TINJAUAN PUSTAKA

Landasan Teori

Sejumlah landasan teori dipergunakan sebagai dasar dalam penelitian "Strategi Pengembangan Kebijakan Kedaulatan Siber Nasional untuk Mengantisipasi Ancaman Serangan Berbasis Teknologi Informasi dalam Bingkai Pemutakhiran Doktrin Pertahanan Negara" ini. Keseluruhan teori yang relevan tersebut dapat dibagi menjadi tiga domain kelompok sesuai dengan keterkaitannya dengan fokus penelitian, yaitu:

1. Teori Makro - terkait dengan Filsafat Ilmu Pertahanan, Ancaman Berbasis Teknologi Informasi, dan Strategi Pertahanan Negara;
2. Teori Meso – terkait dengan Doktrin Pertahanan Negara dan Kedaulatan Siber; dan
3. Teori Mikro – terkait dengan Strategi Pengembangan dan Evaluasi Kebijakan

Filsafat Ilmu Pertahanan

Kamus besar Bahasa Indonesia mendefinisikan "ilmu" sebagai suatu pengetahuan tentang sebuah bidang yang disusun secara bersistem menurut metoda-metoda tertentu, yang dapat digunakan untuk menerapkan gejala-gejala tertentu di bidang (pengetahuan) tersebut, seperti ilmu hukum, ilmu pendidikan, ilmu ekonomi dan sebagainya. Pengertian tersebut menyimpulkan bahwa ilmu merupakan kumpulan pengetahuan yang disusun sedemikian rupa secara sistematis, berbasis pada metoda-metoda tertentu (Nagatsu et al., 2020). Suatu pengetahuan dapat dikatakan sebagai ilmu apabila memenuhi sejumlah persyaratan, antara lain adalah: (i) adanya obyek kajian; (ii) memiliki metoda; (iii)

bersifat sistematis; (iv) berlaku secara universal; (v) bersifat obyektif; (vi) bersifat analitis; dan (vii) bersifat verifikatif. Dalam konteks ini, pertahanan dapat dikatakan sebuah ilmu karena memenuhi ketujuh kriteria tersebut, dengan keterangan ringkas sebagai berikut:

1. Obyek kajian yang dipelajari adalah *state behavior* atau perilaku negara dalam mempertahankan eksistensi, kedaulatan, dan keselamatannya;

2. Metoda yang dipergunakan dalam mempelajari perilaku negara tersebut berupa kajian empiris dan metodologis, melalui model penelitian kuantitatif, kualitatif, dan kombinasi keduanya;

3. Tata cara yang dipergunakan untuk melahirkan berbagai konsep dan teori terkait dengannya dilakukan secara sistematis, yaitu melalui kajian, penelitian, maupun pendekatan ilmiah terstruktur lainnya;

4. Pengetahuan yang dihasilkan bersifat universal, mengingat negara merupakan entitas yang telah ada selama ribuan tahun dan di dalamnya terdapat begitu banyak *body of knowledge* yang dipegang teguh, diadopsi, dan diimplementasikan oleh penyelenggara negara maupun pemangku kepentingan terkait;

5. Dalam menggeluti khasanah pengetahuan ini, dilakukan beragam usaha berbasis kegiatan analitis, mengingat sangat sarat spektrum bahasan yang berhubungan dengan strategi, kebijakan, mekanisme, prosedur, dan kerangka; dan

6. Kebenaran akan topik bahasan di seputarnya dapat diverifikasi mengingat seluruh aktivitas didasarkan pada fakta dan data yang dikumpulkan secara valid serta diolah dengan menggunakan kaidah-kaidah akademik yang berlaku (baca: pendekatan ilmiah).

Terdapat perbedaan yang mendasar antara “ilmu” dan “pengetahuan”. Ilmu dapat diartikan sebagai pengetahuan mengenai suatu bidang tertentu, dan telah disusun dengan sistematis menurut metoda tertentu sehingga dapat menjelaskan secara rinci, detail, dan memiliki kebenaran yang bersifat umum. Sementara pengetahuan adalah informasi yang sudah diketahui oleh seseorang atau sekelompok orang, walaupun kebenarannya masih belum duji dan dikaji secara ilmiah (Maxwell, 2019).

Tabel 2. 1 Perbedaan Ilmu dan Pengetahuan

	Ilmu	Pengetahuan
Karakteristik	Memiliki sistem yang sudah tersusun secara sistematis	Belum tersusun secara sistematis
Jangkauan	Lebih luas	Tidak terlalu luas
Metode Pembuktian	Bersifat objektif	Bersifat subjektif
Objek yang disampaikan	Telah diuji dan dikaji	Belum diuji dan dikaji
Kebenaran	Harus bersifat umum dan universal	Sesuai pemahaman sekelompok orang

Sumber : Perbedaan Ilmu dan Pengetahuan (Rofiq, 2018)

Pengetahuan dapat menjadi sebuah ilmu apabila telah teruji kebenarannya dan memiliki sejumlah persyaratan karakteristik yang terkait dengannya sebagaimana telah dipaparkan sebelumnya (Rofiq, 2018). Tabel di atas memperlihatkan perbedaan keduanya dipandang dari aspek karakteristik, jangkauan, metoda pembuktian, obyek yang disampaikan, dan kebenaran.

Pada mulanya, pertahanan dianggap sebagai sebuah pengetahuan, karena adanya fenomena sebagai berikut:

1. Adanya pengetahuan kolektif yang terkumpul selama berabad-abad lamanya dan ditularkan secara turun temurun mengenai teknik berperang sebagai bagian tak terpisahkan dari usaha menjaga dan mempertahankan keutuhan negara (seperti pada zaman Kekaisaran Romawi, Kerajaan Yunani, Dinasti Cina, dan lain sebagainya) (Dwicahyo, 2019);

2. Ditemukannya berbagai artefak pengetahuan dalam bentuk arsip maupun dokumen berbasis pengalaman seseorang atau sekolompok orang yang kemudian didokumentasikan dalam bentuk publikasi seperti karya-karya klasik semacam *The Art of War* dari Sun Tzu, *the Military Institutions of the Roman* dari Vegetius, *Mes Reveries* dari Maurice de Saxe, maupun *The Military Maxims of Napoleon* dari Napoleon Bonaparte (Giles, 2013; Jordán, 2020; Sultana, 2017);

3. Diimplementasikannya konsep-konsep pertahanan yang dikembangkan berbagai pihak dalam hidup berbangsa dan bernegara, dimana prinsip-prinsip pengetahuan yang ada dimanifestikan dalam berbagai artefak seperti: peraturan, kebijakan, mekanisme, prosedur, kerangka, dan lain sebagainya (Anggoro, 2003; Rahman, 2018); dan

4. Terbentuknya Kementerian Pertahanan di berbagai negara dunia dimana pengetahuan mengenai prinsip, strategi, dan pendekatan pertahanan sebuah negara menjadi panduan sekaligus pengangan dalam menghasilkan berbagai kebijakan dan produk strategis pertahanan negara (Arvianissa & Fitriani, 2018; Riana Nugraha, 2017).

Ontologi dari ilmu pertahanan adalah "*state behavior*" atau perilaku sebuah negara untuk menjaga keberadaan/eksistensi dan mengembangkan keberlanjutan negara yang bersangkutan. Perilaku yang dimaksud adalah suatu

proses alami atau terancang yang terjadi dalam sebuah negara dalam rangka menjaga *vis-à-vis* mempertahankan keberadaannya *(defense mechanism)*. Mekanisme ini perlu dimiliki karena begitu banyaknya kejadian, fenomena, dan intervensi dari dalam dan luar negara yang berpotensi mengganggu dan/atau mengancam keberadaannya. Negara dianggap ada apabila terjadi integrasi dan konvergensi antara empat komponen penting, yaitu adanya wilayah geografis, rakyat, pemerintahan, dan pengakuan dari negara lain. Kedaulatan sebuah negara akan terancam apabila terjadi gangguan pada wilayahnya, rakyatnya, pemerintahannya, atau persepsi/pandangan negara lain terhadap eksistensi yang bersangkutan (Jazuli, 2016).

Dalam rangka menjaga keutuhan suatu negara, perlu adanya dua fungsi utama yang harus dikelola secara holistik, yaitu pertahanan dan keamanan. Pertahanan dirumuskan sebagai segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah sebuah negara, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara. Sementara keamanan itu sendiri merupakan upaya menegakkan ketertiban masyarakat di dalam negeri berdasarkan hukum yang berlaku. Dimensi dari ancaman bermacam-macam, seperti aspek ideologi, politik, ekonomi, sosial-budaya, teknologi, dan militer yang berpotensi menimbulkan dampak serius terhadap eksistensi sebuah negara, seperti (Anggoro, 2003; “Konsep Dan Sist. Keamanan Nas. Indones.,” 2016):

1. Ancaman terhadap Wilayah – sengketa wilayah perbatasan, penetrasi militer negara asing, perang terbuka maupun perang dingin, dan lain sebagainya;

2. Ancaman terhadap Masyarakat – adu domba antar etnis, aktivitas kriminal penjahat, perusakan fasilitas umum, dan lain sebagainya;

3. Ancaman terhadap Pemerintah – kudeta berdarah, revolusi inskonstitusional, pembunuhan pejabat negara, dan lain sebagainya; dan

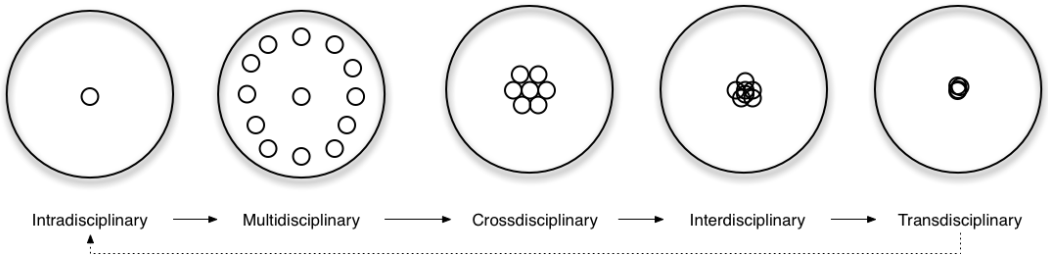
4. Ancaman terhadap Pengakuan Negara Lain – isu separatisme, kasus pelanggaran sumber daya manusia, tuntutan referendum, dan lain sebagainya.

Sebagaimana tubuh manusia yang selalu berusaha bertahan dari serangan berbagai benda asing semacam bakteri atau virus, negara pun memiliki “sistem antibodi”-nya tersendiri, yang diperoleh melalui proses dan aktivitas terencana, maupun dari hasil pertumbuhan organiknya melalui berbagai peristiwa yang terjadi semenjak negara tersebut berdiri.

Oleh karena itulah maka espitemologi ilmu pertahanan sarat dengan berbagai teori, konsep, paradigma, strategi, dan prosedur - yang diperoleh melalui berbagai kajian, pengalaman, dan penelitian secara kualitatif maupun kuantitatif – yang berkaitan dengan seni dan teknik mempertahankan sebuah negara. Lahir daripadanya berbagai artefak ilmu pengetahuan seperti strategi militer, prinsip dalam berperang, pendekatan mempertahankan negara, teknik mengelabui musuh, dan lain sebagainya.

Aspek aksiologi dari ilmu pertahanan pada dasarnya adalah untuk membantu negara dalam merumuskan strategi dan kebijakan pertahanan yang tepat. Mengembangkan atau menyusun aturan maupun strategi tanpa dilandasi oleh ilmu pengetahuan yang mumpuni, tidak saja akan berakibat rendahnya efektivitas implementasinya, namun justru dapat berpotensi menimbulkan kerentanan terhadap sistem pertahanan itu sendiri. Oleh karena itulah maka ilmu pertahanan harus dipergunakan dalam merancang, mengorganisasikan, mengelola, mengeksekusi, dan mengendalikan berbagai sistem pertahanan dan keamanan dalam ekosistem berbangsa dan bernegara. Ada dua aliran besar pandangan para ilmuwan (baca: *scholars*) terkait dengan kedudukan pertahanan dalam rumpun ilmu pengetahuan. Aliran pertama adalah yang menganggap pertahanan sebagai sebuah sub-ilmu tersendiri, yang merupakan turunan dari ilmu lain yang telah ada sebelumnya, seperti ilmu sosial, teknik, manajemen, pemerintahan, ekonomi, maupun psikologi. Pandangan ini menganggap pertahanan sebagai sebuah *intradisciplinary knowledge.* Sementara aliran kedua yang menganggap ilmu pertahanan merupakan konvergensi dari sejumlah ilmu lain dalam tingkatan keterhubungan yang berbeda, sehingga memiliki tiga

domain, yaitu: (i) multi-disiplin; (ii) lintas-disiplin; (iii) inter-disiplin; dan (iii) multi-disiplin.



Gambar 2. 1 Perbedaan antara Berbagai Relasi Rumpun Keilmuan

Sumber : Perbedaan antara Berbagai Relasi Rumpun Keilmuan (Zeigler, 1990)

Gambar di atas memperlihatkan bagaimana tahapan konvergensi dari yang paling rendah dan bersifat sporadis yaitu multi-disiplin, hingga yang paling tinggi tingkat keterhubungannya, yaitu trans-disiplin. Adapun ilmu-ilmu yang saling berkaitan membentuk rumpun ilmu pertahanan adalah: manajemen, sosial, psikologi, budaya, teknik, sejarah, hukum, militer, ekonomi, hubungan internasional, komunikasi, dan seni.

Dengan beranggapan bahwa pertahanan merupakan sebuah ilmu bertahan dari berbagai serangan dari dalam dan luar negara, maka dunia siber yang tidak memiliki teritori dan batasan fisik geografis harus diletakkan pada posisi yang tepat. Cara pandang dalam menempatkan posisi dan peran siber dalam konteks ilmu pertahanan akan sangat berpengaruh terhadap berbagai aksi nyata berupa penyusunan kerangka, pembuatan strategi, maupun pengembangan kebijakan terkait dengan keberadaannya.

Pertahanan dalam Konteks Keamanan Nasional

Filosofi keamanan nasional bertumpu pada adanya ketertiban atau keteraturan dalam kehidupan berbangsa dan bernegara (baca: bermasyarakat). Situasi dan kondisi tersebut akan terjadi apabila segenap masyarakat hormat dan tunduk pada regulasi dan peraturan perundang-undangan yang berlaku. Oleh karena itulah maka dikenal sejumlah sub-sistem keamanan nasional yang berkaitan secara langsung terhadap ilmu pertahanan.

Pertama adalah *human security* yang merupakan tingkat keamanan paling mendasar, karena langsung menyentuh pada setiap individu dalam komunitas masyarakat sebuah negara. Berbagai tindakan yang mengganggu keamanan individu tentu saja akan berdampak pada komunitas di sekitarnya, yang jika tidak ditangani secara sungguh-sungguh akan menjalar menjadi ancaman yang lebih besar (Shani, 2017). Terjadinya kejahatan atau tindakan yang menimpa satu atau beberapa orang, jika tidak ditangani secara sungguh-sungguh akan berakibat pada ketidakamanan wilayah, karena akan semakin banyak aktivitas kriminal yang berpotensi terjadi dalam skala lebih luas (Chandler, 2012).

Kedua adalah *public security*, yang memiliki ruang lingkup keselamatan masyarakat umum. Fenomena terjadinya *riot* atau kerusuhan akibat berbagai hal tentu saja mencemaskan masyarakat dari beragam kalangan. Ketidakteraturan dan ketidakpatuhan pada aturan yang berlaku dalam kondisi semi *chaos* ini berpotensi membahayakan negara (Kapucu & Demirhan, 2019; Yin, 2020).

