team on Internet Infrastructure (ID-SIRTII)," *Jurnal Pertahanan dan Bela Negara Vol. 9 No. 1*, (2019): 13-29.

[10] Maulia Jayantina Islami, "Tantangan dalam Implementasi Strategi Keamanan Siber Nasional Indonesia ditinjau dari Penilaian Global Cybersecurity Index," *Jurnal Masyarakat Telematika dan Informasi Vol 8, No. 2 (Oktober-Desember)*, (2017): 137-144.

Studi ini dilakukan dengan pendekatan pertahanan negara yang melihat serangan siber sebagai suatu ancaman nirmiliter yang berimplikasi terhadap pertahanan dan keamanan negara. Sehingga kajian ini mengarah pada pemikiran potensial ancaman siber guna memastikan bahwa Indonesia dapat mempertahankan sistem dan infrastruktur digitalnya secara dini serta memungkinkan respon cepat dan efektif terhadap ancaman siber sehingga stabilitas keamanan nasional dapat terjaga.

Hasil dari penelitian ini diharapkan dapat membantu pemerintah dan lembaga terkait dalam mengevaluasi kerentanan infrastruktur teknologi informasi di Indonesia terhadap serangan siber. Dengan memahami celah keamanan dan tingkat kerentanan sistem, dapat dirumuskan strategi untuk memperkuat perlindungan terhadap infrastruktur yang vital sekaligus mengembangkan kebijakan pertahanan siber yang adaptif dan proaktif demi menjaga kedaulatan digital Indonesia.

Tinjauan Literatur

Ancaman

Purnomo Yusgiantoro memberikan definisi umum terkait ancaman yaitu sebagai tindakan yang berasal dari dalam dan luar negeri yang dapat membahayakan keadaan negara dan keselamatan rakyat atau sesuatu sifatnya dapat menjadi penghambat serta penghalang terhadap kepentingan negara.[11] Adapun John M. Collins lebih terfokus pada evaluasi teknis terhadap ancaman. Dalam pemahamannya, Collins memandang terdapat tiga hal yang harus dipertimbangkan dalam memahami ancaman yakni metode dalam melihat kemampuannya (*capabilitie*s), intensitasnya (*intension*) dan kemudahan supaya dapat diserang (*vulnerabilities*). Sistem pertahanan dan keamanan negara perlu diarahkan untuk memastikan berdiri kokoh dan menguatkan fondasi negara bangsa dari ancaman dari luar dan dalam negeri.[12]

Burhan D. Magenda menjabarkan perihal pentingnya *software* yang merupakan ideologi negara dengan disokong oleh sistem politik, ekonomi dan sosial budaya. Sedangkan *hardware* yaitu instansi-instansi fungsional

[11] ITB, *Belajar Memahami Teori Ancaman dari Prof. Purnomo Yusgiantoro,* 2019, https://www.itb.ac.id/news/read/57328/home/belajar-memahami-teori-ancaman-dari-prof-purnomo-yusgiantoro; accessed Januari 13 2023.

[12] Wahyono, S.K, *Pengertian dan Lingkup Keamanan Nasional,* (Depok: KSKN UI, 2003).

berupa sumber daya nasional (sumdanas), selain itu juga didukung oleh partai politik, aparatur negara, serta dukungan dari masyarakat ekonomi dan masyarakat sipil. Ini menunjukkan bahwa Magenda memandang hadirnya ancaman ialah karena pengaruh ideologis dan budaya.[13]

Definisi-definisi di atas memiliki fokus dan prioritas yang berbeda dalam memandang suatu ancaman. Namun secara konseptual, ketiga ahli memiliki pandangan yang sama bahwa ancaman bersifat kompleks baik secara fisik (misalnya serangan terhadap infrastruktur) maupun non fisik (ideologi, sistem politik dan lain sebagainya).

Dalam konsep pertahanan negara, ancaman siber masuk dalam kategori ancaman nirmiliter karena sifatnya yang tidak melibatkan kekerasan fisik secara langsung, namun memiliki potensi yang serius terhadap keamanan nasional, baik melalui serangan terhadap infrastruktur vital, pencurian informasi rahasia negara, atau bahkan pengacauan sistem politik. Ancaman ini muncul dari dunia maya melalui perangkat lunak, jaringan komputer, dan internet. Sehingga peneliti menilai perlu untuk mengkaji potensi ancaman siber terhadap pertahanan negara Indonesia agar pemerintah memiliki acuan dalam pembentukan kebijakan, regulasi, investasi dalam teknologi keamanan, pelatihan personel, serta kerja sama internasional untuk memitigasi ancaman siber.

Ancaman Siber

Ancaman siber atau (*cyber threat*) merupakan segala aktivitas yang dapat menargetkan atau mempengaruhi perangkat, aplikasi, sistem, jaringan, misi, atau fungsi sistem yang menjadi infrastruktur penting sebuah organisasi.[14] Ancaman siber juga dapat didefinisikan sebagai segala sesuatu yang menimbulkan kerugian karena mengancam kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) sistem dan informasi.[15] Tren ancaman siber sudah mengalami perkembangan yang pesat dan mencakup segala aspek kehidupan dan kepentingan seperti kepentingan pertahanan, ekonomi, kepentingan tatanan dunia,

[13] Burhan D Magenda, *Penyiapan Pertahanan Negara Ditinjau Dari Strategi Ketahanan,* (Jakarta: FISIP UI, 2008).

[14] Deborah J. Bodeau, Catherine D. McCollum and David B Fox, "Cyber Threat Modeling: Survey, Assessment, and Representative Framework," *HSSEDI: Homeland Security System Engineering & Development Institute, April 7*, (2018).

[15] Ratno Dwi Putra, Supartono dan Deni D.A.R, "Ancaman Siber dalam Perspektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta)," *Jurnal Peperangan Asimetris, Vol. 4 No. 2*, (2018): 99-120.

kepentingan politik maupun kepentingan ideologi.[16] Saat ini serangan siber telah menjadi ancaman nyata terhadap suatu Negara sebab ruang siber (*cyber space*) telah menjadi domain kelima dalam peperangan selain darat, laut, udara, dan angkasa.

