Jurnal Strategi Kampanye Militer
Volume 11, Nomor 2, 2025 E-ISSN 2830-3261

PERAN DPR RI DALAM PEMBENTUKAN REGULASI KEAMANAN SIBER UNTUK KETAHANAN NASIONAL

Muhammad Iqbal Dzuhri
Universitas Pertahanan RI
iqbaldzuhri17@gmail.com

Abstract

Cyberspace has emerged as a strategic domain that significantly affects political, social, economic, and national defense stability. The rapid development of digital technologies has transformed the nature of threats, compelling states to establish new regulatory frameworks that are legal, accountable, and democratic in order to address evolving cybersecurity challenges. In this context, legislative institutions occupy a central position in ensuring that cybersecurity policies are formulated in a legitimate, inclusive, and nationally resilient manner. This study identifies three strategic aspects of the DPR RI role in cybersecurity governance, the formulation of legal frameworks for cybersecurity, the exercise of oversight over executive cybersecurity policies, and the harmonization of public representation with multi-stakeholder collaboration. A strong and adaptive legislative role, supported by effective oversight mechanisms, is essential for producing cybersecurity policies capable of mitigating risks and threats that may undermine national resilience.

Keywords: *DPR RI, national resilience, legislature, cybersecurity, policy oversight*

Abstrak

Ruang siber menjadi tempat strategis dimana dapat mempengaruhi stabilitas politik, sosial, ekonomi dan pertahanan negara. Banyak ancaman yang bentuknya berubah akibat pesatnya perkembangan teknologi, hal ini menuntut negara untuk membangun regulasi baru yang legal, akuntabel, dan demokratis untuk menghadapi perubahan bentuk ancaman tersebut. Lembaga legislatif memiliki posisi pusat dalam memastikan kebijakan keamanan siber dibentuk secara sah, inklusif dan berorientasi pada ketahanan nasional. Hasil penelitian ini menunjukan tiga aspek strategis peran DPR RI dalam pembentukan kerangka hukum keamanan siber, pelaksanaan fungsi pengawasan terhadap kebijakan lembaga eksekutif, dan harmonisasi kebijakan representasi publik dan kolaborasi multi-stakeholder. Peran legislatif yang kuat, adaptif dengan pengawasan yang efektif, akan menghasilkan kebijakan keamanan

siber yang dapat mencegah resiko dan ancaman yang dapat melemahkan ketahanan nasional.

Kata Kunci : DPR RI, ketahanan nasional, legislatif, keamanan siber, pengawasan kebijakan

1. Pendahuluan

Ketahanan nasional dibentuk untuk menanggapi adanya ancaman konvensional terutama agresi militer antar negara dan konflik perang bersenjata. Tetapi dengan semakin pesatnya perkembangan teknologi digital, negara juga semakin bergantung terhadap teknologi yang menyebabkan munculnya ancaman keamanan, dimana ruang digital menjadi ruang strategis baru dalam berpolitik, sosial dan hukum (Kello, 2017).

Ancaman digital memiliki sifat asimetris yang dimana hal ini sulit dideteksi dan tidak terikat oleh batas teritorial negara (Nye, 2017). Serangan siber dapat diberlakukan oleh aktor negara atau non-negara dengan biaya yang rendah, tetapi dapat menyebabkan dampak besar terhadap stabilitas nasional, dengan menarget infrastruktur vital dan sistem pemerintahan (Carr, 2021). Hal ini membuat keamanan siber menjadi bagian menyeluruh pada ketahanan nasional modern di ranah teknologi informasi, yang dimana jika keamanan siber melemah dan tidak dapat diatasi maka dampak serangan siber dapat melemahkan stabilitas sosial-politik dan dapat memicu krisis pada kepercayaan masyarakat terhadap institusi negara.