Ketiga adalah *infrastructure security* atau keamanan infrastruktur, yang menyangkut ketersediaan operasional fasilitas publik yang menguasai hajat hidup orang banyak seperti air, listrik, transportasi, internet, dan lain sebagainya (Cai, 2018; Setiyawan, 2019). Gangguan terhadap distribusi listrik yang dapat menyebabkan terjadinya *blackout* selama beberapa jam saja berpotensi membahayakan negara. Dapat dibayangkan berapa fasilitas militer yang terganggu ketika pasokan listrik putus selama beberapa jam. Serangan atau penetrasi musuh ke dalam teritori negara Indonesia dapat terjadi pada masa krisis tersebut (Bhardwaj et al., 2016).

Keempat adalah *territory security*, yang berkaitan dengan keamanan wilayah atau area geografis negara. Kasus pemberontakan atau terorirsme di sebuah daerah seperti Papua dan Aceh misalnya, secara langsung maupun tidak langsung berakibat terhadap keberlangsungan Negara Kesatuan Republik Indonesia (mengancam integrasi dan keutuhan negara) (Elden, 2007; Rose-Redwood, 2012).

Dan yang terakhir, kelima, adalah *state security*, yaitu keamanan penyelenggara negara, yaitu pemerintah dan mitra kerjanya (baca: lembaga eksekutif, legislatif, dan yudikatif). Gangguan secara langsung maupun tidak langsung terhadap institusi terkait akan memberikan pengaruh terhadap jalannya pemerintahan negara, yang berakibat pada terjadinya gangguan di sana sini (Hama, 2017; Pepping et al., 2015). Demonstrasi masyarakat terhadap parlemen, mosi tidak percaya kepada presiden, melawan keputusan Mahkamah Agung, walaupun konstitusional, jika tidak dikelola secara baik dan benar, berpotensi menimbulkan gangguan pada level nasional.

Menghadapi seluruh potensi gangguan atau ancaman keamanan tersebut, ilmu pertahanan sangatlah diperlukan, dengan sejumlah pertimbangan antara lain sebagai berikut:

1. Setiap peristiwa gangguan yang terjadi harus ditanggapi dengan aksi yang tepat, cepat, dan efektif sehingga dibutuhkan metoda untuk menilai suatu situasi dan kondisi agar ditemukan intervensi penanganan yang benar.

2. Setiap potensi ancaman atau risiko yang ada perlu dipetakan dan dicegah agar tidak terjadi, tentu saja diperlukan model analisa yang tepat untuk menentukan strategi mitigasinya.

Dalam kondisi normal ketika tidak terjadi peristiwa yang mengganggu keamanan, kestabilan, dan kedaulatan negara, ilmu pertahanan pun diperlukan untuk mencegah terjadinya berbagai hal yang tidak diinginkan, baik secara teknis maupun psikologis, seperti:

1. Mengembangkan strategi pertahanan dan keamanan yang sesuai dengan karakteristik negara kepulauan *(archipelago continent)* sehingga menghadirkan efek *deterrent* yang diharapkan (Hidayat & Ridwan, 2017);

2. Mengelola sumber daya pertahanan dan keamanan yang ada di dalam wilayah NKRI secara efektif, efisien, dan terkendali (Sebastian, 2018);

3. Memajukan industri teknologi pertahanan yang handal di dalam negeri, sehingga terciptalah berbagai alutsista dan persenjataan yang canggih (Fitri & Sanur, 2019);

4. Mempersiapkan sumber daya manusia yang kompeten, terampil, dan ahli di bidang pertahanan sesuai dengan kemajuan dan dinamika perkembangan jaman (Anwar, 2018; Sebastian, 2018); dan lain sebagainya.

Oleh karena itulah maka ilmu pertahanan memegang peranan krusial dalam konteks penyelenggaraan sistem keamanan nasional di Indonesia.

Konsep keamanan nasional secara tradisional menyatakan bahwa keamanan pada dasarnya adalah kondisi bebas dari ancaman, rasa takut, dan bahaya. Sesuatu dianggap dalam kondisi aman apabila berada dalam dua kondisi. Pertama adalah ketika tidak ada apapun yang mengancam properti bernilai yang dimilikinya. Dan kedua, seandainya ancaman tersebut ada, yang bersangkutan tetap merasa aman apabila mampu mempertahankan dirinya dari bahaya tersebut dengan biaya yang masuk akal (sesuai dengannya). Konsepsi mengenai keamanan nasional dalam pandangan konvensional atau tradisional terdiri dari lima dimensi (Bajoghli, 2019; Geers, 2010).

Dimensi pertama adalah *The Origin of Threats* atau Asal Muasal Ancaman. Ancaman terhadap keamanan nasional berasal dari negara lain, terutama yang tidak puas dengan kondisi *status quo* yang dialami. Kebanyakan ancaman berasal dari negara tetangga, karena adanya godaan dan peluang untuk mempermasalahkan masalah klasik seperti isu perbatasan, etnis, sejarah,

dan nasionalisme. Atau adanya situasi lain yang dapat diangkat dan menarik bagi dunia internasional, seperti masalah sumber daya alam, kebijakan ekonomi, pengungsian, dan lain sebagainya.

Dimensi kedua adalah *The Nature of Threats* atau Karakteristik dari Ancaman. Secara tradisional, ancaman yang dimaksud tidak lain adalah agresi militer yang dilakukan terhadap negara. Namun karena relatif sult mengukur kapabilitas menyerang (*offense*) dan bertahan (*defense*) yang dimiliki negara tetangga di sekitar, maka ancaman tersebut dianggap berada pada level potensial. Seandainya negara tetangga disinyalir memiliki kemampuan atau kapabilitas menyerang yang lebih tinggi, maka potensi ancaman tersebut perlu diperkecil atau diimbangi dengan cara menjalin aliansi dengan musuh mereka.

Dimensi ketiga adalah *The Response* atau Tindakan Jawaban (Respon). Cara menjawab atau merespon balik terhadap berbagai ancaman tradisional berbasis militer yang membayangi adalah melawan dengan menggunakan perspektif militer pula. Misalnya adalah dengan meningkatkan efek gentar dengan meningkatkan kemampuan bersenjata, atau memobilisasi pasukan besar-besaran ke daerah perbatasan sebagai *show-of-force*, atau membangun aliansi dengan negara kuat yang berseberangan dengan mereka (musuh potensial).

Dimensi keempat adalah *The Responsible for Providing Security* atau Tanggung Jawab Pemberian/Penyediaan Keamanan. Mengingat tidak adanya sebuah lembaga super terpercaya yang dapat menjamin keamanan negara-negara, setiap negara bertanggung jawab untuk mengamankan wilayahnya masing-masing. Oleh karena itulah maka setiap negara harus memiliki kemampuan mandiri dalam mengembangkan sistem keamanan dirinya.

Dimensi kelima adalah *Core Values for the Defense* dimana sebuah negara senantiasa siap untuk berperang untuk mempertahankan kedaulatannya, menjaga wilayah negaranya, mempertahankan kemerdekaannya, memastikan integritas teritorial, dan melawan berbagai jenis intervensi yang dilakukan pihak lain terhadapnya.

Kelima dimensi tradisional ini memperlihatkan bahwa pada masanya dulu, karakteristik perang lebih didominasi dengan tindakan agresi militer secara fisik. Sangat berbeda dengan yang terjadi pasca perang dingin, dimana konflik antar berbagai negara lebih banyak terjadi secara non-militer, seperti dalam konteks: persaingan ekonomi, perdagangan narkoba, pelanggaran hak asasi manusia, penyerangan siber, dan lain sebagainya.

Pemahaman yang tepat akan apa yang dimaksud dengan pertahanan negara dan keamanan nasional akan menjadi pisau analis yang tajam ketika berbicara mengenai ancaman dan serangan siber. Walaupun bersifat tidak kasat mata, namun fenomena serangan yang terjadi belakangan ini dalam wilayah NKRI telah terbukti memberikan dampak negatif yang luar biasa terhadap keutuhan hidup berbangsa dan bernegara, termasuk menciptakan ancaman yang lebih besar dalam bentuk disintegrasi bangsa.

Pendekatan Kesisteman Sektor Pertahanan

Sektor pertahanan di Indonesia berkembang dari masa ke masa sejalan dengan sejarah perjalanan bangsa. Berbasis pada ekosistem sektor pertahanan, dapat dikembangkan kerangka konseptual mengenai berbagai elemen-elemen pembentuknya sebagaimana terlihat pada diagram berikut. Adapun penjelasan ringkasnya adalah sebagai berikut:

1. Dalam menetapkan sistem pertahanan negara, Indonesia mengadopsi model Taylor yang membagi ekosistem menjadi tiga domain utama, yaitu (Erbel & Kinsey, 2018; Milevski, 2016):

    1. *Ends*, adalah tujuan yang ingin diraih dari adanya sebuah kebijakan. Rumusan tujuan kebijakan ini ditentukan oleh banyak faktor, baik internal maupun eksternal dalam sebuah negara.

    2. *Ways*, adalah cara atau strategi yang dipilih untuk mencapai hasil akhir yang didefinisikan oleh kebijakan dimaksud. Ada

berbagai pilihan yang tersedia, sehingga harus dilakukan tahapan sistematis dan metodologis untuk mendapatkan strategi terbaik.

3. *Means*, adalah berbagai sumber daya yang dimiliki oleh pemilik/pembuat kebijakan, yang dipakai sebagai entitas atau aset berdasarkan strategi yang dipilih. Keberaaan, pemilihan, dan pengerahan dari sumber daya ini sangat tergantung dari rumusan strategi yang diambil.

1. Pada domain *Ends* terdapat sejumlah komponen utama, yaitu:

    1. Visi, misi, dan tujuan nasional dari Indonesia;

    2. Konstitusi atau undang-undang tertinggi negara yang di dalamnya terdapat falsafah atau ideologi bangsa yang melandasi kehidupan bernegara seluruh masyarakat untuk menerapkan visi, misi, dan tujuan nasional yang dicanangkan, yang dalam konteks NKRI adalah Pancasila dan UUD 1945;

    3. Doktrin pertahanan negara yang dianut berdasarkan tujuan, konstitusi, dan falsafah negara;

    4. Sejumlah produk strategis pertahanan negara sebagai pengejawantahan doktir pertahanan negara yang ditetapkan;

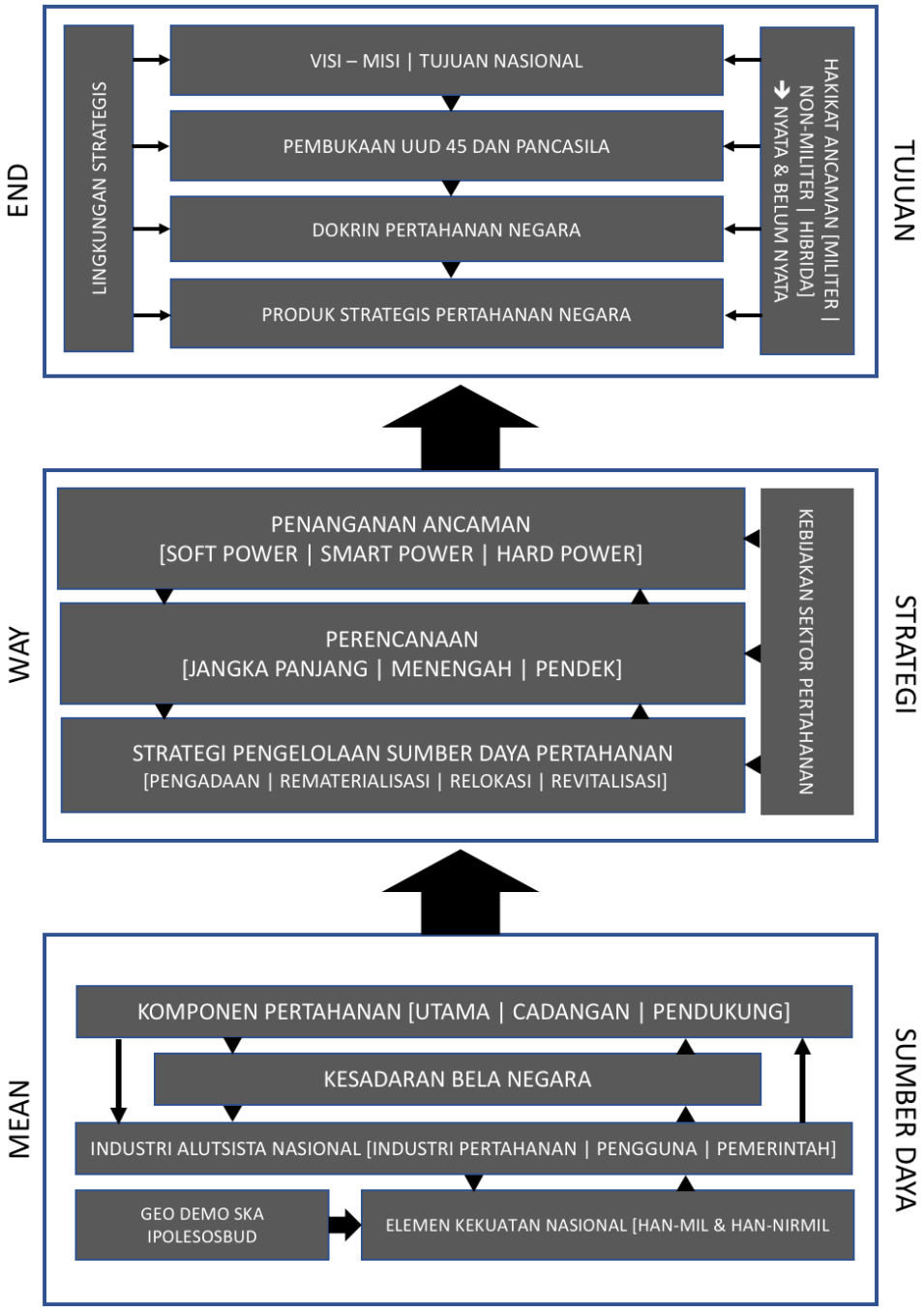
    5. Lingkungan strategis bangsa secara geopolitik dan geostrategi yang berpengaruh terhadap keempat elemen di atas; dan

    6. Profil ancaman militer, non-militer, dan hibrid yang secara dinamis membayangi negara.

1. Pada domain *Ways* yang merupakan cara mencapai tujuan terdapat sejumlah komponen penting, yaitu:

1. Strategi penanganan ancaman yang diidentifikasikan, baik melalui pendekatan *soft power, hard power,* maupun *smart power*;
2. Perencanaan strategis jangka panjang, jangka menengah, dan jangka pendek;
3. Strategi pengelolaan sumber daya pertahanan, berupa siklus manajerial yaitu pengadaan, rematerialisasi, relokasi, dan revitalisasi; dan
4. Sejumlah kebijakan agar secara konstitusional ketiga hal di atas dapat menjadi program pemerintah.

1. Pada domain *Means* yang merupakan sumber daya strategis yang dimiliki oleh bangsa dan negara memiliki sejumlah elemen, yaitu:
    1. Komponen pertahanan, yang terdiri dari komponen utama, kemudian komponen cadangan, dan komponen pendukung;
    2. Konsepsi program bela negara yang merupakan bentuk *soft defense* yang harus menjadi semangat seluruh warganegara dalam bingkai patrotisme dan nasionalisme yang tinggi;
    3. Industri alutsista nasional yang merupakan tambahan potensi kekuatan pertahanan nasional;
    4. Kondisi negara yang sangat strategis dengan berbagai kekayaan alam terbarukan maupun tak terbarukan yang dimilikinya – termasuk modal ideologi, politik, sosial, budaya, dan ekonomi yang lahir bersamanya; dan
    5. Seluruh elemen kekuatan nasional yang terkandung dalam bumi negara dalam bentuk fisik maupun aset *intangible* yang dimilikinya.