Berdasarkan sifatnya, Ghernaouti-Helie mengkategorikan ancaman siber ke dalam dua jenis yaitu serangan aktif dan serangan pasif. Serangan aktif mencakup upaya langsung untuk menembus, merusak, atau mengganggu sistem komputer atau jaringan. Serangan ini dilakukan oleh aktor siber dengan tujuan untuk mengubah sumber daya sistem seperti serangan *Denial-of Service* (DoS) atau *Distributed Denial-of-Service* (DDoS) yang ditujukan pada situs web atau infrastruktur penting, mengganggu layanan publik atau militer. Sedangkan serangan pasif mencakup upaya untuk memperoleh informasi atau mengintai tanpa merusak atau mengganggu operasi sistem komputer atau jaringan secara langsung. Serangan pasif cenderung fokus untuk melakukan pencurian data atau informasi tanpa merusak infrastruktur seperti serangan *phising yang menggunakan trik untuk mendapatkan informasi login atau informasi pribadi dari karyawan pemerintah atau militer*. Dalam konteks pertahanan nasional, kedua jenis serangan ini memiliki dampak yang serius terhadap keamanan, kestabilan, dan kelangsungan operasional negara sebab pada dasarnya ancaman siber dapat terjadi dalam berbagai bentuk dan metode yang sulit diprediksi.

Kekuatan siber menurut Nye, dijelaskan sebagai "*Cyber power can be used to produce preferred outcome within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace*". Terdapat tiga faktor yang menjadi inti dari penjelasan diatas yaitu *within*, *outside*, dan *instrument*, tiga faktor tersebut selanjutnya mendasari fungsi dan aplikasi dari kekuatan siber.

Within merujuk pada ancaman yang berasal dari dalam suatu entitas seperti negara atau organisasi. *Outside* merujuk pada ancaman yang berasal dari luar entitas seperti serangan dari negara lain atau pelaku kejahatan siber independen. *Instrument* mengacu pada bagaimana teknologi dan perangkat lunak digunakan sebagai alat penyerang atau sarana pertahanan siber.[17] Ketiga faktor tersebut memiliki nilai strategis bagi pemerintah atau organisasi untuk mengembangkan strategi

[16] Tamarell Vimy, Surya Wiranto, Rudiyanto, Pujo Widodo, dan Panji Suwarno, "Ancaman Perang Siber Pada Keamanan Nasional Indonesia," *Jurnal Kewarganegaraan, Vol. 6 No. 1 Juni*, (2022): 2319-2327.

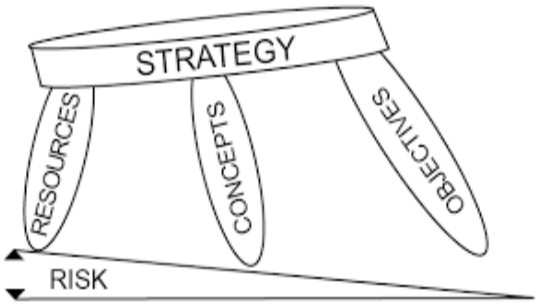
[17] Joseph S Nye, *Cyber Power,* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010).

pertahanan siber yang komprehensif dengan fokus pada mitigasi risiko, deteksi dini, dan respons yang cepat terhadap ancaman siber baik dari dalam maupun luar.

Strategi

Strategi adalah domain dari pemimpin senior di eselon negara yang lebih tinggi, militer, perusahaan bisnis, atau institusi lain. Henry Eccles menggambarkan strategi sebagai "... arah komprehensif dari kekuasaan untuk mengontrol kondisi dan wilayah untuk mencapai tujuan." Pada konteks penjelasan diatas maka strategi yaitu penggunaan instrumen atau elemen dalam menguasai kekuasaan baik di ranah politik, ekonomi, militer, dan teknologi informasi dalam pencapaian tujuan politik negara baik dengan cara bekerja sama atau bersaing dengan aktor lain demi memenuhi tujuannya sendiri.[18]

Penjelasan lain dijelaskan oleh Yarger dengan menggunakan model strategi Arthur Lykke yang menyatakan bahwa pembentukan strategi memiliki empat elemen yang harus diperhitungkan; tujuan (*ends / objectives*), cara (*ways / strategic concepts / courses of action*), dan sumber daya (*means / resources*), dan level bahaya (*risk*). Yerger menyatakan bahwa "*there are never enough resources or a clever enough concept to assure 100 percent success in the competitive international environment, there is always some risk*".



Gambar 2.2 Model Strategi Lykke

Model strategi Lykke (*ends, ways, means, dan risk*) yang terstruktur dan holistik dalam mengembangkan strategi dan rencana dalam berbagai

[18] H Richard Yarger, "Toward a Theory of Strategy: Art Lykke and the U.S. Army War College." In *U. S. ARMY WAR COLLEGE GUIDE*, by J. Boone Bartholomees Jr, 45-50, Carlisle Barracks: Strategic Studies Institute, (2012).

konteks, memungkinkan pemikiran yang lebih sistematis dan terkoordinasi dalam mencapai tujuan yang ditetapkan. Hal ini dapat diterapkan dalam berbagai sektor termasuk pertahanan siber untuk memastikan perlindungan yang efektif terhadap aset digital dan infrastruktur penting negara.[19]

Dengan teori ini, peneliti akan menganalisis strategi pertahanan dalam menghadapi ancaman perang siber di Indonesia dengan menggunakan keempat unsur yaitu tujuan, cara, sumber daya dan level bahaya. Unsur tujuan menjadi arah utama yang akan menjadi fokus dari strategi yang dirancang. Dalam konteks pertahanan siber, unsur tujuan dapat merujuk pada hasil yang diinginkan dalam perlindungan infrastruktur krusial, pengamanan data sensitif, atau memastikan kontinuitas operasional sistem krusial.

Unsur cara merujuk pada pendekatan yang diambil untuk mencapai tujuan yang telah ditetapkan. Ini melibatkan pemilihan metode, kebijakan, atau taktik yang dianggap efektif untuk mencapai tujuan yang telah ditetapkan. Dalam konteks pertahanan siber, unsur ini dapat meliputi investasi dalam teknologi keamanan terkini, peningkatan kerjasama internasional dalam pertukaran informasi intelijen siber, atau penyediaan pelatihan keamanan bagi personel yang terlibat.