Tanpa adanya kerangka regulasi yang jelas dan demokratis, kebijakan keamanan siber dapat beresiko menghasilkan implementasi pengawasan berlebihan yang dapat mengikis kepercayaan publik terhadap pemerintah dan kebebasan masyarakat, hal ini menjadikan regulasi keamanan siber menjadi instrumen strategis yang menjembatani kebutuhan keamanan negara dan perlindungan hak warga negara (Deibert, 2020). Penting adanya peran lembaga legislatif dalam menjaga keseimbangan antara keamanan dan kebebasan sipil, karena lembaga legislatif harus

dapat memastikan bahwa kebijakan siber harus berorientasi pada keamanan negara dan perlinduingan hak digital masyarakat (Bovens, 2007).

Regulasi keamanan siber menjadi arsitektur normatif yang mengatur hak dan kewajiban dan koordinasi antar aktor dalam merespon ancaman digital (Kshetri, 2021). Regulasi juga menetapkan tata kelola, akuntabilitas institusi, batas kewenangan negara dalam mengelola ruang digital, dan mengatur penindakan kejahatan siber. Kebutuhan regulasi keamanan siber semakin diperlukan jika dihubungkan dengan semakin menignkatnya frekuensi serangan terhadap data pemerintah dan swasta. DPR RI memiliki peran yang krusial dalam membentuk dan menjaga kerangka regulasi keamanan siber, dan memiliki tanggung jawab konstitusional dalam pengawasan terhadap implementasi kebijakan dengan menyerap aspirasi masyarakat dalam proses legislasi. Namun masih lemahnya harmonisasi pada aspek hukum, kelembagaan dan teknologi, sedangkan DPR RI memiliki tanggung jawab strategis dalam membentuk regulasi yang mampu menyeimbangkan antara keamanan nasional, kepastian hukum dan perlindungan hak asasi manusia. Legitimasi kebijakan keamanan sangat bergantung pada keterlibatan aktif parlemen dalam proses perumusan dan pengawasan kebijakan strategis.

Kebijakan siber dapat efektif jika ada keterlibatan legislatif dalam memastikan keseimbangan antara kepentingan keamanan, perlindungan hak asasi manusia dan kepastian hukum (Mueller, 2019). Dengan itu lembaga legislatif perlu menjadi penghubung antara pemerintah dan masyarakat dalam memastikan kebijakan siber yang inklusif. Peran legislatif dalam pembentukan regulasi keamanan siber nasional, sangat penting, dan relevan dalam keterlibatannya secara prosedural dan juga substansial dalam memahami cara ketahanan nasional dibentuk dalam era digital. Penelitian berfokus pada menganalisis peran DPR RI dalam pembentukan dan pengawasan regulasi keamanan siber sebagai bagian dari ketahanan nasional dengan melihat bagaimana DPR RI bekerja dalam menjalankan fungsi-fungsinya untuk memastikan kebijakan siber nasional dapat bersifat adaptif, inklusif dan demokratis.

2. Tinjauan Pustaka

2.1. Keamanan Siber sebagai Bagian dari ketahanan Nasional

Keamanan siber menjadi elemen fundamental dalam konsep ketahanan nasional modern, dimana ketergantungan terhadap teknologi digital menjadikan ruang siber sebagai tempat strategis yang setara dengan darat, laut, udara dan antariksa. Kekuatan nasional pada era digital menjadi sangat penting, dimana hal tersebut bisa menentukan kemampuan negara dalam melindungi dan mengendalikan struktur informasi serta infrastruktur digitalnya, karena dengan adanya ancaman dan gangguan pada ruang siber dapat menghasilkan dampak sistemik yang dapat melampaui kerusakan fisik (Nye, 2017).

Keamanan siber memiliki karakter lintas sektor dan lintas aktor, dengan begitu ancaman siber yang ada bukan hanya berasa dari negara lain, tetapi juga dari aktor non negara (Dunn Cavelty, 2018). Kondisi tersebut menyebabkan keamanan siber menjadi salah satu isu ketahanan nasional yang kompleks, karengan serangan digital tersebut memperlihatkan kemampuan negara dalam menjaga integritas sistem informasi, kepercayaan publik dan dapat mengganggu fungsi vital negara dalam lingkup ketahanan nasional.