END
TUJUAN
LINGKUNGAN STRATEGIS
VISI – MISI | TUJUAN NASIONAL
PEMBUKAAN UUD 45 DAN PANCASILA
DOKRIN PERTAHANAN NEGARA
PRODUK STRATEGIS PERTAHANAN NEGARA
HAKIKAT ANCAMAN [MILITER | NON-MILITER | HIBRIDA]
NYATA & BELUM NYATA
WAY
STRATEGI
PENANGANAN ANCAMAN
[SOFT POWER | SMART POWER | HARD POWER]
PERENCANAAN
[JANGKA PANJANG | MENENGAH | PENDEK]
STRATEGI PENGELOLAAN SUMBER DAYA PERTAHANAN
[PENGADAAN | REMATERIALISASI | RELOKASI | REVITALISASI]
KEBIJAKAN SEKTOR PERTAHANAN
MEAN
SUMBER DAYA
KOMPONEN PERTAHANAN [UTAMA | CADANGAN | PENDUKUNG]
KESADARAN BELA NEGARA
INDUSTRI ALUTSISTA NASIONAL [INDUSTRI PERTAHANAN | PENGGUNA | PEMERINTAH]
GEO DEMO SKA IPOLESOSBUD
ELEMEN KEKUATAN NASIONAL [HAN-MIL & HAN-NIRMIL

Gambar 2. 2 Kerangka Sistem Sektor Pertahanan Negara

Sumber : Kerangka Sistem Sektor Pertahanan Negara

(hasil pengembangan peneliti pada kajian terdahulu)

Strategi dan Pengembangan Kebijakan

Secara etimologi, kata strategi pada dasarnya berasal dari bahasa Yunani yaitu “strategos”. Kata tersebut pada zaman demokrasi Athena dahulu dapat dikatakan sebagai “komandan militer”. Berikut ini adalah sejumlah definisi strategi dari berbagai ahli:

1. Carl Von Clausewitz: “Stategi adalah suatu pengetahuan terhadap penggunaan pertempuran agar dapat memenangkan sebuah peperangan. Dan perang itu sendiri adalah kelanjutan dari politik.”

2. Scholes dan Johnson: “Strategi merupakan arah dan ruang lingkup dari organisasi atau lembaga dalam jangka panjang. Yang mencapai keuntungan melalui konfigurasi dari sumber daya dalam lingkungan, untuk memenuhi kebutuhan atau kepentingan tertentu.”

3. Syafrizal**: “**Strategi merupakan suatu cara untuk dapat mencapai tujuan berdasarkan analisa terhadap faktor internal dan eksternal.”

4. Rangkuti: “Strategi merupakan alat untuk mencapai suatu tujuan tertentu.”

5. Andrews: “Strategi adalah pola sasaran, tujuan, serta kebijakan/rencana umum untuk meraih tujuan yang telah atau sudah ditetapkan.”

6. Craig and Grant: “Strategi adalah penetapan tujuan dan sasaran dalam jangka panjang.”

7. Kaplan and Norton: “Strategi adalah seperangkat hipothesis yang dapat diekspresikan dalam hubungan sebab-akibat.”

8. Hamel and Prahalad: “Strategi adalah tindakan yang bersifat inkremental dan terus-menerus, serta dilakukan berdasarkan sudut pandang tentang apa yang diharapkan di masa depan.”

9. David: “Strategi adalah sarana bersama dengan tujuan jangka panjang yang hendak dicapai.”

Sementara kamus besar Bahasa Indonesia mendefinisikannya sebagai “ilmu dan seni menggunakan semua sumber daya bangsa untuk melaksanakan kebijaksanaan tertentu dalam perang dan damai.” KBBI ini juga mengkonfirmasi bagaimana sejarah kata strategi ini berasal dari kalangan militer, sehingga dalam definisi alternatifnya didefinisikan pula sebagai “ilmu dan seni memimpin bala tentara untuk menghadapi musuh dalam perang.”

Terlepas dari begitu banyak definisi yang dikenal, dapat diambil kesimpulan bahwa pada dasarnya strategi adalah sebuah ilmu dan/atau seni untuk mencapai suatu tujuan melalui pengelolaan sumber daya yang dimiliki. Strategi haruslah dirumuskan, diterapkan, diawasi, dinilai, dan dikembangkan. Pada tahapan perumusan, perlu dilakukan sejumlah aktivitas, seperti: mengidentifikasikan lingkungan sekitar, melakukan analisis faktor internal dan eksternal, merumuskan faktor-faktor keberhasilan, menentukan tujuan dan target, serta memilih skenario yang paling sesuai. Sementara dalam tahap penerapan, dilaksanakanlah seluruh program dan kegiatan yang telah dirumuskan sebelumnya, dalam bentuk: penciptaan value bagi yang berkepentingan (stakeholders), pengembangan budaya yang suportif, penyiapan anggaran, pengerahan dan mobilisasi sumber daya, dan pengendalian implementasi di lapangan. Setelah itu adalah tahap pengawasan, menyangkut berbagai proses seperti: pemberian asistensi, pelaksanaan kontrol/kendali, pendampingan usaha, dan lain sebagainya. Pada tahap selanjutnya yaitu penilaian, dilakukanlah proses pengukuran kinerja, evaluasi, dan pengambilan langkah korektif demi kinerja yang lebih baik. Dan pada tahap pengembangan adalah menyesuaikan strategi secara fleksibel sesuai dengan perubahan dinamika lingkungan yang bergerak secara cepat.

Strategi pengembangan kebijakan pada dasarnya bertujuan untuk mencari cara yang paling tepat dalam menyusun kebijakan mengingat adanya sejumlah tantangan karakteristik sebagai berikut:

1. Tingginya dinamika lingkungan internal dan eksternal sehingga membutuhkan model kebijakan yang *agile*, dalam arti kata dapat secara cepat atau fleksibel diubah menyesuaikan perkembangan jaman;
2. Berkembangnya teknologi secara sangat cepat sehingga menyulitkan regulator dalam membuat kebijakan yang senantiasa relevan dengan situasi dan kondisi yang bergerak terus;
3. Begitu banyaknya *stakeholder* atau pemangku kepentingan yang terlibat secara langsung maupun tidak langsung dalam proses atau akibat dari pembuatan kebijakan tertentu;
4. Banyaknya dan kompleksnya komponen yang diatur dalam kebijakan dimana satu dan lainnya memiliki hubungan inter-relasi yang sangat erat; dan
5. Tingkat keterhubungan dengan kebijakan lain yang relatif tinggi, karena merupakan sub-sistem yang tidak berada di ruang hampa.

Perang dalam Doktrin Pertahanan Negara

Sebagaimana diketahui bersama, doktrin peran Indonesia adalah "Bangsa yang cinta damai, tapi lebih mencintai kemerdekaan". Dalam bingkai perspektif teori perang, doktrin ini mengandung makna sebagai berikut (Arvianissa & Fitriani, 2018):

1. Sejauh mungkin bangsa Indonesia akan menghindari perang apabila tersedia berbagai alternatif lain untuk menyelesaikan konflik, seperti: negosiasi, diplomasi, perjanjian bilateral, dan lain sebagainya. Prinsip *"war itself is not inevitable"* menjadi pegangan dalam menjalankan peran ini. Namun apabila pihak yang berkonflik dengan Indonesia tetap memaksakan kehendaknya untuk menuju ke arah konflik lebih jauh (baca: perang) yang

berpotensi mengganggu kemandirian dan kedaulatan negara (baca: kemerdekaan), maka bangsa Indonesia tidak segan-segan untuk maju ke medan tempur.

2. Konsepsi politik luar negeri yang “bebas aktif” juga sejalan dengan prinsip di atas, dimana Indonesia secara aktif berperan untuk mewujudkan perdamaian dunia melalui berbagai perannya yang tidak tergantung pada kehendak atau perintah negara-negara lain di dunia. Indonesia menentang segala bentuk penjajahan di muka bumi, sehingga walaupun mengutamakan kedamaian, sebagai bangsa Indonesia siap berperan jika terdapat agresi aktif dari negara lain ke NKRI yang mengancam keutuhan dan kedaulatan bangsa.

Dilihat dari kacamata teori konflik, perilaku permusuhan dapat terlihat dalam fenomena sebagai berikut:

1. Adanya pernyataan atau perilaku yang bersifat ancaman dari satu pihak ke pihak lainnya dalam berbagai bentuk aksi atau tindakan. Dalam konteks kenegaraan, pernyataan ancaman yang dimaksud misalnya adalah menakut-nakuti akan dilakukannya embargo ekonomi jika suatu permintaan tak terpenuhi, atau akan adanya agresi militer jika kondisi tertentu tidak ditaati, atau akan dipergunakannya senjata militer jika terjadi situasi yang tak diinginkan, dan lain sebagainya (Toprak, 2019). Sementara ancaman yang bersifat tindakan non-kekerasan fisik antara lain adalah menyandera kapal negara lain di pelabuhan, dikuasai atau diambilalihnya aset negara lain secara paksa, masuk ke wilayah teritori perairan negara lain (Fallon, 2015), dan lain sebagainya.

2. Adanya perilaku irasional yang mengemuka dari satu pihak dimana membuat pihak lain merasa terpojok karena ulahnya. Perilaku irasional timbul biasanya apabila sang pimpinan suatu negara dilanda emosi yang tak terkendali, sehingga membuat keputusan yang tak masuk akal dan membawa permusuhan. Misalnya adalah memerintahkan seluruh warga negara untuk

keluar dari wilayah tertentu, membangun tembok pemisah berpagar tinggi di daerah perbatasan yang dilengkapi pengaman listrik tegangan tinggi (Dorsey & Diaz-Barriga, 2010; Macias et al., 2020), dan lain sebagainya.

3. Adanya tindakan kekerasan fisik secara langsung yang diperlihatkan satu pihak ke pihak lainnya. Perbuatan dimaksud misalnya adalah pembunuhan warga negara dengan ras atau etnis tertentu (Gordon & Ram, 2016; Hägerdal, 2019), penyiksaan para individu yang dituduh mata-mata negara lain, pengambilalihan wilayah sengketa secara sepihak, dan lain sebagainya.
4. Adanya sinyal-sinyal yang senantiasa terkesan mencari-cari kesalahan oleh pihak satu terhadap pihak lainnya, dan keenganan untuk menjalin hubungan yang harmonis di antara keduanya. Misalnya adalah permusuhan abadi antara dua ras, aliran, atau ideologi tertentu (dengan berbagai alasan rasional maupun irasional) (Crow, 2015; Leader Maynard, 2019), konflik perbatasan yang tak kunjung usai, dan lain sebagainya.

Dipandang dari perspektif teori konflik, signal permusuhan sebagaimana dicontohkan di atas cenderung memiliki karakteristik sebagai berikut (Chappelow, 2019):

1. Bersifat *“coercive action”* atau sebuah perilaku aktif yang bernuansa memaksakan kehendak dari satu pihak ke pihak yang lain;
2. Terdapat ketidakseimbangan kekuatan antar pihak, sehingga pihak yang (merasa) lebih kuat cenderung berinisiatif mengeluarkan sinyal permusuhan terlebih dahulu; dan
3. Disinyalir memiliki intensi atau motivasi yang tidak mengarah pada keinginan untuk menyelesaikan masalah dengan damai sehingga sinyal-sinyal permusuhan tetap diperlihatkan.

Permusuhan itu sendiri dapat disebabkan karena berbagai pemicu, baik yang bersifat historis maupun berbasis kondisi termutakhir yang berkembang, seperti:

1. Permusuhan karena adanya kepentingan dua atau beberapa negara yang saling bertolak belakang, misalnya karena alasan ekonomi (perebutan aset strategis), politik (perselisihan kekuasaan), sosial (pertikaian antar aliran), budaya (peristiwa masa lalu), dan lain sebagainya (von Billerbeck & Gippert, 2017);
2. Permusuhan karena adanya skenario tertentu yang dipicu oleh sebuah intensi atau motivasi khusus dimana akan ada pihak yang merasa dirugikan karena ketidaksinkronan obyektif antara sejumlah pihak, seperti: niat menguasai wilayah tertentu yang bukan menjadi haknya, gerakan menyebarkan aliran (baca: -isme) yang tidak sesuai dengan nilai-nilai di masyarakat, pemboikotan hubungan bilateral atau multilateral dalam berbagai bentuk, dan lain sebagainya (Christian, 2015); dan
3. Permusuhan karena adanya pihak ketiga yang melakukan politik adu domba dengan melancarkan perang *proxy*, dengan menggunakan instrumen moderen berbasis siber dan teknologi informasi, seperti *hoax*, disinformasi, misinformasi, serangan siber, dan lain-lain (Marshall, 2016; Nastiti et al., 2018).

Konsep tradisional mengenai keamanan cukup jelas, yaitu kondisi bebas dari ancaman, ketakutan, dan bahaya (Shvindina, 2019). Suatu entitas dikatakan dalam keadaan aman apabilia dua kondisi terpenuhi, yaitu: (i) tidak adanya pihak yang menjadi ancaman terhadap aset berharga atau bernilai yang dimiliki entitas terkait; dan (ii) seandainya adapun, entitas yang bersangkutan memiliki kemampuan atau kapabilitas melindungi diri dari bahaya yang mengancam tersebut dengan menggunakan biaya yang sepadan dengannya. Dalam konteks keamanan nasional, konsepsi yang ada memiliki 5 komponen penting, yaitu:

1. Sumber ancaman – bisa berasal dari negara lain, atau aktor lain non-negara seperti gerakan, etnis, komunitas, aliran, dan lain-lain;
2. Karakteristik ancaman – dimana ada yang bersifat ancaman militer, maupun non-militer, seperti: serangan siber, sabotase infrastruktur strategis, pemberontakan/separatisme lokal, dan lain sebagainya;
3. Sikap antisipasi dan penanggulangan ancaman – dapat dilakukan dengan gelar pasukan dan senjata, maupun teknik lainnya seperti diplomasi, negosiasi, perjanjian bilateral, dan lain-lain;
4. Tanggung jawab layanan keamanan – strategi negara dalam menyediakan infrastruktur dan suprastruktur untuk menjaga keamanan masyarakat dan sumber daya yang dimilikinya; dan
5. Nilai dan entitas berharga/bernilai negara – yang harus dipertahankan mati-matian karena merupakan kunci dari keutuhan, kedaulatan, dan kemerdekaan segenap bangsa dan negara.

Tabel di bawah ini memperlihatkan perbedaan karakteristik dari kelima komponen tersebut di masa perang dingin masa lalu, dan pasca perang dingin. Terlihat dalam masa moderen, perang lebih bersifat non-militer, yang melibatkan kebanyakan aktor non-negara, dimana penyelesaiannya diserahkan kepada kondisi global, melibatkan banyak negara, sebagai jawaban untuk melindungi nilai-nilai kemanusiaan dan kesejahteraan masyarakat.

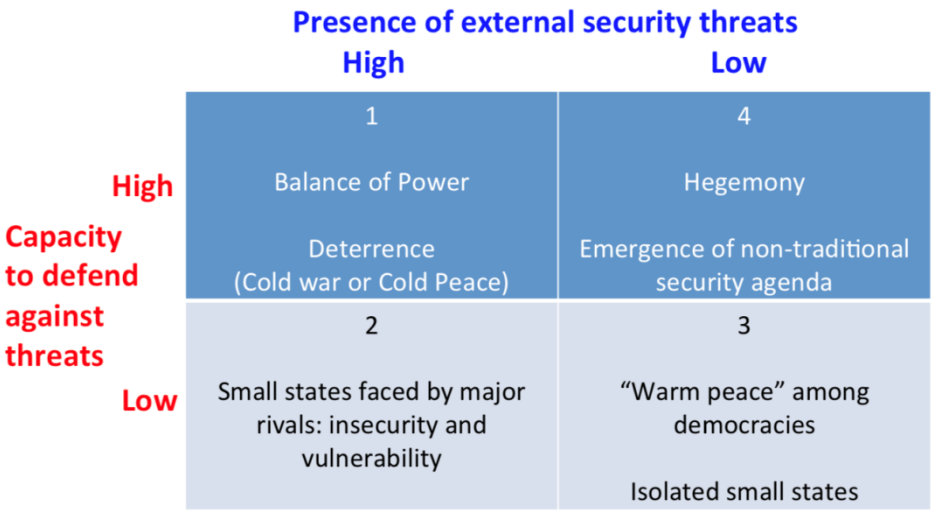
Tabel 2. 2 Perbandingan Karakteristik Perang Dingin dan Pasca Perang Dingin

Traditional		Post-Cold War
Origin of threats	Rival states (neighbors/great powers)	Nonstate: domestic /trnsboroder The state versus its citizens
Nature of threats	Military capabilities	Nonmilitary: economic, domestic, political. Transnational/global (Immigration drugs, diseases, environment, proliferation of WMD, crime, terrorism)
The Responses	Military (arms and alliance)	Nonmilitary: free/global markets, democratization, state-building.
The Rensponsibility for providing security	The State	International institutions, multilateral interventions

Sumber : Perbandingan Karakteristik Perang Dingin dan Pasca Perang Dingin

(Cha, 2002)

Berpedoman pada keseluruhan penjelasan di atas, maka dapat dilihat bahwa tingkat keamanan sebuah negara sangat tergantung pada dua hal utama, yaitu: (i) besarnya keberadaan ancaman eksternal yang mengintip negara terkait; dan (ii) kapabilitas, kapasitas, serta kemampuan negara tersebut dalam mempertahankan diri terhadap ancaman yang ada. Kedua aspek ini dapat digambarkan dalam sebuah matriks 2x2 yang membagi tingkat keamanan menjadi 4 (empat) level atau kuadran, sebagaimana terlihat dari gambar sebagai berikut.