Unsur sarana merujuk pada sumber daya yang tersedia atau diperlukan untuk melaksanakan strategi yang telah ditetapkan. Ini mencakup aspek-aspek seperti sumber daya finansial, teknologi, infrastruktur, tenaga kerja, dan keterampilan yang dibutuhkan. Dalam konteks pertahanan siber, means dapat melibatkan alokasi dana untuk investasi dalam keamanan siber, perekrutan dan pelatihan tenaga ahli keamanan siber, serta pengembangan infrastruktur yang mendukung.

Adapun unsur terakhir yaitu resiko berkaitan dengan identifikasi, evaluasi, dan manajemen risiko yang terkait dengan implementasi strategi. Risiko-risiko yang mungkin terjadi dalam menjalankan strategi perlu diidentifikasi, dievaluasi, dan langkah-langkah mitigasi perlu diambil untuk mengurangi risiko atau menghadapinya dengan lebih baik. Dalam konteks pertahanan siber, langkah-langkah mitigasi risiko bisa meliputi pemantauan terus-menerus terhadap ancaman, pengembangan rencana darurat dan respons terhadap serangan, serta meningkatkan kesadaran akan keamanan siber di seluruh sektor.

[19] Lykke, S. T. (2017), Strategic Decision-Making in Defense and Security: Insights from the Literature and Cases Since 9/11. Security Studies, 26(3), 479-516.

Metode Penelitian

Dalam penelitian ini, peneliti menggunakan metode penelitian kualitatif dengan pendekatan deskriptif analisis. Pemilihan metode kualitatif dalam penelitian ini didasarkan pada kebutuhan untuk mendapatkan wawasan yang lebih dalam, kontekstual, dan interpretatif mengenai bagaimana ancaman siber dipahami, dinilai, dan dihadapi di tingkat individu, organisasi, atau pemerintah. Melalui pendekatan ini, diharapkan bahwa penelitian akan memberikan pemahaman yang lebih kaya dan komprehensif tentang dinamika serta respon potensial terhadap ancaman siber di Indonesia. Metode kualitatif juga memungkinkan fleksibilitas dalam proses pengumpulan data, sehingga memberi peluang yang lebih besar kepada peneliti untuk memiliki pemahaman yang lebih luas terhadap ancaman siber di Indonesia. Sumber data penelitian ini diperoleh melalui sumber data sekunder berupa studi kepustakaan terhadap literatur ilmiah seperti buku, jurnal, dokumen resmi maupun bahan ilmiah lainnya yang relevan dengan topik penelitian. Selanjutnya data-data yang telah dikumpulkan dianalisis secara kualitatif dan disajikan dalam bentuk narasi. Dengan pendekatan kualitatif, diharapkan peneliti dapat melakukan analisis yang lebih kompleks terhadap data yang diperoleh sekaligus menemukan perspektif atau aspek baru terkait ancaman siber yang belum teridentifikasi sebelumnya. Penelitian ini juga diharapkan dapat memberikan kontribusi teoretis dengan memperkaya pemahaman tentang pemikiran strategis dalam menghadapi ancaman siber di Indonesia.

Pembahasan

Era teknologi informasi dan komunikasi yang mengglobal telah mengubah sifat konflik. Dalam beberapa dekade terakhir, kemajuan teknologi informasi seperti internet, komunikasi seluler, big data, kecerdasan buatan, dan teknologi lainnya telah menjadi pendorong utama perubahan dalam cara konflik terjadi, berkembang, dan terselesaikan. Konflik tidak lagi hanya terjadi dalam bentuk konflik militer konvensional, tetapi juga melalui serangan siber, propaganda online, atau taktik-taktik asimetris lainnya yang memanfaatkan kelemahan dan kerentanan teknologi. Ketergantungan pada teknologi membuat negara menjadi lebih rentan terhadap gangguan, sabotase, atau serangan terhadap infrastruktur teknologi yang vital. Perubahan ini menimbulkan tantangan baru bagi

keamanan nasional dan stabilitas global yaitu berupa ancaman di ruang siber.

Meningkatnya ketergantungan masyarakat modern terhadap teknologi digital mendorong hadirnya kerentanan sistem digital yang tanpa batas. Revolusi aktivitas siber telah mengubah tatanan politik, bisnis, budaya, dan aspek masyarakat lainnya, serta melahirkan tipe baru komunitas yang bermuara pada pertumbuhan organisasi sebagai jaringan yang mampu menciptakan tuntutan untuk peran baru bagi pemerintah dan umumnya menantang birokrasi hierarkis sambil mendorong tren menuju desentralisasi.[20] Sejak tahun 2007, berbagai macam kasus siber terjadi di berbagai belahan dunia dan tidak hanya menyasar individu non-negara, melainkan juga menargetkan keamanan pada skala nasional.

Secara umum, ancaman siber dapat bersifat internal dan eksternal. Ancaman internal umumnya berasal dari personel lembaga swasta atau publik, atau pengguna jaringan itu sendiri. Sedangkan ancaman eksternal berasal dari *hacker,* kelompok kriminal atau organisasi teroris, serta badan intelijen dan investigasi.[21] Lebih lanjut, Michael D. Mcdonnell dan Terry L. Sayers mengkategorikan ancaman siber ke dalam tiga kelompok yaitu:

a. Ancaman Perangkat Keras (*hardware threat*), seperti *jamming* dan *network intrusion*;
b. Ancaman Perangkat Lunak (*software threat*), seperti pencurian informasi atau *information theft*, perusakan informasi atau sistem atau information (*system destruction*), manipulasi informasi atau *information corruption*;
c. Ancaman Data/Informasi (data/*information threat*), seperti *information warfare.*

Dalam konteks keindonesiaan, Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber telah mengklasifikasi bentuk-bentuk ancaman *siber* yang meliputi: serangan *Advanced Persistent Threats* (APT), *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS); serangan *defacement*; serangan *phishing*; serangan *malware*; penyusupan siber; spam; dan penyalahgunaan protokol komunikasi. Namun beberapa ancaman di atas belum dapat dikategorikan ke dalam ancaman perang siber. Perang siber menurut Pedoman Pertahanan Siber merupakan semua tindakan yang dilakukan

[20] Joseph S Nye, *Power in the Global Information Age,* (New York: Routledge, 2004).