Regulasi keamanan siber berfungsi sebagai instrumen strategis untuk menyatukan aspek teknis, hukum dan politik. Tanpa adanya kerangka hukum yang jelas negara akan kesulitan membangun respon nasional yang terkoordinasi terhadap ancaman siber, yang dapat membuat ketahanan nasional menjadi rapuh walaupun kapasitas teknologinya sudah tinggi (Lewis, 2020). Dengan begitu, maka keamanan siber harus dipahami sebagai bagian menyeluruh dari suatu strategi ketahanan nasional yang memerlukan legitimasi politik dan hukum yang kuat. Keamanan siber memiliki dampak strategis pada stabilitas negara dan hak warga negara, dengan pembentukan

regulasi yang legal dan demokratis merupakan syarat utama dalam membangun ketahanan nasional digital.

2.2. Peran Lembaga Legislatif dalam Regulasi Keamanan Siber

Lembaga legislatif memegang peran utama dalam politik dimana menjadi ruang batas antara keamanan nasional, kebebasan masyarakat, dan kontrol negara pada ruang digital (Kello, 2017).

Legislatif memiliki peran yang krusial dalam kebijakan keamanan siber, dimana ancaman siber sering digunakan untuk memperluas kewenangan negara. Jika tidak ada pengawasan parlemen yang efektif, kebijakan keamanan siber memiliki potensi untuk berkembang menjadi instrumen pengawasan berlebihan yang dapat merusak prinsip demokrasi, dengan begitu parlemen perlu berfungsi sebagai mekanisme *checks and balances* agar kebijakan keamanan siber tidak bersifat represif (Deibert, 2019).

Parlemen menjadi ruang deliberatif yang mempertemukan kepentingan negara, sektor privat dan masyarakat sipil dalam merumuskan regulasi siber yang inklusif dan berkelanjutan (Carr, 2021). Dengan begitu, legitimasi kebijakan keamanan siber sangat ditentukan dengan sampai sejauh mana proses legislasi yang transparan dan partisipatif.

2.3. Tantangan Hukum dan Legislasi Siber di Era Dinamis

Tantangan utama dari regulasi keamanan siber adalah sifat dari ancaman siber yang sangat dinamis dan cepat berubah, dimana perkembangan tersebut jauh lebih cepat dari proses legislasi, sehingga banyak regulasi siber berisiko menjadi usang sejak awal diberlakukan. Menurut Brenner (2019), hal tersebut disebut sebagai *regulatory lag,* dimana kondisi hukum yang tertinggal dari realitas teknologi yang menyebabkan hilangnya efektivitas dalam menghadapi ancaman baru.

Karakter lintas batas dalam ruang siber membuat tantangan yang lebih serius bagi konsep kedaulatan hukum nasional. Serangan siber sering berasal dari

yurisdiksi yang berbeda, dengan melibatkan aktor anonim, dan menggunakan infrastruktur global. Menurut Goldsmit dan Wu (2018), hukum nasional menghadapi keterbatasan struktural ketika diterapkan pada ruang siber yang tidak mengenal batas geografis, yang menyebabkan perlu adanya koordinasi internasional yang sering tidak sejalan dengan kepentingan politik domestik.

Regulasi keamanan siber terlalu menekankan aspek kontrol dan pengawasan yang dapat menimbulkan pelanggaran privasi, pembatasan berekspresi dan chilling effect dalam kehidupan politik masyarakat dimana hal tersebut menjadi tantangan yang menjadi dilema antara keamanan dan perlindungan hak asasi manusia. Tanpa batasan hukum yang jelas, teknologi pengawasan digital dapat menggeser demokrasi menuju bentuk kontrol yang tidak terlihat namun efeknya sangat efektif.