Gambar 2. 3 Matriks Tingkatan Keamanan Negara

Sumber : Matriks Tingkatan Keamanan Negara

(Herbst et al., 2017; Wohlforth et al., 2007; Wu, 2018)

Situasi 1: “Negara menghadapi tingginya ancaman eksternal dari luar wilayahnya, pada saat yang sama negara memiliki kemampuan untuk mempertahankan diri dengan biaya yang sepadan dengannya”.

Situasi ini menghasilkan kondisi *“balance of power”* karena adanya kemampuan penangkalan (baca: *deterrence*) yang baik, dimana dalam penerapannya akan bermanifestasi menjadi inisiatif pemutakhiran senjata militer (baca: lomba penguasaan senjata militer) untuk menghadapi berbagai kemungkinan terburuk dalam pertempuran (Herbst et al., 2017; Wohlforth et al., 2007; Wu, 2018). Walaupun kondisi peperangan nyata tidak terjadi, biasanya situasi semacam ini terlihat dalam ekosistem negara-negara maju yang memicu perang dingin.

Situasi 2: “Negara menghadapi tingginya ancaman eksternal dari luar wilayahnya, namun yang bersangkutan tidak memiliki kemampuan untuk mempertahankan dirinya seandainya terjadi serangan”.

Ini adalah kondisi buruk dan sangat mengkhawatirkan bagi sebuah negara, karena ketidakberdayaannya dalam menghadapi berbagai ancaman dan serangan dari luar. Ketidakmampuan ini bisa karena tidak memiliki sumber daya yang mencukupi, atau tidak memiliki mitra jejaring (baca: aliansi negara) yang dapat membela kepentingan mereka. Kondisi kerawanan ini dapat menyebabkan hilangnya kemandirian, kedaulatan, dan kemerdekaan negara tersebut jika terjadi serangan dari luar (J. Zhang & Pezeshkan, 2016).

Situasi 3: “Negara tidak memiliki atau tidak sedang menghadapi ancaman eksternal dari luar wilayahnya, walaupun pada kenyataannya yang bersangkutan tidak memiliki kemampuan untuk mempertahankan dirinya dari ancaman atau serangan yang terjadi”.

Kondisi seperti ini biasanya menerpa negara-negara kecil, yang tidak pernah berpikir akan menghadapi perang atau bentuk pertempuran apapun dalam kehidupannya. Negara yang kebanyakan merupakan pulau-pulau kecil ini senantiasa dalam keadaan dan kondisi damai, karena merupakan sebuah komunitas plural yang aman. Contohnya adalah negara semacam Andorra, Haiti, Grenada, Kiribati, Kepulauan Marshall, Dominica, dan Kosta Rika yang hingga kini tidak memiliki tentara di dalam wilayah teritorinya ("A Strategy for the Weaker Country in the Asymmetrical Military Alliance Alignment," 2020).

Situasi 4: "*Negara tidak memiliki atau tidak sedang menghadapi ancaman eksternal dari luar wilayahnya, namun memiliki kemampuan untuk mempertahankan dirinya dari ancaman atau serangan seandainya terjadi".*

Pada situasi seperti ini, terjadi kondisi hegemoni (Good, 2018). Ancaman bukanlah merupakan hal utama yang menjadi agenda pertahanan dari negara terkait. Namun ketika ada sedikit serangan, maka hal tersebut akan menjadi prioritas tertinggi dari negara yang cenderung cinta damai tersebut.

Keempat situasi berbeda tersebut akan sangat menentukan pengembangan strategi pertahanan dan keamanan negara yang tepat untuk diadopsi. Di masa moderen ini, sebuah negara dapat secara dinamis mengalami perpindahan kuadran situasi, karena berbagai fenomena relasi antar negara yang semakin beragam dan kompleks sifatnya.

Sejumlah teori ini memperlihatkan bahwa pada dasarnya untuk menciptakan strategi pertahanan yang efektif, harus dipergunakan doktrin pertahanan negara yang holistik dan komprehensif. Ranah siber harus memiliki tempat yang tepat di antara keberadaan wilayah darat, laut, dan udara yang menjadi garis-garis pembatas wilayah NKRI. Jika siber hanya dianggap sebagai sub-bagian dari sekedar alat, instrumen, media, atau arena tempat bermukimnya sejumlah ancaman non-militer semata maka negara akan gagal atau mengalami kesulitan dalam membangun strategi pertahanan siber yang ampuh dan handal.

Ancaman Teknologi Informasi dan Komunikasi

Perkembangan teknologi informasi dan informasi yang sedemikian cepat, telah melahirkan sebuah arena siber yang terbentuk karena adanya koneksi antara jutaan sumber daya komputasi di seluruh dunia. Bahkan penempatan sensor-sensor pada benda-benda fisik yang terhubung ke internet (baca: *internet-of-things)* telah melahirkan sebuah era revolusi baru yang diberi julukan *Cyber Physical System* yang mewarnai lahirnya era Revolusi Industri 4.0. Implementasi dan pemanfaatan teknologi internet dalam seluruh sektor kehidupan masyarakat seperti pendidikan, kesehatan, perdagangan, keuangan, transportasi, distribusi, manufaktur, pemerintahan, dan lain sebagainya (termasuk militer dan pertahanan) telah meningkatkan level ketergantungan manusia akan dunia siber (baca: *cyber dependency*). Internet adalah jejaring raksasa yang terbentuk dari terkoneksinya ribuan sistem sumber daya komputasi yang ada di bumi ini (Lilienthal & Ahmad, 2015a; Prinz et al., 2018; Wang et al., 2019). Arena virtual yang terbentuk dengan adanya jaringan internet ini diistilahkan sebagai “dunia siber”. Siber ini memiliki karakteristik yang sangat unik, yaitu (Denning, 2015):

1. *Social*, tempat bertemunya berbagai individu yang beragam untuk berkomunikasi, berinteraksi, dan berkolaborasi;
2. *Interactive*, terjadinya komunikasi multi-arah yang aktif antar mereka yang saling terhubung secara maya;
3. *Vulnerable*, rentan atau rawan terhadap beragam gangguan karena berkumpulnya pihak-pihak dengan kepentingan yang berbeda;
4. *Unregulated*, tidak adanya aturan baku atau pihak regulator yang memiliki otoritas mengatur lalu lintas data dan komunikasi yang terjadi;

5. *Anonymous*, kecenderungan tidak diketahuinya identitas beragam pihak yang berinteraksi dalam ekosistem internet;
6. *Global*, terbuka secara bebas bagi seluruh individu yang ada di planet bumi untuk ikut berinteraksi tanpa adanya hambatan;
7. *Dependent*, sangat tergantung dari ketersediaan dan kehandalan teknologi transmisi dan komputasi yang membentuk ekosistem internet;
8. *Insecure*, adanya perasaan tidak aman karena berinteraksi secara maya dengan pihak-pihak yang tidak dikenal;
9. *Uncontrollable*, tidak mungkin dikendalikan karena secara arsitektur dibangun oleh titik-titik *(nodes)* dan jaringan *(paths)* yang terhubung secara jamak *(mash);*
10. *Dynamic*, berkembang secara pesat karena semakin hari semakin banyak pihak yang bergabung dan layanan yang ditawarkan; dan
11. *Ubiquitous*, dapat diakses dengan berbagai piranti digital dari mana saja dan kapan saja.

Sejalan dengan meningkatnya manfaat internet bagi kehidupan manusia, pada saat yang sama tinggi pula risiko yang menyertainya. Nilai atau *value* dari internet dianggap semakin lama semakin tinggi karena adanya fenomena sebagai berikut:

1. Mengalirnya data dan informasi penting via internet, seperti: nomor kartu kredit, kata kunci atau *password* penting, nilai uang transfer, dokumen rahasia, informasi transaksi, *log file* peristiwa, dan lain sebagainya;
2. Menjamurnya *platform application* yang di dalamnya terdapat jutaan anggota dengan data detail mengenai profil, jati diri, preferensi, dan rekam jejak interaksinya;

3. Meningkatnya jumlah situs dan aplikasi perdagangan (*e-commerce*) yang memiliki volume serta frekuensi transaksi tinggi;

4. Membanjirnya situs-situs media sosial yang menghubungkan ribuan komunitas dan jutaan individu dari berbagai belahan dunia;

5. Memungkinkannya internet dipakai sebagai media untuk mengendalikan berbagai sistem atau sub-sistem digital, terutama yang berkaitan dengan teknologi *internet-of-things*;

6. Membludaknya jumlah data terstruktur maupun tidak terstruktur (*big data*) yang tersimpan di berbagai fasilitas komputasi; dan lain sebagainya.

Tentu saja tingginya *internet value* dan dunia siber ini menarik perhatian para kriminal dan penjahat dunia maya. Bagi mereka, melakukan tindakan kejahatan di siber memiliki sejumlah kelebihan dibandingkan dunia fisik, antara lain (Gawthorpe, 2016; Hathaway et al., 2012; Rahmawati, 2017): (i) tidak memerlukan biaya tinggi; (ii) besarnya potensi keuntungan atau hasil kejahatan; (iii) relatif mudah pelaksanaannya; (iv) cepat eksekusinya; dan (v) luas dampak atau eksposurnya.

Risiko terbesar yang dihadapi dunia siber adalah adanya gangguan. Secara prinsip, ribuan jenis serangan yang ada dapat digolongkan menjadi 4 (empat) kelompok, berdasarkan modus operandi dan tujuan yang ingin dicapai (Lilienthal & Ahmad, 2015a):

1. Intersepsi: berupa usaha untuk memperoleh data atau informasi rahasia dengan menggunakan beragam teknik penyadapan. Teknik semacam *spyware, sniffing, man-in-the-middle attack*, dan lain-lain sering dipakai sebagai instrumen dalam melakukan serangan berjenis ini.

2. Interupsi: gangguan terhadap layanan atau operasional suatu sistem karena adanya sejumlah serangan fisik maupun virtual, seperti: pemutusan jaringan *fiber optic*, serangan *botnet*, *malware, worms,* dan lain sebagainya.

3. Modifikasi: aktivitas mengubah data atau konten suatu pesan sehingga terjadi fenomena disinformasi atau misinformasi. Contoh-contoh jenis serangan ini antara lain adalah: *web defacement, SQL injection, trojan*, dan lain sebagainya.

4. Fabrikasi: teknik mengelabui seseorang atau pihak dengan cara menyamar menjadi institusi resmi (*official*), misalnya dengan cara: *phishing, social engineering,* dan lain sebagainya.

Peran maupun keberadaan komputer atau internet sendiri dapat beraneka ragam dalam konteks penyerangan seperti (Gunduz & Das, 2020; Lampson, 2004):

1. Internet dipergunakan sebagai medium untuk menyerang, dengan cara memanfaatkannya sebagai infrastuktur transmisi raksasa dan masif;

2. Internet dipergunakan sebagai alat untuk menyerang, dengan cara memakai sumber-sumber komputasi yang ada di dalamnya sebagai senjata ampuh untuk melumpuhkan berbagai sistem dan/atau mencuri data;

3. Internet sebagai target dari suatu penyerangan, karena dengan demikian maka sistem atau sub-sistem yang berada di dalamnya akan menjadi terganggu;

4. Internet sebagai arena tempat “pertempuran” terjadi, karena wilayah virtual ini dapat mempertemukan berbagai pihak yang memiliki beragam kepentingan berbeda; dan

5. Internet sebagai tempat bersembunyinya atau berinteraksinya para kriminal, terutama dengan adanya perimeter *darknet* dan *deepweb*.

Dengan memperhatikan berbagai fenomena di atas, maka dapat disimpulkan bahwa setiap institusi maupun sektor industri yang memiliki sistem berbasis digital atau internet akan berhadapan dengan beraneka ragam risiko,

seperti: risiko operasional, risiko organisasi, risiko reputasi, dan lain sebagainya (Ghafir et al., 2018; Wiśniewski, 2020). Dari seluruh potensi kejadian yang tidak diinginkan, yang paling ditakuti adalah jika gangguan tersebut berpotensi menimbulkan krisis. Contoh kejadian serangan terhadap siber di negara lain yang memicu terjadinya krisis nasional di bidang pertahanan adalah:

1. Serangan terhadap sistem pembangkit dan distribusi listrik yang mengakibatkan padamnya listrik di ibukota negara dalam waktu yang lama *(total blackout)* (Czosseck et al., 2011; Haataja, 2017);
2. Serangan terhadap instalasi nuklir yang dikendalikan dengan sistem digital sehingga membahayakan masyarakat di sekitarnya (Ahn et al., 2015; Kim et al., 2020);
3. Serangan terhadap persenjataan militer yang dapat berbalik diprogram untuk melumpuhkan negara pemiliknya (Eom et al., 2012);
4. Serangan terhadap sistem radar pesawat udara komersial, yang jika terjadi dapat membahayakan jiwa ribuan manusia (C. W. J. Poirier & Lotspeich, 2013; W. J. Poirier & Lotspeich Maj, 2013); dan lain sebagainya.

Serangan terhadap sistem atau sub-sistem ini jelas memiliki potensi memicu terjadinya krisis nasional, dalam arti kata terjadi situasi yang dapat membahayakan keselamatan, keutuhan, dan kedaulatan bangsa.

Ancaman siber terhadap sektor pertahanan negara pada dasarnya berbeda-beda di setiap konteks dan masa. Biasanya ancaman tersebut sesuai dengan tingkat kerawanan atau *vulnerabilities* yang dimiliki oleh sebuah negara. Dengan melakukan eksploitasi terhadap kelemahan tersebut, maka sebuah negara dapat diganggu bahkan dihancurkan eksistensinya melalui serangan yang efektif. Kasus yang terjadi di Mesir dan Tunisia memperlihatkan betapa dahsyatnya dampak serangan siber dari dalam dan luar negeri yang ditujukan padanya.

Karakteristik Dunia Siber

Siber adalah suatu arena atau domain jejaring interaksi yang terbentuk dari terkoneksinya jutaan komputer melalui sistem transmisi infrastruktur digital. Sejumlah kajian kolektif menyebutnya sebagai *cyberspace* yang memiliki ciri-ciri: sosial (kumpulan berbagai pihak dengan berbagai kepentingan), *virtual* (tidak terlihat secara kasat mata), interaktif (sarat aktivitas komunikasi antar entitas), *vulnerable* (rawan terhadap berbagai gangguan), *unregulated* (tidak teratur dan diatur), *anonymous* (tidak dikenal atau tidak ada yang memilikinya), *global* (lintas ruang dan waktu), *dependent* (terdiri dari sumber daya komputasi yang saling berhubungan), *insecure* (tidak aman), *unscale* (sangat tergantung keterbatasan teknologi pembentuknya), *elite* (monopoli aplikasi oleh beberapa vendor besar), *uncontrollable* (nir kendali), *dynamic* (senantiasa berkembang, *ubiquitous* (beragam cara untuk mengaksesnya), dan *discrete* (secara teknis tidak dapat dihancurkan) (Ministry of Defence, 2013; Mueller, 2019). Sejumlah pandangan membagi dunia siber menjadi tiga *layer*, masing-masing adalah: *near space, mid space,* dan *far space* (Rowland et al., 2014; Willett, 2019). Pembagian ini dipandang dari perspektif *cyberpower* atau kekuatan sebuah negara dalam mengendalikan jejaring siber yang fokus pada akses terhadap obyek vital dan infrastruktur kritis nasional.