[21] Mahendro Bhirowo, Fauzia Gustarina Cempaka Timur, dan Mardi Siswoyo, Brunei Darussalam's E-Government Strategy in Overcoming Cyber Threats. *Jurnal Pertahanan Vol. 4, No. 3* (2018); 145-161.

dengan tujuan mengganggu kedaulatan Negara. Perang siber dapat berupa serangan terorisme (*cyber terrorism*) atau spionase (*cyber espionage*) dan memiliki beberapa karakteristik tertentu seperti disengaja (*intentional*), merupakan kegiatan aktif, dan berskala besar.[22] Beberapa peristiwa perang siber yang terdokumentasi di berbagai belahan dunia baru-baru ini dapat diuraikan sebagai berikut:[23]

Maret 2023:

- Peretas Rusia melumpuhkan situs web Majelis Nasional Perancis selama beberapa jam menggunakan serangan DDoS. Dalam sebuah posting Telegram, peretas mengutip dukungan pemerintah Prancis untuk Ukraina sebagai alasan serangan itu.
- Grup spionase siber China menargetkan perusahaan perlindungan data Asia Timur yang melayani entitas militer dan pemerintah yang berlangsung sekitar satu tahun
- Pejabat Estonia mengklaim bahwa peretas tidak berhasil menargetkan sistem pemungutan suara internet negara itu selama pemilihan parlemen baru-baru ini. Pejabat tidak merilis rincian tentang serangan itu atau memberikan atribus
- Peretas Korea Utara menargetkan perusahaan riset keamanan siber yang berbasis di AS dalam kampanye phishing. Kampanye itu dimaksudkan untuk mengirimkan malware untuk cyber espionage
- Polandia menyalahkan peretas Rusia atas serangan DDoS di situs web layanan pajak resminya. Peretas memblokir akses pengguna ke situs tersebut selama kurang lebih satu jam, tetapi tidak ada data yang bocor dalam serangan itu. Sebuah kelompok peretasan pro-Rusia sebelumnya menerbitkan pernyataan di Telegram tentang niatnya untuk menyerang layanan pajak Polandia
- Badan Keamanan Siber Uni Eropa (ENISA) merilis laporan yang mengutip ancaman signifikan terhadap

[22] Amber Corrin, "Some Key Events in the History of Cyber Warfare," October 15, 2009. https://fcw.com/articles/2009/10/19/feat-dod-cyber-timeline.aspx; accessed Maret 4 2023.

[23] CSIS, *Significant Cyber Incidents.* n.d. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents; accessed 8 Januari 2023.

sektor transportasi UE, dengan 98 insiden antara Januari 2021 dan Oktober 2022

Februari 2023:
- Polisi Belanda meretas dan membongkar Exclu, platform komunikasi terenkripsi, untuk mengganggu aktivitas organisasi kriminal. Pejabat Belanda juga meng eksfiltrasi data komunikasi dari server Exclu untuk digunakan dalam penyelidikan. Eurojust, Europol, dan polisi dari Italia, Swedia, Prancis, dan Jerman membantu dalam operasi tersebut
- Peretas Rusia menyebarkan malware untuk mencuri informasi dari organisasi Ukraina dalam kampanye phishing. Malware ini mampu mengekstrak informasi akun dan file, serta mengambil tangkapan layar. Para peneliti di Symantec percaya kelompok itu adalah pemain kunci dalam kampanye dunia maya Rusia melawan Ukraina
- Kelompok peretas pro-Rusia Killnet mengklaim bertanggung jawab atas serangan DDoS terhadap jaringan NATO yang digunakan untuk mengirimkan data sensitif. Serangan itu mengganggu komunikasi antara NATO dan pesawat yang memberikan bantuan gempa ke pangkalan udara Turki. Serangan itu juga membuat situs NATO offline sementara
- Pejabat Polandia melaporkan kampanye disinformasi yang menargetkan publik Polandia. Target menerima disinformasi anti-pengungsi Ukraina melalui email. Pejabat mengklaim kegiatan ini mungkin terkait dengan peretas yang terkait dengan Rusia
- Grup peretasan Korea Utara Lazarus melakukan kampanye spionase antara Agustus dan November 2022. Peretas menargetkan penelitian medis, perawatan kesehatan, pertahanan, energi, teknik kimia, dan universitas riset, mengekstraksi lebih dari 100MB data dari setiap korban namun tetap tidak terdeteksi. Kelompok ini terkait dengan pemerintah Korea Utara
- Hacktivists Iran mengganggu siaran televisi yang dikelola negara dari pidato presiden Iran Ebrahim Raisi selama upacara Hari Revolusi. Peretas menyiarkan

slogan "Matilah Khamenei" dan mendorong warga untuk bergabung dalam protes anti pemerintah

- Pihak berwenang dari Pusat Keamanan Siber Nasional Belanda mengklaim peretas pro-Rusia meluncurkan serangan DDoS yang menargetkan situs web rumah sakit di Belanda dan negara lain di Eropa

Januari 2023:

- Pejabat Latvia mengklaim bahwa peretas yang terkait dengan Rusia meluncurkan kampanye phishing spionase dunia maya terhadap Kementerian Pertahanannya. Kementerian Pertahanan Latvia menyatakan operasi ini tidak berhasil.
- CISA, NSA, dan Pusat Analisis dan Berbagi Informasi Multi-Negara mengeluarkan peringatan penasehat bersama tentang peningkatan peretasan pada cabang eksekutif sipil federal yang menggunakan perangkat lunak akses jarak jauh. Ini mengikuti laporan bulan Oktober 2022 tentang kampanye phishing bermotivasi finansial terhadap beberapa lembaga cabang eksekutif sipil federal AS
- Peretas yang terkait dengan Rusia mengerahkan serangan ransomware terhadap layanan pos Inggris, Royal Mail. Serangan itu mengganggu sistem yang digunakan untuk melacak surat internasional. Butuh waktu 20 hari bagi Royal Mail untuk memulihkan sepenuhnya layanan surat internasional
- Peretas mengganggu akses ke lebih dari 1.500 situs web pemerintah Nepal dengan membanjiri server utamanya dengan lalu lintas
- Peretas menargetkan jaringan pemerintah, militer, dan sipil di seluruh Asia Pasifik dengan memanfaatkan malware untuk mendapatkan informasi rahasia. Malware menargetkan data pada mesin korban serta audio yang ditangkap oleh mikrofon mesin yang terinfeksi
- Peretas mengirim lebih dari seribu email berisi tautan berbahaya ke akun pemerintah Moldova

Merujuk dari beberapa peristiwa di atas, dapat disimpulkan bahwa serangan siber pada serangan siber memiliki sasaran yang beragam seperti perorangan/masyarakat umum/organisasi, objek vital

infrastruktur negara, dan kepentingan nasional. Eksploitasi ruang siber ini tentu menimbulkan banyak dampak yang dapat berbentuk gangguan fungsional, pengendalian sistem secara *remote* untuk tujuan kejahatan, penyalahgunaan informasi, kerusuhan/ketakutan/kekacauan/konflik; dan kondisi lain yang sangat merugikan baik secara materiil maupun immaterial.