Parlemen dalam merumuskan regulasi yang adaptif harus tetap berlandaskan prinsip negara hukum, yang menjadikan tantangan terbesar dalam regulasi keamanan siber bukan pada kekurangan teknologi, melainkan pada kemampuan institusi politik untuk mengelola ketidakpastian dan risiko secara demokratis (Dunn Cavelty dan Wenger, 2020).

3. Metode Penelitian

Penelitian ini menggunakan metode kualitatif deskriptif menggunakan pendekatan studi dokumen, penelitian kualitatif relevan untuk menggali makna, konteks, serta konstruksi kebijakan dalam institusi politik dan hukum (Creswell dan Poth, 2018). Kualitatif digunakan untuk memahami peran, logika kebijakan, dan perubahan normatif lembaga legislatif dalam pembentukan regulasi keamanan siber.

Analisis dokumen digunakan untuk dapat melihat ide, kepentingan dan norma dibentuk sebagai kebijakan tertulis yang sesuai sebagai kajian legislasi dan tata kelola keamanan (Bowen, 2009). Pengumpulan data regulasi

keamanan siber dasarnya merupakan produk politik dan hukum yang terekam dalam dokumen resmi negara dan literatur kebijakan.

Peraturan perundang-undangan terkait keamanan siber di indonesia, yang akan digunakan berupa Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), kemudian Undang-Undang Perlindungan Data Pribadi (UU PDP), dan Rancangan Undang-Undang Keamanan dan Ketahanan Siber. Dokumen tersebut digunakan untuk memahami kontribusi DPR RI dalam proses legislasi serta fungsi pengawasannya terhadap kebijakan keamanan siber.

Dokumen akademik dan riset kebijakan digunakan untuk membahas peran lembaga legislatif, cybersecurity, dan ketahanan nasional. Literatur-literatur ini digunakan untuk membuat kerangka konseptual, memperkuat analisis normatif yang dalam hal kasus nasional ini bisa masuk dalam diskursus global (Snyder, 2019).

Analisis komparatif terbatas terhadap regulasi keamanan siber di beberapa negara digunakan sebagai referensi untuk mengidentifikasi praktik legislasi yang dianggap relevan pagi penguatan peran parlemen. Dengan adanya perbandingan hukum bisa digunakan sebagai alat reflektif dalam pembentukan kebijakan domestik (Kan-Freund, 2017).

Pendekatan ini memberi gambaran yang lengkap bagaimana peran DPR RI dalam merumuskan regulasi keamanan siber, mengidentifikasi tantangan institusional dan normatif yang dihadapi lembaga legislatif dalam menanggapi perubahan ancaman siber yang semakin berkembang.

4. Hasil dan Diskusi

4.1. DPR RI sebagai Pembentuk Kerangka Hukum Keamanan Siber

Berdasarkan analisis terhadap UU ITE, UU Perlindungan Data Pribadi dan RUU Keamanan dan Ketahanan Siber, terlihat bahwa DPR RI menjadi

aktor utama dalam pembentukan batas hukum keamanan siber nasional, dimana lembaga legislatif memiliki posisi sebagai instrumen adaptif yang harus menyesuaikan diri dengan perubahan ancaman siber yang berkembang pesat. Keamanan siber memiliki lingkungan ancaman yang dinamis, dimana hal ini perlu adanya regulasi yang mengatur dengan tingkat fleksibilitas normatif yang tidak mengorbankan kepastian hukum.

Dengan adanya revisi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan terbentuknya Undang-Undang Perlindungan Data Pribadi (UU PDP) yang memperlihatkan peran DPR RI dalam menutup celah hukum yang muncul akibat percepatan transformasi digital. UU perlindungan Data Pribadi memperlihatkan adanya perubahan pendekatan yang awalnya hanya pada pengendalian konten, menjadi kepada perlindungan hak digital warga negara. Dengan proses revisi UU ITE dan pembahasan RUU Keamanan dan Ketahanan Siber memperlihatkan tindakan DPR RI dalam mengurangi resiko *legal lag* atau hukum yang tertinggal dari perkembangan teknologi. Nilai demokrasi harus tetap menjadi pondasi dalam pembuatan regulasi yang adaptif tetapi tetap memiliki batas normatif yang jelas dan tetap melindungi kepentingan nasional tanpa membatasi kebebasan masyarakat menjadi harapan kepada DPR RI kedepannya.