Environment	Description
Near Space	Local networks and systems that are considered vital to support the critical national infrastructure and services, and are assumed to be controlled and protected by national or governmental agencies.
Mid Space	Networks and systems that are critical to access global cyberspace, but over which there is no local control or protection. Typically, these assets are geographically distant and are owned by foreign companies or third parties.
Far Space	Networks and systems that form the near space of a competitor or adversary, and must be influenced or controlled as part of a campaign to project power and influence in cyberspace.

Tabel 2. 3 Tiga Layer Cyber Space

Sumber : Tiga Layer Cyber Space (Rowland et al., 2014; Willett, 2019)

Kenyataan ini memperlihatkan bahwa tidak bisa memperlakukan dunia siber sebagaimana dunia fisik karena sifat dan karakteristiknya yang jauh berbeda. Jika dalam dunia fisik teritori sebuah negara jelas terlihat melalui batasan darat, laut, dan udara yang melekat padanya, dalam dunia siber hukum tersebut tidak berlaku karena eksistensinya yang lintas batas dan ruang.

Kerawanan Siber dan Pertahanan Negara

Dalam konteks pertahanan negara, siber memiliki peranan yang sangat penting, terutama dengan adanya beragam fenomena sebagai berikut (Chotimah et al., 2019; Sa'diyah & Vinata, 2016; Suratman, 2017; Sutrisno, 2016):

1. Perangkat komunikasi elektronik yang dipergunakan sehari-hari oleh personal TNI telah beralih ke teknologi digital, dimana koneksi antar piranti tersebut dilakukan melalui infrastruktur internet sebagai perwujudan dari dunia siber;

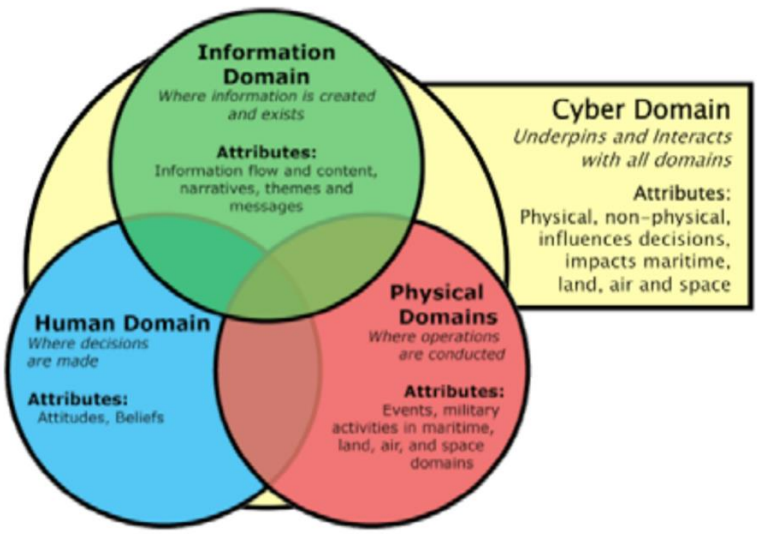
2. Alutsista moderen yang telah dilengkapi dengan fitur teknologi canggih berbasis digital yang saling terkoneksi satu dan lainnya via internet atau siber;

3. Data, informasi, dan pengetahuan yang dimiliki TNI merupakan artefak dalam bentuk *file* berformat digital yang disimpan, diorganisasikan, diakses, dan disebarluaskan melalui infrastruktur siber;

4. Frekuensi analog yang biasa dipergunakan dalam berbagai perangkat elektronik diubah dan ditransformasikan secara digital melalui jejaring siber;

5. Interaksi atau hubungan antar personal TNI untuk kebutuhan komunikasi, koordinasi, kooperaasi, dan kolaborasi dilakukan via siber dengan memanfaatkan berbagai perangkat *hardware*, *software*, dan aplikasi berbasis internet seperti *web,* media sosial, *teleconference,* dan lain-lain;

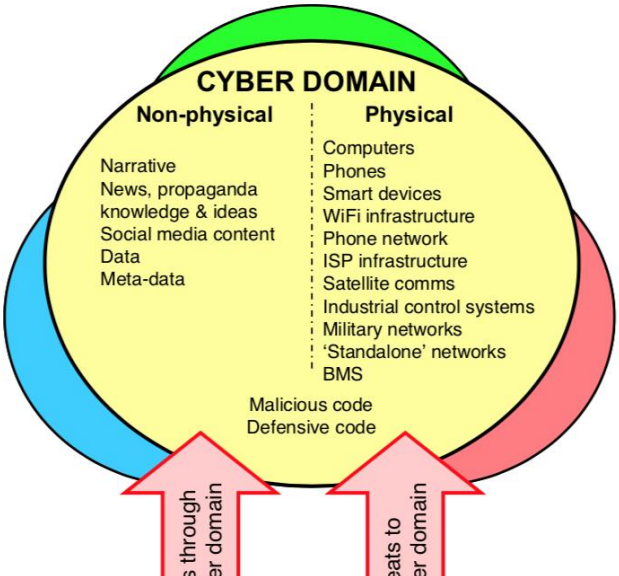
6. Fasilitas kendali dan *surveilans* seperti kamera pengawas, *command center*, *data center*, *access devices*, dan lain sebagainya merupakan teknologi digital yang dihubungkan melalui internet; dan contoh-contoh lainnya.



Gambar 2. 4 Hubungan Dunia Fisik dan Siber dalam Militer

Sumber : Hubungan Dunia Fisik dan Siber dalam Militer (Wardrop, 2015)

Mengingat karakteristik artefak digital yang rawan untuk dimanipulasi dan dunia siber yang melibatkan begitu banyak pemangku kepentingan, maka risiko terhadap banyaknya gangguan terhadap situasi pertahanan negara pun meningkat. Para ahli mengidentifikasi paling tidak ada tiga aktor yang kerap mengancam dunia siber, yaitu: *state actors, non-state actors,* dan *state proxies* (Sigholm, 2016). Mereka melakukan serangan siber terhadap aset atau sumber daya fisik (komputer, jaringan, satelit, sistem kendali, *chip*, dan lain-lain) maupun non-fisik (data, informasi, pengetahuan, konten, dan lain-lain). Lebih lanjut beragam studi memperlihatkan bagaimana berbagai serangan siber telah mampu melumpuhkan pertahanan sejumlah negara sebagaimana terjadi di Estonia, Saudi Arabia, Iran, Rusia, Chekoslovakia, Pakistan, dan sejumlah negara di daerah Timur Tengah maupun Eropa Timur. Berbagai perusahaan raksasa pun tak luput dari serangan siber yang masif terjadi, misalnya yang menimpa Microsoft, Google, Adobe, dan Sony Corporation (Kuehn, 2018; Mitchell & Zunnurhain, 2019)



an RI

Gambar 2. 5 Faktor Ancaman terhadap Dunia Siber (Wardrop, 2015)

Sumber : Faktor Ancaman terhadap Dunia Siber (Wardrop, 2015)

Dalam konteks pertahanan siber terlihat bahwa tidak ada negara yang dapat dikatakan aman dari berbagai ancaman serangan. Kenyataan memperlihatkan bagaimana negara adidaya seperti Amerika, Rusia, China, Inggris, Jepang, maupun Australia pernah dan masih mengalami serangan siber yang berdampak signifikan terhadap kedaulatan negara dan keamanan nasionalnya. Kerawanan pada sistem pertahanan siber adalah sebuah keniscayaan, sehingga harus dicari strategi mitigasi yang paling efektif dan optimum.

Aktivitas Militerisasi dalam Dunia Siber

Kasus pelumpuhan instalasi nuklir Iran oleh virus Stuxnet pada tahun 2010 menandai suatu era baru yang dikenal dengan istilah OCO atau *Offensive Cyber Operations.* Pada titik inilah doktrin pertahanan berbagai negara di dunia mengalami proses penyesuaian mengingat domain siber selama ini belum pernah menjadi variabel yang diperhitungkan (Cartin, 2014; Smeets, 2018).

Tabel 2. 4 Faktor Ancaman terhadap Dunia Siber (Wardrop, 2015)

State Interaction	Characteristics
Strong state versus superpower	• OCOs provide only marginal advantages and useful only for difficult to attribute attacks against civilian or military infrastructure • A superpower may perceive vulnerability in cyber-space and may not initiate aggression • OCOs act as a counter-force or counter-value weap-on against conventional capabilities
Weak state versus strong state/ superpower	• Weak state lacks the ability to follow through from the OCO with conventional attacks • Weaker state could launch OCOs against stronger adversary but is limited due to fear of possible escala-tion through conventional means • OCOs from strong state/superpower may not occur due to lack of targets in cyberspace
Weak state versus weak state	• Lack of conventional capabilities would shift conflict over to cyberspace • Limited conventional capabilities would limit esca-lation

Sumber : Faktor Ancaman terhadap Dunia Siber (Wardrop, 2015)

Kesadaran akan pentingnya mengelola dan mengendalikan dunia siber melahirkan berbagai artefak baru seperti strategi siber nasional dan lembaga yang bertanggung jawab atas peperangan berbasis siber atau yang biasa dikenal dengan *cyber war*. Dalam studi yang sama, ditemukan tiga entitas yang sangat

mempengaruhi aktivitas militerisasi dalam dunia siber, yaitu: (i) doktrin militer dan kebijakan terkait dunia siber; (ii) strategi keamanan siber nasional; dan (iii) unit militer atau non-militer yang terkait dengan *cyber defense* dan/atau *cyber offense*. Hasil riset menarik terkait karakteristik perang siber melibatkan tiga jenis negara, yaitu: *superpower*, negara kuat, dan negara lemah (Liff, 2013).

Brandes (2013) dalam studinya menggambarkan perbedaan mendasar dari perang tradisional dan perang siber. Aspek yang diperbandingkan masing-masing adalah: sumber daya, aset fisik, aktor, dampak, aktivitas penyerangan, dan dukungan intelijen.

Tabel 2. 5 Perbandingan Perang Konvensional dan Siber

Characteristic	Cyberspace Domain	Traditional Domains
Resources	• Inexpensive relative US air, land and sea • Human capital-driven	• Limited to nations with significant financial resources • Industrial-based assets
Physical	• Artificial construct, permeable virtual boundaries • Multi-use environment (government, military, commercial) • Distributed, dynamic and non-linear	• Exists naturally, discrete physical boundaries • Multi-use environment (government, military, commercial)
Actors	• Ambiguous • From nation-states to individuals to criminal organizations to commercial entities	• Identity of adversary usually known
Effects	• Global in nature • Non-Kinetic or Kinetic • Collateral damage on 2nd/3rd order effects potentially global	• Usually regionally focused (Space is exception) • Usually Kinetic (EW exception) • Collateral damage limited to active battlespace
Authorities for Offensive Action	• Elevated • Evolving ROE	• Local • Establish ROE
Intelligence Support	• Requires knowledge of adversary capabilities and intent • Compressed timeline ("net" speed) • Attribution is challenging	• Requires knowledge of adversary capabilities and intent

Sumber : Perbandingan Perang Konvensional dan Siber (Brandes, 2013)

Bukan merupakan rahasia umum bahwa sektor pertahanan dan militer telah begitu banyak memutakhirkan sistemnya sehingga berbasis elektronik dan digital yang berarti bahwa seluruh aset dan sumber daya yang melekat padanya terhubung dengan teknologi informasi ke dunia siber. Sejalan dengan manfaat yang diperoleh, risiko ancaman besar terhadapnya membayangi juga dari masa ke masa. Para petinggi dan pimpinan pertahanan negara harus memastikan bahwa mereka memiliki kendali penuh terhadap seluruh instalasi aset dan sumber daya militer yang dimiliki, terutama yang terhubung ke dunia siber secara langsung maupun tidak langsung.

Penyusunan dan Pengembangan Kebijakan Publik

Thomas Dye memberikan tiga pertimbangan atau alasan terkait dengan mengapa secara akademis analisis kebijakan publik perlu dipelajari, yaitu (Goldsmith, 2015):

1. Alasan atau pertimbangan ilmiah (*scientific reasons*), dimana kebijakan publik dipelajari untuk menambah pengetahuan yang mendalam mengenai hal-hal terkait dengannya, seperti yang berkaitan dengan asal muasal, proses, perkembangan, dan dampak bagi masyarakat.
2. Alasan atau pertimbangan profesional (*professional reasons*), dimana disadarinya terdapat pemisahan yang jelas antara *scientific-estate* (mencari untuk kepentingan ilmu pengetahuan) untuk pemecahan masalah dengan *professional-estate*

(menerapkan ilmu pengetahuan) untuk diterapkan sebagai solusi praktis atas masalah sosial yang dijumpai.

3. Alasan atau pertimbangan politis (*political reasons*), dimana kebijakan publik dipelajari agar peraturan perundang-undangan dan regulasi yang dirancang serta ditetapkan pemerintah dapat secara tepat guna mencapai tujuan yang ditargetkan.

Dalam ranah diskursus akademik, terdapat sejumlah definisi dari kebijakan publik, antara lain (Fischer & Miller, 2017; Goodin et al., 2009; "Handb. Public Policy Anal.," 2017):

1. Robert Evestone: "hubungan beragam unit yang ada dalam pemerintahan dengan lingkungannya"
2. Heinz Eulau dan Kenneth Prewitt: "keputusan tetap yang mengikat, dengan adanya ciri konsistensi dan pengulangan (repetisi) tingkah laku pembuat dan mereka yang mematuhi keputusan tersebut"
3. Chandler dan Plano: "pemanfaatan strategis terhadap sumber daya-sumber daya yang ada dalam rangka memecahkan berbagai problema yang dihadapi publik atau pemerintah"
4. Dye: "apa yang dipilih oleh pemerintah untuk dapat dikerjakan atau tidak dikerjakan"
5. Richard Rose: "sebuah rangkaian yang panjang dari sejumlah kegiatan yang saling berhubungan satu dengan lainnya dan memiliki konsekuensi bagi yang berkepentingan sebagai suatu keputusan yang berbeda"
6. Carl Friedrich: "serangkaian tindakan atau kegiatan yang diusulkan oleh individu, kelompok manusia (komunitas), atau pemerintah dalam suatu lingkungan tertentu, dimana terdapat sejumlah hambatan (kesulitan) dan kemungkinan-kemungkinan (peluang) dimana kebijakan tersebut diusulkan dapat berguna dalam mengatasinya untuk mencapai tujuan dimaksud"

7. James Anderson: “serangkaian kegiatan yang memiliki maksud atau tujuan tertentu yang selanjutnya diikuti serta dilaksanakan oleh seorang aktor atau sekelompok aktor yang berhubungan dengan suatu masalah atau hal yang menjadi fokus perhatian”
8. David Easton: “manifestasi atau pengejawantahan sebagai ‘otoritas’ dalam sistem politik, yaitu ‘para senior’, raja, kepala tertinggi, eksekutif, hakim, administrator, penasehat, dan sebagainya”

Berbasis pada sejumlah pandangan yang dikemukakan dalam beragam perspektif definisi di atas, pertanyaan mengapa perlu dipelajari analisis kebijakan publik dapat dijawab sebagai berikut:

1. Agar kebijakan yang dihasilkan benar-benar memberikan manfaat positif bagi masyarakat sesuai dengan tujuan pemerintah ketika merancang dan menyusunnya;
2. Agar kebijakan yang dihasilkan dapat memecahkan masalah yang dihadapi oleh publik/masyarakat dengan cara paling efisien atau tepat guna;
3. Agar kebijakan yang dihasilkan tidak saling tumpang tindih dengan berbagai peraturan yang telah ada sebelumnya, sehingga berdampak mengurangi efektivitas implementasinya;
4. Agar kebijakan yang dihasilkan dapat secara efektif diterapkan dan diimplementasikan sesuai dengan harapan; dan
5. Agar kebijakan yang dihasilkan dapat dipertanggungjawabkan secara hukum maupun etika karena disusun dengan mengikuti tahapan metodologi yang benar.