Secara faktual, Indonesia belum pernah mengalami peristiwa ancaman siber berupa perang. Meski demikian, pemerintah tetap harus membangun strategi *cybersecurity* secara handal dan sedini mungkin untuk mengantisipasi potensi ancaman perang siber yang dapat terjadi di masa mendatang. *Cybersecurity* merupakan sistem infrastruktur penting yang sangat berguna dalam mengamankan ruang siber dari resiko ancaman siber. *Cybersecurity* mencakup segenap fungsi seperti fungsi identifikasi, perlindungan, dete ksi, tanggapan, dan pemulihan. *Cybersecurity* membantu organisasi dalam mengekspresikan manajemen resiko keamanan siber dengan mengatur sistem keamanan siber untuk mencegah atau bahkan menangani ancaman siber.[24] Terdapat lima jenis *cybersecurity* yang dapat dijadikan rujukan mendasar dalam membangun keamanan siber nasional, yaitu *critical infrastructure cybersecurity; network security; cloud security; iot (internet of things) security; application security.*[25]

Disamping itu, Negara dapat membangun strategi antisipasi melalui konsep *six ware cybersecurity framework* (SWCSF). Konsep *six ware cybersecurity framework* (SWCSF) merupakan solusi untuk meningkatkan sistem keamanan jaringan komputer dan sistem informasi. SWCSF menekankan pada peningkatan sistem keamanan jaringan komputer dan sistem informasi instansi atau organisasi dengan menutup celah kerentanan yang terdapat dalam sistem komputer. SWCSF mengelaborasi platform *NIST Network Security Framework* agar menjadi lebih praktikal terutama pada tingkat taktis operasional pengamanan sistem jaringan komputer dan sistem informasi. SWCSF melibatkan enam komponen utama yaitu:[26]

a. Brainware atau *human factor* (faktor manusia)

Sumber daya manusia merupakan komponen terpenting dalam membangun sistem pertahanan dan keamanan ruang siber.

[24] National Institute of Standars and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," April 16, (2018).

[25] IT Governance, *What are the five types of cyber security.* n.d. https://www.itgovernance.co.uk/what-is-cybersecurity; accessed Januari 8, 2023.

[26] Rudy Gultom, *Cyber Warfare: Sudah Siapkah Kita Menghadapinya?,* (Jakarta: UNHAN Press, 2021).

Namun para pakar justru menyebut bahwa manusia merupakan komponen terlemah dalam lingkungan keamanan siber, hal ini yang kerap menjadi faktor rapuhnya sistem pertahanan dan keamanan siber di suatu negara. Sehingga setiap instansi harus memiliki sumber daya manusia yang kompeten dan dapat bertanggung jawab sebagai *Chief Information Security Officer* (CISO) untuk mengamankan sistem informasi di wilayah tugasnya.

b. *Hardware* (perangkat keras sistem komputer)

Serangan siber umumnya tidak hanya menggunakan satu teknik saja melainkan menggunakan beragam teknik serangan yang dapat memberikan dampak cukup kompleks. Untuk menghadapi keadaan demikian, maka kombinasi *risk assessment* dan *threat analysis* sangat dibutuhkan. Menjadi tanggung jawab CISO untuk mendidik seluruh tingkatan level sumber daya manusia untuk dapat menggunakan peralatan atau perangkat keras secara aman. Dalam hal ini, pemakaian firewall fisik sebagai perangkat keras untuk memantau dan mengatur lalu lintas data yang masuk dan keluar dari jaringan. Firewall ini bisa berfungsi sebagai pertahanan pertama terhadap serangan dari luar.

c. *Software* (perangkat lunak sistem aplikasi)

Perangkat lunak juga memiliki potensi tinggi untuk menjadi sasaran dalam serangan siber. Penyerang cenderung akan memanfaatkan sistem aplikasi target seperti email, website atau sosial media untuk diserang menggunakan virus atau *malware*. Untuk mengantisipasi ancaman ini, maka dibutuhkan pemakaian perangkat lunak antivirus dan antispyware pada setiap komputer dalam jaringan untuk mendeteksi dan menghapus ancaman siber seperti virus, malware, atau program jahat lainnya.

d. *Infrastructure Ware* (infrastruktur sistem jaringan komputer)

Infrastruktur sangat erat kaitannya dengan faktor manusia. Seringkali manusia tidak sadar bahwa sistem jaringan komputer yang mereka gunakan memiliki resiko serius terhadap serangan siber. Infrastruktur harus dimonitor secara teratur untuk memastikan keamanan sistem jaringan komputer dari potensi bahaya siber. Untuk mendukung upaya ini, dapat di implementasi sistem enkripsi pada seluruh komunikasi yang terjadi di dalam jaringan, baik yang berlangsung secara internal maupun

eksternal. Ini bertujuan untuk melindungi data yang dikirimkan agar tidak dapat diakses oleh pihak yang tidak berwenang.

e. Firmware (dokumen pendukung penyelenggaraan kegiatan)

Dalam rangka mengelola dan mengamankan jaringan komputer atau sistem informasi, maka perlu adanya dokumen pendukung yang dijadikan pedoman atau *grand design* dalam penyelenggaraan pengamanan sistem. Kebijakan keamanan siber yang mencakup prosedur untuk mengelola kata sandi yang kuat, batas waktu penggantian kata sandi, serta langkah-langkah dalam mengelola akses dan izin pengguna dapat menjadi pilihan dalam pengelolaan jaringan komputer.

f. Budgetware (sumber daya anggaran)

Komponen yang bernilai strategis lainnya yaitu sumber daya anggaran. Keberhasilan penyelenggaraan sistem pertahanan dan keamanan ruang siber sangat dipengaruhi oleh ketersediaan anggaran yang memadai. Hal ini perlu dipersiapkan dan direncanakan secara serius oleh pemerintah atau pimpinan instansi terkait agar upaya pengamanan ruang siber dapat dilakukan secara optimal. Anggaran untuk investasi pertahanan siber dapat dialokasikan untuk memperbarui sistem keamanan, melakukan pembaruan perangkat lunak, atau investasi dalam teknologi keamanan siber terkini yang diperlukan untuk melindungi infrastruktur digital dari ancaman.