Regulasi siber terbentuk dari proses legislasi yang memiliki tingkat legitimasi publik yang lebih tinggi dibanding kebijakan yang bersifat teknokratis atau didelegasi kepada lembaga eksekutif. Dalam pembentukan hukum, DPR RI berperan dalam hal-hal yang berkaitan dengan legitimasi demokratis kebijakan keamanan siber, hal ini berfungsi juga sebagai penjaga keseimbangan antara kebutuhan keamanan negara dan perlindungan hak warga negara di ruang digital. Hal ini menjadi temuan yang memperlihatkan bahwa proses legislasi keamanan siber di Indonesia masih mengalami tantangan pada menjaga fleksibilitas regulasi dan kepastian hukum. Perlu

adanya ketepatan dalam pembuatan regulasi, dimana regulasi tidak boleh dibuat terlalu longgar atau terlalu kaku, yang dapat mempengaruhi inovasi dan adaptasi dalam pembuatan regulasi selanjutnya, dan bisa dapat disalahgunakan jika regulasi tersebut memiliki celah dalam pembentukannya.

4.2. Fungsi Pengawasan dan Akuntabilitas Publik

Legislasi dalam fungsi pengawasan, menjadi elemen yang dibutuhkan dalam memastikan implementasi kebijakan keamanan siber berjalan sesuai prinsip demokrasi dan hak asasi manusia. Fungsi pengawasan legislasi dipandang menjadi kunci dalam mencegah penyalahgunaan kekuasaan dalam sektor keamanan. Akuntabilitas publik menjadi jantung dari tata kelola demokratis yang menyangkut kebijakan pengawasan dan kontrol teknologi. Kebijakan keamanan siber dapat berubah dari melindungi masyarakat menjadi alat politik dalam mengkontrol masyarakat, jika tidak berpedoman pada pengawasan demokrasi, yang dapat mengancam privasi masyarakat.

DPR RI memiliki instrumen pengawasan seperti rapat dengar pendapat, evaluasi anggaran dan pemanggilan kementerian atau lembaga teknis terkait keamanan siber, yang dengan adanya mekanisme parlemen tersebut memperlihatkan bahwa kebijakan siber ada dalam pengawasan legislatif dalam mencegah kecenderungan sekuritisasi yang berlebihan. Akuntabilitas perlu dilakukan oleh semua pihak yang terlibat dalam pembuatan regulasi, karena kolaborasi ini harus memastikan agar kebijakan keamanan siber tidak bergeser menjadi alat kontrol yang berlebihan terhadap masyarakat.

Pengawasan parlemen harus memastikan bahwa teknologi pengawasan tidak melanggar prinsip proporsional dan keadilan, dengan menjaga norma agar kebijakan keamanan siber tetap selaras dengan ketahanan nasional yang demokratis dan inklusif. Hal ini memperlihatkan bahwa masih perlu adanya peningkatan fungsi pengawasan DPR RI pada evaluasi kebijakan dan transparansi pelaksanaan, karena ketika pengawasan lembaga legislatif lemah,

maka dapat mengakibatkan kebijakan keamanan siber hanya berada diatas kertas dan tidak berpengaruh signifikan pada implementasi di lapangan dalam peningkatan keamanan nasional. Hal ini menjadi poin dimana perlu adanya prosedur audit reguler dan pelaporan yang transparan pada publik agar kebijakan keamanan digita dapat dievaluasi dan dibangun secara demokratis.