Pemahaman mendalam tentang konsep pengembangan kebijakan publik akan pula memberikan manfaat yang jelas kepada para praktisi pembuat kebijakan akan berbagai hal, seperti: (i) isi dan maksud dari kebijakan yang dikembangkan; (ii) dampak dari kebijakan terhadap lingkungannya; (iii) model pengaturan berbagai kelembagaan pelaksana kebijakan; (iv) proses-proses politik yang melatarbelakangi pembuatannya; (v) akibat kebijakan publik

terhadap sistem politik pemerintahan dan negara; (vi) evaluasi pelaksanaan kebijakan dalam ruang lingkup hidup bermasyarakat dan bernegara (Caywood et al., 1988; Goldsmith, 2015).

Perlu diperhatikan bahwa pada dasarnya kebijakan dipandang sebagai sebuah variabel terikat, sehingga fokus banyak tertuju pada faktor-faktor politik maupun lingkungan yang mempengaruhi penentuan substansi dari kebijakan atau diduga berpengaruh terhadap problema kebijakan publik yang ada. Sementara itu kebijakan dapat pula dilihat sebagai variabel independen apabila fokus perhatian ditujukan pada dampak kebijakan terhadap sistem politik atau lingkungan yang memiliki pengaruh terhadap subyek atau obyek kebijakan yang dihasilkan.

Perlu ditambahkan bahwa pada prinsipnya, terdapat tiga tahapan penting dalam metodologi analisis kebijakan publik yang perlu dimengerti, yaitu formulasi kebijakan (*policy formulation*), implementasi kebijakan (*policy implementation*) dan evaluasi kebijakan (*policy evaluation*) (Ramdhani & Ramdhani, 2017). Sementara menurut Anderson, ada lima tahapan penting dalam membuat kebijakan, yaitu: (i) *problem formulation*; (ii) *policy formulation*; (iii) *adoption*; (iv) *implementation*; dan (v) *evaluation*.

Secara deskripsi, kategori kebijakan terdiri dari 5 butir, yaitu: (i) *policy demands*; (ii) *policy decisions*; (iii) *policy statements*; (iv) *policy outputs*; dan (v) *policy outcomes*. Berikut ini adalah penjelasan singkat beserta contoh-contohnya dalam konteks Indonesia (Nopriono & Suswanta, 2019; Politik, 2017).

Policy Demand

Kebutuhan akan kebijakan berasal dari adanya isu, permalasahan, kejadian, permintaan, atau peluang yang ada di masyarakat. Permintaan atau kebutuhan akan suatu kebijakan tersebut disalurkan masyarakat, baik secara pribadi maupun berkelompok, melalui sistem politik yang dianut. Contoh kebutuhan akan kebijakan adalah sebagai berikut:

1. Perlunya kebijakan ramah investasi di Indonesia agar para investor luar bersedia menanamkan uangnya di tanah air;
2. Perlunya kebijakan untuk mempercepat penciptaan lapangan kerja di Indonesia sebagai bagian dari pengentasan kemiskinan dan mengurangi pengangguran;
3. Perlunya kebijakan pengelolaan kemanan siber di Indonesia agar aset-aset strategis berbasis teknologi informasi terlindungi dari berbagai serangan yang memanfaatkan internet;
4. Perlunya kebijakan pengendalian terhadap emisi karbon agar Indonesia terhindar dari dampak pemanasan global; dan lain sebagainya.

Policy Decision

Keputusan kebijakan ini berisi keputusan-keputusan yang dibuat oleh para pejabat publik yang berwenang untuk mengatur dan memberi isi pada tindakan kebijakan publik. Berkaitan dengan butir-butir di atas, berikut adalah contoh dari sebuah keputusan kebijakan:

1. Diputuskan bahwa pengurusan ijin bagi investor luar yang ingin berinvestasi di Indonesia tidak boleh lebih dari 24 jam;
2. Diputuskan bahwa para pengusaha luar negeri yang beroperasi di Indonesia dan memiliki lebih dari 10,000 karyawan akan memperoleh keringangan pajak;
3. Diputuskan bahwa setiap Badan Usaha Milik Negara harus melaksanakan audit resmi terhadap keamanan teknologi informasi yang dimilikinya;
4. Diputuskan bahwa setiap pabrik atau manufaktur di Indonesia harus mentaati standar emisi yang telah ditetapkan negara; dan lain sebagainya

Policy Statement

Pernyataan kebijakan ini adalah ungkapan secara eksplisit dan formal mengenai kebijakan yang telah diputuskan dan ditetapkan. Dalam contoh kasus di atas adalah sebagai berikut:

1. “Investor asing yang ingin berinvestasi di Indonesia dapat mengajukan permohonan penanaman modal melalui sistem *e-capital* yang dikelola oleh Badan Koordinasi Penanaman Modal (BKPM). Proses permohonan akan memakan waktu paling lambat 24 jam semenjak permohonan diajukan.”
2. “Para pengusaha luar negeri yang beroperasi di Indonesia dalam bentuk penananam modal asing pada sebuah perseroan terbatas, apabila memiliki jumlah karyawan tetap lebih dari 10,000 orang akan memperoleh insentif pengurangan pajak dengan besaran proporsional terhadap jumlah karyawan dimaksud. Adapun besarannya dapat dilihat pada Tabel Instentif Pajak yang dikeluarkan oleh Kementerian Keuangan Republik Indonesia.”
3. “Setiap Badan Usaha Miliki Negara wajib melakukan audit sistem dan teknologi informasi secara berkala, yaitu minimum 6 (enam) bulan sekali secara berkesinambungan.”
4. “Pabrik atau manufaktur yang beroperasi di wilayah Indonesia wajib memenuhi standar emisi yang ditetapkan bersama oleh Kementerian Perindustrian, Kementerian Kesehatan, dan Kementerian Lingkungan Hidup.”

Policy Output

Hasil dari kebijakan adalah merupakan perwujudan nyata dari kebijakan publik, atau sesuatu yang sesungguhnya dikerjakan menurut keputusan dan pernyataan kebijakan, atau apa yang dikerjakan pemerintah. Dengan kata lain, hasil kebijakan merupakan manifestasi kebijakan publik yang riil nampak secara nyata di lapangan (masyarakat). Contohnya adalah:

1. Proses perijinan bagi investor asing menjadi sangat cepat, karena semua selesai dalam 24 jam.
2. Perusahaan asing yang ada di Indonesia berlomba-lomba melakukan ekspansi dan merekrut karyawan, karena insentif pajak yang signifikan jumlahnya.
3. Setiap BUMN secara berkala melakukan proses audit sistem dan teknologi informasi yang dimilikinya.
4. Pengusaha yang memiliki pabrik berinvestasi untuk memastikan terpenuhinya standar emisi yang ditetapkan pemerintah.

Policy Outcomes

Dampak kebijakan adalah konsekuensi yang timbul di masyarakat baik disengaja maupun tidak akibat tindakan yang dilakukan pemerintah melalui kebijakan yang diberlakukannya. Contohnya adalah sebagai berikut:

1. Semakin banyak investor luar negeri tertarik untuk menanamkan modalnya di Indonesia karena cepat dan mudah, sehingga secara tidak langsung berkontribusi terhadap pertumbuhan ekonomi nasional.
2. Semakin berkurangnya pengangguran (dan kemiskinan) karena banyak perusahaan yang tidak khawatir melakukan ekspansi peningkatan jumlah karyawan akibat adanya insentif pajak yang signifikan.
3. Berkurangnya kasus keamanan siber *(cyber crime)* di lingkungan BUMN karena institusi terkait telah memiliki sistem keamanan handal yang senantiasa diaudit kinerjanya.
4. Terhindarnya Indonesia dari isu pemanasan global karena adanya reduksi yang signifikan terhadap emisi karbon yang ada di tanah air.

Walaupun telah memiliki Undang-Undang Informasi dan Transaksi Elektronik di tengah-tengah berbagai regulasi lain yang mendahuluinya dan yang direncanakan untuk disusun, dipandang dari sisi kebijakan publik agak sulit untuk

mengatakan bahwa keseluruhan paket regulasi dan kebijakan publik tersebut akan mampu menjawab kebutuhan akan kedaulatan sistem pertahanan siber negara. Kenyataan memperlihatkan bahwa kebijakan publik yang dibuat terkait dengan dunia siber masih bersifat sporadis, berbasis sektoral, sarat akan birokrasi, dan sulit menegakkan hukum bagi yang melanggarnya. Artinya adalah bahwa model kebijakan publik yang dibuat dalam mengatur sistem siber di Indonesia tidak selaras atau kongruen dengan karakteristik dunia siber itu sendiri. Tanpa adanya perubahan pola pikir ke arah yang benar ketika memandang dan mengelola dunia siber akan menyulitkan bagi negara dalam mengembangkan atau menyusun berbagai kebijakan publik yang efektif.

Soft System Methodology

Manusia dalam kehidupannya kerap berhadapan dengan beragam fenomena permasalahan dengan karakteristik yang berbeda-beda. Setiap permasalahan pada dasarnya memiliki karakteristiknya masing-masing. Metoda numerik dan kuantitatif misalnya dipergunakan sebagai instrumen dalam memahami dan menyelesaikan masalah yang bersifat deterministik dan empiris. Sementara model statistik banyak dipergunakan untuk menggambarkan fenomena secara obyektif melalui metoda deskriptif, komparatif, asosiatif, dan perdiktif. Pada tataran fenomena sosial, kerap ditemukan permasalahan yang bersifat rumit, kompleks, multi-dimensi, tak beraturan, dan nir struktur. Pendekatan matematis kuantitatif atau statistik deskriptif yang bersifat “hard thinking” dianggap tidak mampu dalam menjawab tantangan permasalahan yang ada. Dalam konteks inilah Peter Checkland bersama koleganya membangun dan memperkenalkan sebuah metoda “soft thinking” yang diberi nama Soft System Methodology atau SSM. Metoda SSM ini dikembangkan di atas aksioma sebagai berikut:

1. Masalah apapun yang ditemui dalam kehidupan manusia tidak berdiri sendiri, keberadaannya adalah merupakan manifestasi dari kesadaran manusia dalam menghadapi fenomena hidupnya dilihat

dari perspektif kemanusiannya, sehingga hindari fokus pada isu yang dihadapi, tapi lebih melihat pada situasi yang dihadapi;

2. Karena sifatnya yang tidak berdiri sendiri, maka permasalahan yang ditemui manusia bersifat multi-dimensi, karena selain dapat dilihat dari berbagai perspektif berbeda, terdapat relasi keterkaitan secara “mess” antar berbagai komponen dalam beragam dimensi berbeda;

3. Setiap manusia pada dasarnya memiliki “worldview” atau dunia pandang yang berbeda-beda, dimana setiap pandangan masing-masing individu secara subyektif adalah sah adanya, dan tak dapat dipersalahkan;

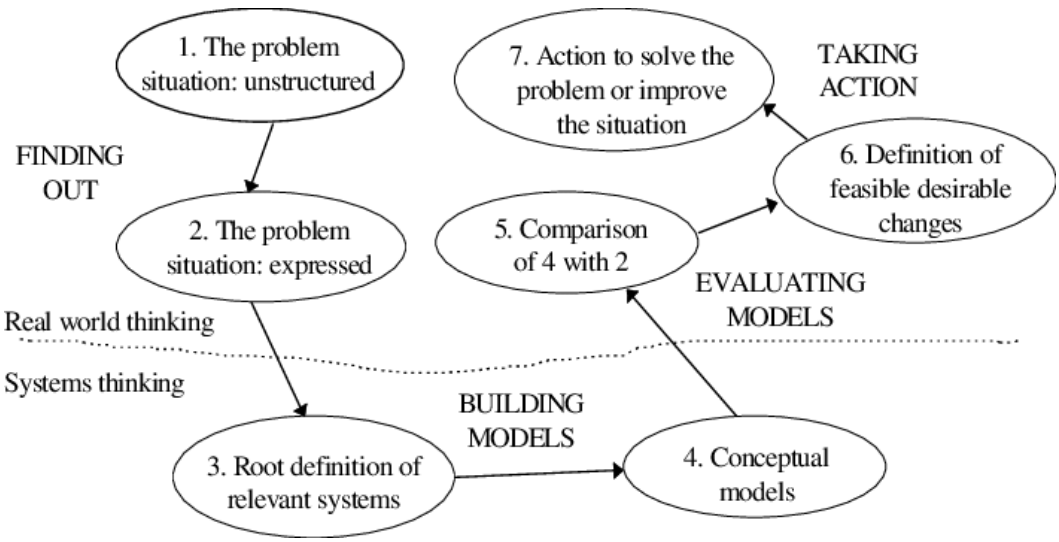
4. Karena masalah didefinisikan sebagai sebuah feomena multi-dimensi, maka solusinya pun bersifat jamak, dalam arti kata terdapat berbagai kombinasi pemecahan solusi yang dapat diterapkan sesuai dengan situasi, kondisi, dan konteksnya yang berbeda-beda pula; dan

5. Perbaikan situasi sebagai solusi hanya akan terjadi apabila terdapat partisipasi dalam rupa saling berbagi persepsi, persuasi, dan perdebatan secara intensif dan interaktif.

SSM dibangun di atas konsep yang menyandingkan kedua domain dunia, yaitu dunia nyata yang pragmatis dan dunia ideal yang ideal secara teoritis. Dengan menggunakan pendekatan *system thinking*k dibangunlah asosiasi kedua dunia tersebut untuk mendapatkan gambaran utuh, holistik, dan komprehensif terhadap situasi yang dihadapi guna mendapatkan solusi pemecahannya. Melalui berfikir secara sistem, masalah yang dihadapi direpresentasikan dalam sebuah *rich picture* yang di dalamnya terdiri dari entitas, komponen, relasi, kendali, dan berbagai atribut lain untuk menstrukturkan permasalahan konteks yang rumit dan tak teratur. Selain *rich picture*, instrumen CATWOE dipergunakan pula untuk membantu memahami permasalahan yang dihadapi. CATWOE merupakan singkatan dari *Customers, Actors, Transformation process, Worldview, Owner,* dan *Environmental constraints*.

Tranformasi dianggap sebagai jantung dari SSM, karena tujuannya adalah mengubah satu status (masalah) menjadi sebuah kondisi baru (solkusi). Tiga indikator kesuksesan transformasi yang dipergunakan adalah 3E, yaitu: *Efficacy, Efficiency,* dan *Effectiveness*.