Dalam era informasi yang meluas, dunia siber telah menjadi domain baru yang penuh dengan kecemasan informasi sebagai akibat dari meluapnya informasi. Menurut Bell & Wurman kelebihan informasi dapat menyebabkan kecemasan informasi. Hal ini merupakan hasil dari realitas online yang baru, di mana perhatian mudah terpecah dan menjadi komoditas dalam ekonomi perhatian. Oleh karena itu, diperlukan kerja sama antara para pemangku kepentingan dalam skala nasional dan global untuk menjaga ketahanan nasional. Ketersediaan informasi yang akurat dan dapat diandalkan pada dasarnya membutuhkan infrastruktur jaringan yang memadai dan aman dalam mentransmisikan pesan secara elektronik. Namun, pada kenyataannya, teknologi infrastruktur sering kali rumit.[27] Di Indonesia, ratusan hingga ribuan komputer, server, router, switch, dan kabel serat optik mendukung infrastruktur kritis nasional agar jaringan internet dapat berfungsi, tetapi sering kali aspek keamanan

[27] NATO, *The history of cyber attacks - a timeline.* 2013. https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm, accessed Januari 8, 2023.

informasi diabaikan. Padahal, keamanan jaringan dan perlindungan data pribadi sangat penting di era dunia siber saat ini.

Dalam konteks internasional, upaya pembangunan pertahanan siber dapat dilakukan melalui diplomasi dunia maya. Diplomasi dunia maya dapat dipahami sebagai serangkaian sikap para aktor internasional yang memberikan ruang terhadap negara mitra untuk saling berdialog yang mendorong terjalinnya kerja sama, kepercayaan antar negara dan terciptanya budaya global tentang keamanan dunia maya. Dengan demikian negara-negara di dunia akan bekerja sama untuk membentuk kebijakan dunia maya termasuk dalam aspek pertukaran informasi intelijen tentang ancaman siber yang dikenali atau serangan yang sedang berlangsung. Hal ini dapat membantu negara-negara untuk secara proaktif mengidentifikasi, menanggapi, dan mencegah serangan siber. Ini tidak hanya akan memberikan implikasi secara internasional melainkan juga akan memberikan dampak terhadap kepentingan nasional negara-negara yang terlibat. Diplomasi siber dan kerja sama internasional dalam keamanan siber menjadi penting untuk menciptakan lingkungan yang aman, stabil, dan terpercaya di ruang siber global. Tanpa kerja sama ini, sulit untuk menghadapi ancaman siber yang semakin kompleks dan menyebar secara global. Untuk mewujudkan tujuan tersebut, aktivitas diplomasi siber harus menyadari keberadaan entitas dan nilai yang beragam di dunia maya tidak hanya terkait aspek sosial politik, melainkan juga aspek teknisnya.[28]

Pertahanan siber telah menjadi salah satu aspek krusial dalam menjaga keamanan suatu negara di era digital ini. Namun, menjaga keamanan dalam ranah siber tidak hanya menyangkut masalah teknis, melainkan juga melibatkan aspek strategis yang kompleks. Kompleksitas dan sifat yang terus berubah dari ancaman siber menuntut pendekatan yang holistik dan terpadu untuk melindungi infrastruktur digital serta kepentingan nasional negara. Dalam konteks nasional, Sebagai regulator, pemerintah bertanggung jawab untuk menjaga agar infrastruktur teknologi nasional yang kritis dapat berfungsi dengan baik. Di Indonesia, *leading sector* dalam penyelenggaraan pertahanan siber adalah Badan Siber dan Sandi Nasional (BSSN) sesuai amanat Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Perpres Nomor 53 Tahun

[28] Fauzia Gustarina Cempaka Timur, The Rise of Cyber Diplomacy — ASEAN's Perspective in Cyber Security. *ICoSaPS Conference Proceedings The 3rd International Conference on Social and Political Science "The Impact of Information Technology on Social and Political Dynamics", (2016), Volume 2017* (pp. 244-250). KnE Social Sciences, (2017).

2017 tentang Badan Siber dan Sandi Negara. Beberapa tugas dan peran utama BSSN meliputi:

a. Melakukan pengembangan dan penerapan standar dan teknologi keamanan siber dan sandi untuk mendukung upaya peningkatan keamanan siber dan sandi di Indonesia;
b. Memberikan bantuan teknis dan layanan kepada pemerintah dan masyarakat dalam bidang keamanan siber dan sandi;
c. Melakukan kerjasama dan koordinasi dengan lembaga terkait dalam upaya peningkatan keamanan siber dan sandi di Indonesia;
d. Melakukan pemantauan dan evaluasi terhadap keamanan siber dan sandi untuk memastikan integritas dan kerahasiaan informasi dalam sistem dan jaringan siber di Indonesia;
e. Melakukan penelitian dan pengembangan teknologi dan solusi keamanan siber dan sandi untuk mendukung upaya peningkatan keamanan siber dan sandi di Indonesia.

Dalam mengupayakan pertahanan siber, BSSN telah meluncurkan tim tanggap insiden siber pada instansi pemerintah pusat atau yang disebut *Computer Security Incident Response Team* (CSIRT). CSIRT sebagai bagian dari proyek utama nasional dalam RPJMN Tahun 2020-2024, memiliki tugas dalam melakukan pemantauan, penerimaan, evaluasi, dan respons terhadap laporan serta kegiatan insiden siber. Tim ini dibentuk dengan tujuan melakukan penyelidikan menyeluruh serta melindungi sistem dari insiden siber yang terjadi di suatu organisasi. Sistem CSIRT diharapkan dapat menciptakan sistem elektronik yang aman dan kondusif di setiap instansi, yang kemudian dapat mendukung sinergi, kerja sama, dan komitmen untuk menciptakan lingkungan siber yang aman dan andal.[29]

Guna mewujudkan pertahanan siber yang ideal, keterlibatan pemerintah sangat diperlukan sebagai prioritas utama. Fokus pemerintah harus difokuskan pada memastikan bahwa perlindungan keamanan siber dapat memperkuat ketahanan nasional, melindungi keamanan, dan kedaulatan negara. BSSN, sebagai lembaga pemerintah yang bertanggung jawab di bidang keamanan siber, diharapkan menjadi pusat perhatian dan koordinator dalam penyelenggaraan keamanan siber di Indonesia terutama dalam membangun 3 strategi utama pertahanan siber yaitu:[30]

[29] Badan Siber dan Sandi Negara, *Bentengi Keamanan Siber Pemerintah BSSN Launching 17 CSIRT Instansi Pusat,* 2 Agustus 2023, https://www.bssn.go.id/bentengi-keamanan-siber-pemerintah-bssn-launching-17-csirt-instansi-pusat/, diakses pada 27 November 2023.