4.3. Harmonisasi Kebijakan dan Kolaborasi Multi-Stakeholder

DPR RI memiliki peran strategis dalam mengharmonisasi kebijakan dan tata kelola multi stake holder, dimana perlu adanya keterlibatan pemerintah, swasta, masyarakat sipil dan komunitas teknologi, hal tersebut diperlukan dalam regulasi keamanan siber karena regulasi ini tidak dapat berdiri sendiri sebagai produk hukum negara. Perlu adanya aspek lain selain keamanan yang perlu diperhatikan seperti, inovasi, ekonomi digital, dan hak warga negara, karena tata kelola ruang siber akan berhasil jika semua hal tersebut dapat seimbang dalam proses pembuatan kebijakan yang dapat diterima oleh masyarakat. Efektifitas regulasi siber sangat bergantung pada sampai mana aktor non negara dilibatkan dalam proses perumusan kebijakan, karena regulasi yang dirancang tanpa partisipasi masyarakat dan pemangku kepentingan, beresiko tidak implementatif dalam prakateknya, dan kehilangan dukungan oleh publik. DPR RI memiliki aspek strategis dalam mengharmonisasikan kepentingan perlindungan negara dan kebebasan individu. Yang dimana hal ini juga menjadi tugas DPR RI yang sebagai fasilitator politik dalam membuka ruang dialog antara negara, pelaku industri digital, ademisi, dan masyarakat sipil dengan instrumen rapat dengar pendapat dan rapat dengar pendapat umum.

Harmonisasi bukan hanya dilakukan kepada setiap aktor yang bersangkutan dalam proses pembuatan regulasi, tetapi juga harmonisasi regulasi pada standar internasional, yang mehasilkan regulasi yang bukan

hanya dapat berfungsi di nasional, tertapi juga selaras dengan wilayah siber internasional. Kolaborasi terhadap aspek pertahanan dianggap penting dalam memastikan regulasi keamanan siber juga mempertimbangkan inovasi, ekonomi digital, hak digital warga negara. Tata kelola teknologi berkelanjutan dapat dicapai dengan keseimbangan antara keamanan, kebebasan dan tanggung jawab bersama, dengan dibantu dengan dibentuknya regulasi yang dibuat oleh lembaga legislasi, diharapkan mampu menjadi penghubung kepentingan dalam lingkup keamanan siber nasional. Koordinasi antar lembaga dan sediktinya ruang partisipasi publik dalam penyusunan kebijakan, menjadi tantangan yang dihadapi dalam proses kolaborasi pembentukan regulasi dengan para stakeholder. Yang membuat DPR RI harus mendorong tata kelola dalam partisipasi masyarakat yang transparan, inklusif dan akuntabel.

5. Kesimpulan

Dari hasil pembahasan, dapat disimpulkan bahwa pembentukan regulasi keamanan siber yang dilakukan oleh DPR RI bersifat sentral dan multidimensional. Dimana dalam pembentukan undang-undang, DPR RI juga memiliki peran strategis dalam pengawasan kebijakan, penghubung kepentingan publik dan juga menentukan arah prioritas keamanan nasional di ranah digital, hal ini semakin penting dalam mencegah terjadinya serangan digital yang semakin berkembang pesat.

Peran Legislatif harus kuat, adaptif dan berorientasi pada prinsip demokrasi, dengan begitu kebijakan yang dibentuk dapat menyesuaikan dengan cepatnya perkembangan ancaman digital. Posisi strategis yang dimiliki DPR RI digunakan untuk memastikan keamanan siber menjadi bagian dari strategi ketahanan nasional yang berkelajutan, bekeadlian dan berlandaskan nilai-nilai demokratis.

Pergeseran paradigma keamanan menuntut negara agar mempunyai regulasi yang dapat menjawab kerumitan dari ancaman non-tradisional seperti ruang siber.