Cara menerapkan SMM adalah dengan menjalani 7 (tujuh) tahapan sekuensial, masing-masing adalah:



Gambar 2. 6 Soft System Methodology

Sumber : Soft System Methodology (SSM) (Checkland, 2001)

1. *The Problem Situation: Unstructured* – menceritakan problem yang dihadapi seperti apa adanya, dengan tidak mengikuti pola logika tertentu, melainkan sesuai dengan aliran pemikiran yang datang walaupun terlihat tak terstruktur dan lompat-lompat;
2. *The Problem Situation: Expressed* – mencoba menggambarkan situasi kompleks yang ada secara terstruktur dengan sejumlah logika tertentu melalui pemanfaatan *rich picture*;

3. *Root Definition of Relevant Systems* – mencari akar permasalahan dari sistem hipotetikal yang digambarkan via *rich picture* agar dapat fokus pada pemahaman situasi guna mencari pemecahan terhadap permasalahan yang dihadapi;

4. *Conceptual Models* – menggali berbagai referensi untuk mendapatkan model konseptual yang ideal sebagai batu pijakan dalam memahami problema yang dihadapi untuk mencari solusinya;

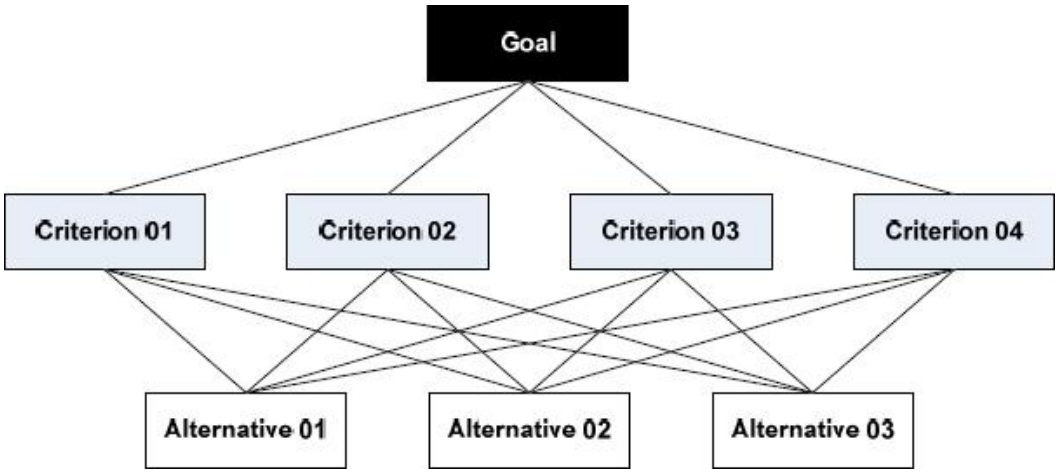
5. *Comparison as Gap Analysis* – membandingkan antara kondisi riil yang dihadapi dalam dunia nyata dengan situasi ideal dalam model konsep guna mendapatkan gap yang harus menjadi perhatian untuk dijembatani;

6. *Definition of Feasible Desirable Changes* – menentukan dan mendefinisikan langkah-langkah yang harus dihadapi untuk mentransformasikan kondisi riil menuju situasi ideal yang diinginkan; dan

7. *Action to Solve the Problem or Improve the Situation* – melaksanakan langkah-langkah yang telah ditetapkan agar masalah atau problem yang dihadapi segera terselesaikan.

Analytic Hierarchy Process

AHP atau *Analytic Hierarchy Process* adalah sebuah metoda untuk membantu manusia dalam mengambil keputusan. Metoda ini menggunakan pendekatan terstruktur dan terorganisasi untuk membantu menganalisa problem pengambilan keputusan yang kompleks. Pendekatan ini menggabungkan antara pendekatan matematika, statistika, dan psikologi. Pada dasarnya AHP adalah salah satu contoh metoda berbasis *Multiple Objectives Multiple Criteria* (MOMC).



Gambar 2. 7 Analytic Hierarchy Process

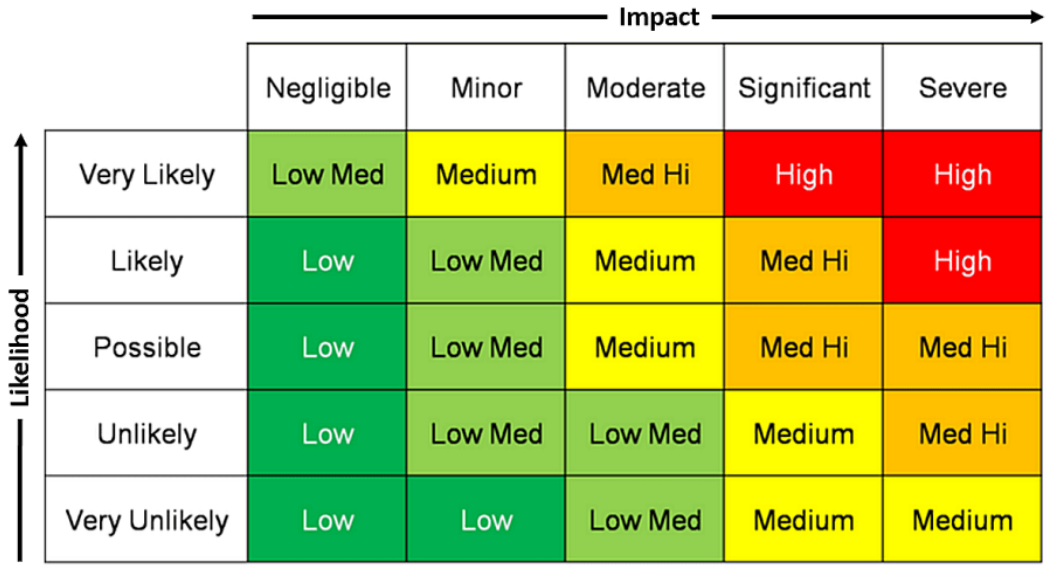
Sumber : Analytic Hierarchy Process (Saaty, 1970)

AHP dapat dimanfaatkan untuk membantu proses pengambilan keputusan dengan melakukan pendekatan sebagai berikut. Pertama, tentukanlah tujuan atau obyektif atau *goal* yang ingin dilakukan via proses pengambilan keputusan. Contoh tujuan adalah "Membangun Sistem Pertahanan Siber yang Kuat". Kedua, tetapkanlah sejumlah alternatif solusi yang dapat dipilih dimana semuanya bermuara pada kehendak untuk mencapai tujuan dimaksud. Misalnya sejumlah alternatif dimaksud antara lain: (i) Membeli teknologi siber tercanggih; (ii) Membentuk tentara siber yang kuat; (iii) Mengembangkan industri pertahanan siber; (iv) Membangun fasilitas *cyber operation center*; dan (v) Mengadopsi *best practices* tata kelola siber. Ketiga, untuk melakukan pemilihan atau pengambilan keputusan yang obyektif, perlu diidentifikasi serta ditetapkan sejumlah kriteria, seperti: biaya yang dikeluarkan, dukungan politik yang diperoleh, kecepatan implementasi, efektivitas penerapan, rintangan yang dihadapi, dan besaran risiko yang dihadapi. Keempat berkaitan dengan membandingkan prioritas antar kriteria untuk mendapatkan bobotnya masing-masing – yang merepresentasikan tingkat kepentingan antar kriteria. Kelima adalah melakukan perbandingan atau

komparasi antar alternatif per masing-masing kriteria – yang bermuara pada penetapan bobot perhitungan untuk setiap alternatif. Keenam merupakan langkah konsolidasi dimana dilakukan operasi matematika terhadap bobot kriteria dan alternatif untuk mendapatkan nilai akhir untuk setiap kriteria. Ketujuh adalah menetapkan keputusan akhir melalui pemilihan alternatif dengan nilai skor tertinggi.

Risk Assesment Method

Metoda asesmen risiko dipergunakan untuk menentukan fokus mitigasi terhadap hal-hal yang tidak diinginkan terjadi. Instrumen yang dipergunakan untuk melakukan risiko adalah melalui matrik dua dimensi. Sumbu pertama berkaitan dengan besara probabilitas atau *likelihood* keterjadian suatu peristiwa atau *event* risiko yang tak diinginkan. Sementara sumbu kedua berhubungan dengan dampak atau *impact* yang dihasilkan seandainya *event* yang tak diinginkan benar-benar terjadi. Untuk memudahkan pemetaan, terhadap probabilitas keterjadian peristiwa tak diinginkan dilakukan pengelompokkan sebagai berikut: *very likely, likelly, possible, unlikely,* dan *very unlikely*. Sementara untuk dampak yang dihasilkan, dilakukan kategorisasi yaitu: *negligible, minor, moderate, significant,* dan *severe*. Fokus atau prioritas mitigasi perlu dilakukan terhadap *event* yang berkaitan dengan tiga kuadran utama, yaitu: *(i) Very Likely – Significant; (ii) Very Likely – Sever;* dan *(iii) Likely – Severe.* Ketiga kuadran ini terpilih karena memiliki tingkat probabilitas keterjadiannya tinggi, dan dampaknya sangat membahayakan. Matrik asesmen risiko ini dapat dipergunakan dalam berbagai situasi yang berkaitan dengan melakukan pemilihan atau fokus pada hal-hal penting untuk dipertimbangkan.

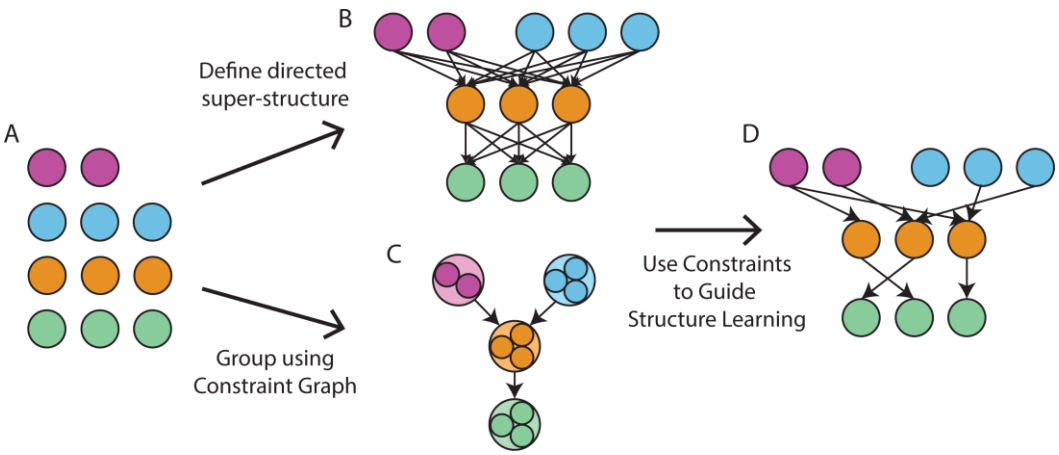


Gambar 2. 8 Risk Assessment Matrix

Sumber : Risk Assessment Matrix (Management Practices)

Cause-Effect Bayesian Network

Bayesian Network meruapkan model grafis berbasis probabilistik kejadian yang dipergunakan untuk menggambarkan relasi antar satu peristiwa dengan peristiwa lainnya. Sebagai mana sebuah *network*, entitas yang dipergunakan ada dua, yaitu *node* dan *path*. Ketika menggunakan Bayesian Network untuk menggambarkan fenomena hubungan sebab-akibat atau *cause-effect relationships*, simbol *node* dipergunakan untuk merepresentasikan sebuah peristiwa, sementara *path* dengan simbol panah satu arah menggambarkan peristiwa mana yang menjadi sebab dan akibat.



Gambar 2. 9 Bayesian Network

Sumber : Bayesian Network (Yang, 2019)

Melalui penggambaran via representasi *graph* ini akan dapat dilakukan berbagai operasi matematis, seperti mencari probabilitas tertinggi, *path* terpendek, optimalisasi obyektif (waktu dan biaya), dan lain sebagainya.

Penelitian Terdahulu

Ada beberapa hasil penelitian terdahulu yang memiliki tingkat relevansi dengan studi ini, terutama dari para ilmuwan maupun praktisi yang fokus membahas masalah-masalah terkait dengan isu-isu seputar:

1. Pertahanan siber dalam konteks pertahanan negara dan keamanan nasional;
2. Ragam ancaman non-militer berbasis digital yang membahayakan keutuhan dan kedaulatan bangsa dan negara, terutama dalam sektor pertahanan;

3. Strategi dan kesiapan berbagai negara (termasuk Indonesia) dalam mengembangkan sistem pertahanan siber nasional yang kuat;

4. Pendapat dan diskursus seputar efektif tidaknya diterapkan model kedaulatan siber oleh masing-masing negara dalam berbagai bentuk dan pendekatannya;

5. Beraneka ragam kebijakan terkait dengan pertahanan siber dalam konteks pengelolaan dan penyelenggaraan pertahanan negara;

6. Model doktrin pertahanan siber yang terpisah maupun terintegrasi dengan doktrin konvensional pertahanan negara yang selama ini dikenal; dan

7. Kerangka berpikir secara teoritis maupun konseptual terkait dengan isu seputar pertahanan negara, kedaulatan siber, doktrin hanneg, kebijakan siber, dan penyelenggaraan sistem pertahanan negara.

Ruang lingkup penelitian terdahulu juga terlihat sangat beragam. Jenis pertama adalah mencoba mengamati berbagai strategi kebijakan pertahanan siber dalam konteks satu negara. Studi ini didasarkan pada pengalaman di masa lalu yang coba dipetik pembelajarannya untuk dilakukan perbaikan pada masa kini dan mendatang. Sementara jenis yang kedua adalah dalam ruang lingkup komunitas negara, seperti ASEAN, NATO, Asia Pasifik, G20, dan lain sebagainya. Basis pengembangan strategi dan kesepakatan kolektif ini adalah diplomasi dan kerjasama di atas kepentingan yang serupa, yaitu untuk menjaga keharmonisan di arena siber. Sementara yang ketiga adalah pada lingkungan global atau tatanan dunia. Pada domain ini terlihat bagaimana sulit dan kompleksnya menghadapi isu keteraturan dan pengendalian terhadap perilaku subyek maupun obyek yang berada dalam dunia siber. Dalam konteks global ini peran negara sejajar dengan aktor-aktor lainnya karena sifat dan karakteristik siber yang *agile, dynamic,* dan *cross border*. Peran sejumlah *non-state actor* seperti pebisnis atau industri dapat setara dengan sebuah negara dalam konteks pengendalian ekosistem siber.

Metoda pengkajian maupun penelitian yang dilakukan untuk memahami dan mendalami beragam fenomena siber pun berbeda. Selain berbasis penelitian kualitatif dan kuantitatif klasik, berbagai metoda pengkajian pun dipergunakan seperti fenomenologi, *mixed methods*, etnografi, *research and development, case study,* dan lain sebagainya. Terlihat dari berbagai penelitian terdahulu adanya fenomena diskursus berisi perdebatan yang sangat seru dan tajam mengenai perspektif memandang dunia siber – yang berpengaruh terhadap lahirnya berbagai pandangan, pendekatan, dan strategi dalam mengembangkan regulasi atau kebijakan pertahanan siber yang efektif, efisien, dan terkendali. Diskursus yang terjadi pun nampak terus berkembang sejalan dengan kemajuan pesat dari ilmu pengetahuan dan teknologi yang melatarbelakangi pembentukan arena maya dimaksud.

Tabel 2. 6 Daftar Penelitian Relevan Terdahulu

NO	JUDUL PENELITIAN, PENULIS, DAN SUMBER	METODA PENELITIAN	HASIL PENELITIAN	RELEVANSI	PERBEDAAN DAN KETERBATASAN
1	*"Regulating Unlawful Behavior in the Global Business Environment: The Functional Integration of Sovereignty and Multilateralism"* (Weismann, 2010) *Journal of World Business, 45(3), 312–321*	Kualitatif	Model kedaulatan siber sebuah negara yang dikembangkan berdasarkan prinsip-prinsip *Convention on Cybercrime*.	Pembahasan mengenai konsep kedaulatan dalam hubungan multilateral negara-negara di dunia	Pendekatan ini dianggap kurang afektif karena banyak melanggar perjanjian kerjsama di bidang perdagangan yang disepakati antar negara.
2	*"A Doctrine of Contingent Sovereignty"* (Nell, 2018) *Orbis, 62(2), 313–334*	Kualitatif	Sebuah usulan pemutakhiran doktrin kedaulatan yang diajukan untuk melawan fenomena kejahatan yang ditimbulkan oleh *non-state actors* dengan memanfaatkan perkembangan teknologi.	Doktrin yang berkaitan dengan hal-hal yang harus dilakukan ketika terjadi gangguan terhadap kedaulatan negara yang ditimbulkan oleh *non-state actors*	Usulan ini hanya cocok untuk negara-negara maju yang dikelilingi (dikeroyok) oleh berbagai musuh *non-state actors* yang tidak memiliki kekuatan militer besar.