[30] Damar Apri Sudarmadi dan Arthur Josias Simon Runturambi, "Strategi Badan

a. Penyusunan kerangka hukum siber

   Di Indonesia, belum ada kerangka hukum yang mengatur secara khusus tentang keamanan siber. Oleh karena itu, sangat penting untuk memiliki dasar hukum yang menjadi landasan dalam pelaksanaan keamanan siber di Indonesia. Dengan adanya landasan hukum yang jelas, BSSN dapat merancang strategi pertahanan siber yang sesuai dengan prioritas keamanan siber. Ini melibatkan kolaborasi dengan berbagai pemangku kepentingan untuk membentuk sebuah organisasi pusat yang menjadi fokus utama dan bertanggung jawab dalam keamanan siber lintas sektor.

b. Peningkatan kapasitas keamanan siber

   Upaya ini dapat dilakukan melalui program kampanye kesadaran publik terhadap pentingnya keamanan siber. Kampanye kesadaran publik dapat dilakukan dengan menyebarkan informasi kepada berbagai pihak melalui organisasi, perpustakaan, komunitas, perguruan tinggi, dan program pendidikan bagi dewasa, sekolah, serta melibatkan organisasi guru dan orang tua untuk menyampaikan pesan tentang perilaku yang lebih aman dalam penggunaan teknologi. BSSN diharapkan dapat mendorong pemerintah untuk lebih memperhatikan sektor keamanan siber dengan menawarkan program mekanisme insentif. Tujuannya adalah untuk memperkuat kapasitas, baik dari segi SDM maupun teknologi dalam bidang keamanan siber. Memberikan insentif untuk pelatihan dan pendidikan di bidang keamanan siber menjadi faktor kunci dalam memastikan kontinuitas dan peningkatan keahlian serta keterampilan dalam pertahanan siber.

c. Penguatan kerja sama dalam keamanan siber

   Pemerintah Indonesia telah melakukan kerja sama baik secara bilateral dengan negara lain maupun secara multilateral dengan banyak negara serta berpartisipasi dalam forum internasional yang dihadiri oleh banyak negara anggota. Kerja sama ini merujuk pada kemitraan nasional yang secara resmi diakui untuk berbagi informasi keamanan siber atau aset lintas batas oleh pemerintah dengan pemerintah asing, entitas regional, atau organisasi internasional. Sebagai koordinator penyelenggaraan keamanan

Siber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber di Indonesia", *Jurnal Kajian Stratejik Ketahanan Nasional,* Volume 2 Issue 2, 2019, (163-183).

siber di Indonesia, diharapkan BSSN dapat meningkatkan kemitraan dalam hal pertukaran informasi atau aset antara kementerian, lembaga, dan instansi pemerintah lainnya sehingga upaya pertahanan siber dapat terintegrasi dan dapat secara optimal melaksanakan upaya mitigasi serangan siber.

Kompleksitas ancaman siber membutuhkan penanganan yang terpadu sehingga penyelenggaraan pertahanan siber harus melibatkan berbagai pihak sebagai wujud implementasi sistem pertahanan semesta. Dalam konteks pertahanan negara, Sistem Pertahanan Rakyat Semesta (Sishankamrata) adalah upaya pertahanan yang melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya. Pertahanan semesta dipersiapkan secara dini oleh pemerintah dengan penyelenggaraan yang bersifat total, terpadu, terarah, dan berkelanjutan.

Sishankamrata menekankan pada peran aktif masyarakat dalam mempertahankan negara dan mempromosikan nilai-nilai nasional seperti persatuan, kedamaian, dan keadilan. Dalam rangka membangun sistem pertahanan siber yang ideal, maka dibutuhkan kesadaran para pemangku kebijakan tentang resiko, ancaman dan kerentanan ruang siber. Dengan demikian, strategi menghadapi potensi ancaman siber dibangun dengan melibatkan seluruh komponen siber yang terkait yang secara khusus mampu melindungi infrastruktur kritis Negara dalam rangka menegakkan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa.

Penutup

Era teknologi informasi dan komunikasi yang berkembang secara masif membawa dampak yang signifikan terhadap perubahan pola ancaman. Ruang siber telah menjadi domain perang kelima yang cenderung dimanfaatkan oleh aktor tertentu baik aktor Negara maupun aktor non Negara untuk mengganggu stabilitas keamanan nasional suatu Negara. Ancaman di ruang siber dapat menyasar perangkat keras, perangkat lunak, dan data/ informasi. Namun tidak setiap serangan dapat dikategorikan sebagai ancaman perang siber. Perang siber diartikan sebagai segala tindakan yang bertujuan mengancam kedaulatan Negara dan memiliki beberapa karakteristik utama yaitu dilakukan dengan sengaja (*intentional*), merupakan kegiatan aktif, dan berskala besar. Peristiwa perang siber pernah terjadi di beberapa Negara di dunia salah satunya Ukraina.

Pembangunan strategi pertahanan siber dapat dilakukan dengan melibatkan beberapa aspek yaitu *brainware* atau *human factor* (faktor manusia), *hardware* (perangkat keras sistem komputer), *software* (perangkat lunak sistem aplikasi), *infrastructure ware* (infrastruktur sistem jaringan komputer), *firmware* (dokumen pendukung penyelenggaraan kegiatan), dan *budgetware* (sistem anggaran). Di Indonesia, terdapat Badan Siber dan Sandi Negara (BSSN) yang menjadi *leading sector* dalam membangun pertahanan siber. BSSN memastikan dan menjamin keamanan informasi dan komunikasi dalam sistem dan jaringan siber, serta menjaga integritas dan kerahasiaan informasi yang dikandung dalam sistem dan jaringan siber di Indonesia. BSSN menyusun Strategi Keamanan Siber Indonesia sebagai acuan bersama seluruh pemangku kepentingan keamanan siber nasional dalam menyusun dan mengembangkan kebijakan keamanan siber di instansi masing-masing.