Keamanan siber merupakan tantangan bagi pemerintah dimana hukum dan tata kelola menjadi hal yang penting berdampingan dengan aspek teknis. Peran DPR RI menjadi kunci dalam mengatur dan memastikan bahwa aspek seperti normatif, kelembagaan dan akuntabilitas dari kebijakan keamanan siber dapat berjalan seimbang.

DPR RI memiliki dua fungsi dimana perannya dalam pembentukan kerangka hukum nasional dan pengawasan terhadap pelaksanaan kebijakan eksekutif agar setiap kebijakan yang dibuat untuk keamanan siber tidak melanggar hak warga negara dan bisa berpotensi disalahgunakan untuk kepentingan politik. Akuntabilitas publik menjadi pusat dalam legitimasi pemerintahan yang demokratis, dimana legislatif mengawasi kontrol demokratis pada kekuasaan eksekutif di bidang siber.

Dalam menghubungkan antara negara dan masyarakat dengan isu-isu keamanan digital, legislatif memiliki peran dalam menjembatani hal tersebut. Dengan adanya keterbukaan informasi dan partisipasi publik, maka legislatif perlu memberikan suatu ruang deliberatif agar bisa mempertemukan kepentingan publik, swasta dan komunitas teknologi. Tata kelola siber memerlukan pendekatan multi-stakeholder agar efektif, karena hal ini dapat menciptakan sinergi lintas sektor agar kebijakan dapat diterima dan dijalankan secara berkelanjutan.

5.1. Saran

- **Penguatan Kapasitas Legislasi Siber**

  DPR RI perlu memperkuat pengetahuan dan keahlian pada bidang keamanan siber dengan membentuk komite khusus, perlu adanya penekanan tentang pemahaman strategis dalam pembuatan kebijakan untuk lebih memahami kompleksitas ruang siber. Perlu adanya pemahaman logika dalam teknologi agar dapat membuat tata kelola pemerintahan yang efektif.

- **Peningkatan Fungsi Pengawasan dan Transparansi**

  Perlu adanya peningkatan dalam implementasi kebijakan keamanan siber agar dapat memperkuat efektivitas keamanan dan perlindungan hak asasi manusia. Dengan adanya peningkatan pengawasan, hal ini dapat meingkatkan juga kepercayaan publik terhadap pemerintah. Transparani yang dilakukan juga dapat memperlihatkan kinerja bulanan, hasil rapat kerja, laporan tahunan, dan forum aspirasi masyarakat yang dapat digunakan untuk menyerap masukan masukan untuk dapat digunakan sebagai referensi dan saran dalam pembuatan kebijakan selanjutnya.

- **Penguatan Pendekatan Multi-Stakeholder**

  DPR RI perlu lebih aktif dan terbuka dalam memfasilitasi dialog antara pemerintah, swasta, akademisi, dan masyarakat sipil dalam proses legislasi keamanan siber, hal ini dipercaya dapat menghasilkan regulasi yang lebih berkualitas dan meningkatkan ketaatan dalam implementasi. Tata kelola ruang siber tidak dapat dicapai hanya jika negara bekerja sendiri, dimana legitimasi dan keefektifitasan kebijakan yang ingin dihasilkan, harus dengan dibantu aktor-aktor lain untuk mendapat kolaborasi yang lengkap dalam menjaga keamanan siber.

- **Harmonisasi Regulasi dan Diplomasi Siber**

  Perlu adanya harmonisasi lintas sektor dalam meregulasi bidang siber, telekomunikasi dan perlindungan data pribadi, dimana hal ini menjadi peran DPR RI dalam menyatukan seluruh regulasi agar sesuai dengan standar internasional. Perlu adanya penguatan dalam kredibilitas

dan kerja sama karena akan menentukan status Indonesia pada tata kelola siber di dunia internasional.