Daftar Pustaka

Aji, Muhammad Prakoso. "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)." *Politica, Vol. 13, No. 2*, 222-238, (2022).

Armawi, Armaidy. *Nasionalisme dalam Dinamika Ketahanan Nasional.* Yogyakarta: UGM Press, 2020.

Badan Siber dan Sandi Negara, *Bentengi Keamanan Siber Pemerintah BSSN Launching 17 CSIRT Instansi Pusat,* 2 Agustus 2023, https://www.bssn.go.id/bentengi-keamanan-siber-pemerintah-bssn-launching-17-csirt-instansi-pusat/, diakses pada 27 November 2023.

Bhattacharya, Shantanu., Agarwal, Avinash Kumar., Rajagopalan, T., dan Patel, Vinay K. *Nano-Energetic Materials: Energy, Environment, and Sustainability.* New York: Springer, 2018.

Bhirowo, Mahendro., Timur, Fauzia Gustarina Cempaka., dan Siswoyo, Mardi. Brunei Darussalam's E-Government Strategy in Overcoming Cyber Threats. *Jurnal Pertahanan Vol. 4, No. 3* , 145-161 (2018).

Bodeau, Deborah J., McCollum, Catherine D., and Fox, David B. "Cyber Threat Modeling: Survey, Assessment, and Representative Framework." *HSSEDI: Homeland Security System Engineering & Development Institute, April 7*, (2018).

Clarke, Richard A. Clarke and Knake, Robert K. *Cyber War: The Next Threat to National Security and What to do About it.* New York: Ecco, 2011.

Corrin, Amber. "Some Key Events in the History of Cyber Warfare." October 15, 2009. https://fcw.com/articles/2009/10/19/feat-dod-cyber-timeline.aspx; accessed on Maret 4, 2023.

CSIS. *Significant Cyber Incidents.* n.d. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents; accessed on Januari 8, 2023.

Gultom, Rudy. *Cyber Warfare: Sudah Siapkah Kita Menghadapinya?* Jakarta: UNHAN Press, 2021.

IT Governance. *What are the five types of cyber security.* n.d. https://www.itgovernance.co.uk/what-is-cybersecurity; accessed on Januari 8, 2023

ITB. *Belajar Memahami Teori Ancaman dari Prof. Purnomo Yusgiantoro.* 2019. https://www.itb.ac.id/news/read/57328/home/belajar-memahami-teori-ancaman-dari-prof-purnomo-yusgiantoro; accessed on Januari 13, 2023.

Kuncorojati, Cahyandaru. *4 Prediksi Serangan Siber 2022 Menurut Acronis.* Januari 3, 2022. https://www.medcom.id/teknologi/news-teknologi/ob34qdYk-4-prediksi-serangan-siber-2022-menurut-acronis; accessed on July 5 2023.

Lykke, S. T. (2017), Strategic Decision-Making in Defense and Security: Insights from the Literature and Cases Since 9/11. Security Studies, 26(3), 479-516.

Magenda, Burhan D. *Penyiapan Pertahanan Negara Ditinjau Dari Strategi Ketahanan.* Jakarta: FISIP UI, 2008.

National Institute of Standars and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." April 16, (2018).

NATO. *The history of cyber attacks - a timeline.* 2013. https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm; accessed on Januari 8, 2023.

Nye, Joseph S. *Cyber Power.* Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.

Nye, Joseph S. *Power in the Global Information Age.* New York: Routledge, 2004.

Putra, Ratno Dwi., Supartono, dan D.A.R, Putra. "Ancaman Siber dalam Perspektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta)." *Jurnal Peperangan Asimetris, Vol. 4 No. 2*, 99-120 (2018).

Rofii, Muhammad Syaroni. "Antisipasi Perang Siber: Postur Ketahanan Nasional Indonesia Merespon Ancaman Perang Siber." *Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 1, No. 2*, 105-114 (2018).

S.K, Wahyono. *Pengertian dan Lingkup Keamanan Nasional.* Depok: KSKN UI, 2003.

Soepandji, Kris Wijoyo, and Muhammad Farid. "Konsep Bela Negara dalam Perspektif Ketahanan." *Jurnal Hukum dan Pembangunan*, 442 (2018).

Sudarmadi, Damar Apri dan Arthur Josias Simon Runturambi, "Strategi Badan Siber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber di Indonesia", *Jurnal Kajian Stratejik Ketahanan Nasional,* Volume 2 Issue 2, 2019, (163-183).

Supply Chain Game Changer. 2021. https://supplychaingamechanger.com/the-industrial-revolution-from-industry-1-0-to-industry-5-0/; accessed on Juni 15, 2023.

Swivelsecure. 2021. https://swivelsecure.com/solutions/manufacturing/manufacturing-is-at-risk-from-cybercrime/; accessed on Juni 15, 2023.

Timur, Fauzia Gustarina Cempaka. The Rise of Cyber Diplomacy — ASEAN's Perspective in Cyber Security. *ICoSaPS Conference Proceedings The 3rd International Conference on Social and Political Science "The Impact of Information Technology on Social and Political Dynamics", (2016), Volume 2017* (pp. 244-250). KnE Social Sciences, (2017).

United Nations. *Cyberconflicts and National Security.* 2021. https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security; accessed on Juni 23, 2023.

Vimy, Tamarell, Wiranto, Surya, Widodo, Pujo, dan Suwarno, Panji. "Ancaman Perang Siber Pada Keamanan Nasional Indonesia." *Jurnal Kewarganegaraan, Vol. 6 No. 1 Juni*, 2319-2327 (2022).

Yarger, H Richard. "Toward a Theory of Strategy: Art Lykke and the U.S. Army War College." In *U. S. ARMY WAR COLLEGE GUIDE*, by J. Boone Bartholomees Jr, 45-50. Carlisle Barracks: Strategic Studies Institute, 2012.