- **Penguatan Nilai Demokrasi dan Hak Digital**

  Nilai-nilai demokratis menjadi hal utama dalam fokus kebijakan keamanan siber, dimana hal ini menjadi poin penting yang lembaga legislatif pegang dalam memastikan regulasi tetap sejalan dengan perkembangan teknologi tanpa membatasi kebebasan berekspresi masyarakat. Dengan adanya keamanan, perlu adanya pengawasan dalam hal melindungi hak digital warga negara, hal ini diperlukan dalam menjaga keseimbangan antara keamanan dan kebebasan yang lembaga legislatif lakukan dalam memastikan kebijakan pada ketahanan siber nasional tidak mengkontrol secara berlebihan, tetapi menjadikan keadilan dan kepercayaan publik terhadap negara sebagai salah satu fokus utama dalam proses pembuatan regulasi.

6. Ucapan Terimakasih

Penulis berterima kasih kepada Universitas Pertahanan RI atas dukungan yang telah diberikan dalam penyusunan penelitian ini. Penulis juga mengapresiasi kepada rekan-rekan Prodi Peperangan Asimetris Cohort XIV yang telah memberikan masukan dan diskus yang konstruktif selama proses penulisan penelitian ini.

Daftar Pustaka

Arvianto, T., & Halkis, M. (2025). *Information security and digital sovereignty: A cyber–crypto–signal defense model for Indonesia*. Journal of Scientific Papers: Social Development and Security, 15(6).p.32-44, https://doi.org/10.33445/sds.2025.15.6.4,

Bovens, M. (2007). *Analysing and assessing accountability: A conceptual framework.* European Law Journal, 13(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

Bowen, G. A. (2009). *Document analysis as a qualitative research method.* Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027

Brenner, J. L. (2019). *Cyber threats and national security: Navigating digital risks.* Oxford University Press.

Carr, M. (2021). *Legislating cyberspace: The politics of cyber security governance.* Journal of Cyber Policy, 6(2), 187–205. https://doi.org/10.1080/23738871.2021.1936472

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches (4th ed.).* Sage Publications.

Deibert, R. (2019). *Reset: Reclaiming the internet for civil society.* House of Anansi Press.

Deibert, R. (2020). *Cybersecurity governance and the challenge of surveillance capitalism.* Journal of Global Security Studies, 5(3), 419–435. https://doi.org/10.1093/jogss/ogaa014

Denardis, L. (2020). *The internet in everything: Freedom and security in a world with no off switch.* Yale University Press.

Denardis, L., & Raymond, M. (2017). *Thinking clearly about multistakeholder internet governance.* Internet Policy Review, 6(3). https://doi.org/10.14763/2017.3.778

Dunn Cavelty, M. (2018). *Cybersecurity governance: The limits of public–private partnerships.* Journal of Cyber Policy, 3(2), 213–235. https://doi.org/10.1080/23738871.2018.1483524

Dunn Cavelty, M., & Wenger, A. (2020). *Cyber security meets security politics: Complex technology, fragmented politics, and networked science.* Contemporary Security Policy, 41(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Goldsmith, J., & Wu, T. (2018). *Who controls the internet? Illusions of a borderless world (2nd ed.).* Oxford University Press.

Kello, L. (2017). *The virtual weapon and international order.* Yale University Press.

Kshetri, N. (2021). *Cybersecurity policy and governance: Global perspectives.* Computer Law & Security Review, 41, 105528. https://doi.org/10.1016/j.clsr.2021.105528

Lewis, J. A. (2020). *Cybersecurity and cyberwar: What everyone needs to know (2nd ed.).* Oxford University Press.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life.* Polity Press.

Mueller, M. (2019). *Networks and states: The global politics of internet governance.* MIT Press.

Ningsih, D. A. N., Halkis, M., & Susanto, R. (2024). Pertimbangan etika dalam pengembangan teknologi militer: Tinjauan filsafat ilmu pertahanan. *Jurnal Kewarganegaraan*, *8*(1).

Nye, J. S. (2017). *Deterrence and dissuasion in cyberspace.* International Security, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war.* W. W. Norton & Company.