3	*"Cyber-Attack as Inevitable Kinetic War"* (Lilienthal & Ahmad, 2015b) *Computer Law and Security Review, 31(3)*	Kualitatif dengan menggunakan penekatan fenomenologi	Studi ini mencoba untuk mengamati apakah fenomena serangan siber tidak bertentangan dengan doktrin perang pada *the United Nations Charter*.	Gambaran mengenai pandangan PBB terhadap fenomena serangan siber yang aktif terjadi antar negara	Hasil studi memperlihatkan bahwa terlepas dari adanya penghormatan terhadap kemerdekaan dan kedaulatan negara, serangan siber tidak akan pernah bisa dihentikan.
4	*"How to Think about Cyber Sovereignty?: the Case of China"* (Hong & Goodnight, 2020) *Chinese Journal of Communication, 13(1)*	Kualitatif dengan berbasis pada pendatan Subyektivisme	Strategi negara China dalam membangun kedaulatan siber melalui konsep *multipolar global digital capitalism*.	Model negara China membangun kedaulatan sibernya yang unik	Selain hanya cocok diterapkan di negara komunis, konsep ini berhadapadan dengan isu security, *privacy*, hukum, dan masa depan bumi.
5	*"Cyber Sovereignty: The Way Ahead"* (Eric T Jensen, 2015) *Texas International Law Journal, 50(2)*	Kualitatif	Peneliti mengajukan suatu usulan pendekatan *the international law doctrine of sovereignty* sebagai cara yang efektif untuk mengelola kedaulatan siber berbagai negara di dunia.	Usulan mengenai salah satu pilihan model kedaulatan siber di masa mendatang	Tidak mudah bagi seluruh negara di dunia untuk bersepakat dalam penyusunan doktrin yang mengikat mereka semua.

6	*"Cyber Sovereignty and the Governance of Global Cyberspace"* (Shen, 2016) *Chinese Political Science Review, 1(1)*	Kualitatif	Pemaparan terkait dengan berbagai model kedaulatan siber dengan menggunakan Amerika Serikat dan China sebagai dua kutub ekstrim yang sangat berbeda pendekatannya.	Gambaran bagaimana Amerika Serikat dan China mengelola kedaulatan dan tata kelola siber nasionalnya	Deskripsi berdasarkan dokumen kebijakan di masa lalu yang belum tentu relevan dengan kebutuhan masa depan.
7	*"Against Sovereignty in Cyberspace"* (Mueller, 2019) *International Studies Review*	Kualitatif	Penelitian yang mencoba membedah ekosistem dunia siber berdasarkan studi literatur dan penelitian terdahulu agar komponen-komponennya dapat diidentifikasi dan diurai.	Berisi komponen-komponen penting yang harus diperhatikan dalam sebuah ekosistem kedaulatan siber	Berkaca pada negara-negara besar seperti Amerika Serikat, Rusia, dan China, dimana memiliki karakteristik berbeda dari negara kebanyakan lainnya
8	*"Exercising State Sovereignty in Cyberspace"* (Liaropoulos, 2013) *The 8th International Conference on Information Warfare and Security, ICIW 2013*	Kualitatif	Pemetaaan wilayah siber terhadap domain darat, laut, udara, dan angkasa untuk memperoleh gambaran mengenai posisi strategisnya.	Tawaran peran dan posisi siber dalam lingkungan fisik yang selama ini dikenal manusia.	Premis ini dibuat sebagai bahan untuk mendesak dunia internasional menerapkan *international cyber-order* yang belum tentu semua pihak menyepakatinya.

9	*"The "Triptych of Cyber Security": A Classification of Active Cyber Defence* (Dewar, 2014)" *International Conference on Cyber Conflict, CYCON, 2014*	Kualitatif	Pengembangan konsep *Active Cyber Defense (ACD)* sebagai inti dari prinsip pengembangan kebijakan kedaulatan siber sebuah negara.	Konsep pertahanan siber aktif yang dapat menjadi alternatif pilihan bagi sektor pertahanan negara.	Relevan untuk negara-negara yang menguasai industri teknologi informasi dan komunikasi secara mandiri.
10	*"Cybersecurity Policy and Its Implementation in Indonesia"* (Rizal & Yani, 2016) *JAS (Journal of ASEAN Studies), 4(1)*	Kualitatif dengan pendekatan deskriptif berbasis studi kasus	Pemaparan kondisi termutakhir di Indonesia terkait dengan kebijakan keamanan siber.	Kebijakan keamanan siber termutakhir di Indonesia beserta ruang lingkup regulasinya.	Bersifat deskriptif mengenai fenomena ancaman dan permasalahan yang dihadapi tanpa adanya rekomendasi solutif.
11	*"Penerapan Military Confidence Building Measures dalam Menjaga Ketahanan Nasional Indonesia di Ruang Siber"* (Chotimah et al., 2019) *Jurnal Ketahanan Nasional, 25(3)*	Kualitatif	Gambaran penerapan konsep *Military Confidence Building Measures* untuk meningkatkan ketahanan siber di Indonesia sebagai respon terhadap berbagai ancaman yang mengemuka.	Contoh jawaban terhadap ancaman siber yang dilakukan oleh militer Indonesia.	Masih kentalnya perdebatan mengenai isu *military restraint* di bidang siber dalam konteks menjaga kedaulatan negara.

12	*"Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?"* (Warner, 1998) *Journal of the American Society for Information Science, 49(4)*	Kualitatif	Jawaban terhadap pertanyaan apakah kedaulatan siber dapat menjawab berbagai ancaman keamanan siber yang terjadi di dunia melalui pendekatan *digital borders*.	Diskursus mengenai perdebatan dalam menentukan batasan ruang maya yang dapat diterima oleh berbagai khalayak.	Tawaran akan pemahaman "perbatasan siber" masih bersifat hipotetikal, sehingga belum tentu mendapatkan dukungan banyak pihak/negara.
13	*"Sovereignty and Neutrality in Cyber Conflict"* (Eric Talbot Jensen, 2012) *Fordharm International Law Journal, 35(3)*	Kualitatif	Pembahasan fenomena paradoksial antara kedaulatan berbasis wilayah fisik dan non-fisik (siber).	Penjelasan mengenai konsep kedaulatan dan netralitas dalam berbagai fenomena konflik di internet.	Filosofi netralitas membuat hanya negara-negara maju saja yang cenderung menguasai dunia siber.
14	*"China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of Internet Sovereignty"* (Zeng et al., 2017) *Politics and Policy, 45(3)*	Kualitatif dengan berdasarkan paradigma kritis	Tawaran negara China kepada dunia terkait konsep kedaulatan internet atau *internet sovereignty* sebagai bagian dari tata kelola dunia siber pada tataran global.	Strategi dan solusi China dalam mengatasi permasalahan tata kelola internet global yang banyak dipengaruhi oleh negara-negara maju terutama Amerika.	Desakan China kepada dunia untuk mengikuti model kebijakan yang disarankan, sebagai perimbangan atas kekuatan dunia barat akan teknologi informasi dan komunikasi

15	*"Respect for Sovereignty in Cyberspace"* (Schmitt & Vihul, 2017) *Texas Law Review, 95(7)*	Kualitatif	Pandangan Kementerian Pertahanan Amerika Serikat terhadap perlunya menghargai kedaulatan siber antar negara.	Pendekatan pengellaan kedaulatan siber melalui rasa percaya dan saling menghargai antar negara.	Proposal yang terlampau *soft* ini sulit dinyatakan dalam bentuk regulasi atau kebijakan, karena sifatnya yang *intangible*
16	*"Cyberspace: A New Threat to the Sovereingty of the State"* (Jackson Adams & Mohamad Albakajai, 2016) *Management Studies, 4(6)*	Kualitatif	Sisi lain ancaman siber yang bukan berasal dari kejahatan, melainkan dari dampak *digital economy*.	Fenomena ancaman baru terhadap kedaulatan siber nasional yang mempengaruhi pertahanan negara.	Pembahasan lebih fokus pada fenomena seputar e-commerce sebagai salah satu manifestasi bisnis di dunia siber.
17	*"Cyber Federalism: Defining Cyber's Jurisdictional Boundaries"* (Rosner, 2017) *Homeland Security Affairs*	Kualitatif	Tawaran membagi juridiksi siber sebagaimana terjadi pada negara federal di dunia nyata.	Usulan menggunakan pendekatan negara federal dalam mengelola batasan arena siber.	Banyak aspek yang tidak dapat disandingkan karena kedua dunia (fisik dan maya) memiliki karakteristik yang sangat berbeda.
18	*"Cyberspace Effects on Civil Society: The Ultimate Game-Changer or Not?"*	Kualitatif	Perubahan struktur kekuatan penguasaan terhadap dunia siber dari masa ke masa.	Peran aktif komunitas sipil dalam berpartisipasi pengamanan dunia siber dalam konteks kehidupan berbangsa	Dominasi negara-negara besar secara bergantian terhadap teknologi siber kurang relevan dengan kondisi negara-negara

	(Montalvan Castilla & Pursiainen, 2019) *Journal of Civil Society, 15(4)*			dan bernegara.	kecil dan menengah dalam mengembangkan kedaulatannya.
19	*"The Cyber Conceptual Framework for Developing Military Doctrine"* (Ormrod & Turnbull, 2016) *Defence Studies, 16(3)*	Kualitatif	Kerangka Konseptual Siber dalam Kerangka Doktrin Militer.	Peran penting dari konseptualisasi dan pemutakhiran doktrin militer yang memperhitungkan keberadaan siber.	Fokus pada domain militer tanpa mempertimbangkan partisipasi pihak lain.
20	*"A Three-Perspective Theory of Cyber Sovereignty"* (Yeli, 2017) *Prism, 7(2)*	Kualitatif	Komparasi antara tiga teori dasar dalam kedaulatan siber.	Cara pandang kedaulatan siber dilihat dari tiga perspektif yang berbeda namun saling terintegrasi.	Teori yang ada belum mengadopsi model kontemporer yang berkembang pasca Revolusi Industri 4.0.
21	*"Conceptualizing Cyber Policy through Complexity Theory"* (Brantly, 2019)	Kualitatif	Pendekatan membuat kerangka konsep kebijakan siber dilihat dari teori kompleksitas.	Cara menggambarkan konsep kebijakan siber dengan menggunakan teori kompleksitas.	Pertentangan antara penggambaran karakteristik fisik dan maya masih terlihat jelas di sini.

	Journal of Cyber Policy, 4(2)				
22	*"Mapping the Cyber Policy Landscape: Indonesia"* (Nugraha & Putri, 2016) *BSSN Review*	Kualitatif berbasis deskriptif dalam sebuah studi kasus	Penggambaran mengenai beragam lansekap kebijakan siber di Indonesia.	Peta kebiajakan siber di Indonesia dilihat dari sejarah kelahirannya dan tingkat efektivitasnya.	Sifatnya adalah pemetaan kondisi termutakhir, bukan usulan kebijakan ideal yang secara komprehensif harus dimiliki.
23	*"Embracing and Controlling Risk Dependency in Cyber-Insurance Policy Underwriting"* (Khalili et al., 2019) *Journal of Cybersecurity, 5(1)*	Kualitatif	Mekanisme pengendalian risiko berbasis siber.	Salah satu cara pendekatan strategi mitigasi terhadap akibat yang ditimbulkan serangan siber.	Pendekatan kebijakan ini terlihat cenderung bersifat sektoral, ke arah pendekatan hukum semata.
24	*"US Policy on Active Cyber Defense"* (Flowers & Zeadally, 2014) *Journal of Homeland Security and Emergency Management, 11(2)*	Kualitatif yang dikerjakan berbasis paradigma Subyektivisme	Deskripsi mengenai bagaimana Amerika Serikat menyusun kebijakannya terkait dengan pertahanan siber yang aktif.	Pilihan untuk mengadopsi pendekatan pertahanan siber yang aktif – berdasarkan prinsip "penyerangan adalah strategi pertahanan yang baik"	Kebijakan ini merupakan jawaban terhadap posisi negara yang memiliki banyak musuh.
25	*"How Australia can Catch-Up to*	Kualitatif	Strategi Australia dalam	Suatu terobosan untuk dapat	Ditekankan bahwa kunci

	US Cyber Resilience by Understanding that Cyber Survivability Test and Evaluation Drives Defense Investment" (Joiner, 2017) *Information Security Journal (Vol. 26, Issue 2)*		mengejar kebertinggalan dengan Amerika Serikat dalam konteks pertahanan siber.	mengimbangi kekuatan angkatan siber dari negara maju.	keberhasilan terletak pada besarnya alokasi investasi pada sektor pertahanan.
26	*"Resilience of Cyber Systems with Over- and Underregulation"* (Gisladottir et al., 2017) *Risk Analysis, 37(9)*	Kualitatif	Usulan konsep mengenai cara menyusun kebijakan ketahanan siber.	Cara menyusun kebijakan siber yang optimum.	Fokus pada kebercukupan regulasi yang dikembangkan.
27	*"Mimic Defense: A Designed-In Cybersecurity Defense Framework"* (H. Hu et al., 2018) *IET Information Security, 12(3)*	Kualitatif	Kerangka keamanan pertahanan siber yang dikembangkan dengan meniru konsep pertahanan negara.	Suatu pendekatan pengembangan kerangka pertahanan siber berbasis dunia nyata.	Terlihat bahwa tidak semua elemen pada konsep dapat dimimikkan.

28	*"Shadows of Stuxnet: Recommendations for US Policy on Critical Infrastructure Cyber Defense Dervied from the Stuxnet Attack"* (Lendvay, 2016) *Homeland Security Affairs*	Kualitatif dan kuantitatif menyangkut kejadian serangan masif dengan kalkulasi kerugian	Cara Amerika Serikat menyusun kebijakan perlindungan terhadap infrastruktur kritis pasca serangan Stuxnet.	Hal-hal yang harus diperhatikan dalam menghadapi serangan paling brutal karena ditujukan pada instalasi nuklir.	Fokus pada satu jenis serangan masif.
29	*"Cyber Posturing and the Offense-Defense Balance"* (Saltzman, 2013) *Contemporary Security Policy, 34(1)*	Kualitatif	Paparan konsep menyeimbangkan antara kemampuan pertahanan dan penyerangan dalam postur siber.	Prinsip yang perlu diadopsi dalam menyeimbangkan antara kemampuan menyerang dan bertahan di dunia siber.	Dikembangkan dengan asumsi negara memiliki sumber daya yang handal.
30	*"Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions"* (Waxman, 2013) *U.S. Naval War College*	Kualitatif	Pola pertahanan mandiri dalam menghadapi serangan siber.	Ragam dimensi strategis, legal, dan politik yang perlu dilihat dalam menghadapi serangan siber.	Dikembangkan dengan memperhatikan aspek hukum, politik, dan strategi.

	International Law Studies, 89				
31	*"Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice"* (Carayannis et al., 2014) *Cyber-Development Review*	Kualitatif	Pemaparan mengenai hubungan antara pembangunan siber, demokrasi siber, dan pertahanan siber.	Relasi erat antara pengembangan siber, demokrasi siber, dan pertahanan siber dalam berbagai perspektif teori, kebijakan, dan praktek.	Penekanan dilakukan pada unsur peluang dan tantangan yang dihadapi.
32	*"A Framework for Exploring Cybersecurity Policy Options"* (Mikolic-Torreira et al., 2017) *Cyber Policy Review*	Kualitatif	Paparan kerangka untuk mengeksplorasi berbagai plihan dalam menyusun kebijakan terkait keamanan siber.	Kerangka untuk dipergunakan sebagai pegangan dalam memilih opsi terbaik dalam mengembangkan kebijakan terkait.	Kerangka lebih fokus pada usaha untuk melakukan audit.
33	*"Cyber Defense as a Complex Adaptive System: A Model-Based Approach to Strategic Policy Design"* (Norman & Koehler, 2017)	Kualitatif	Konsep melihat pertahanan siber sebagai sebuah sistem kompleks yang adaktif.	Pandangan bahwa pertahanan siber bersifat dinamis sehingga kebijakan yang disusun haruslah *agile* dan fleksibel dalam menghadapi perubahan cepat.	Model ditujukan sebagai modal merancang kebijakan yang efektif.

	ACM International Conference Proceeding Series				
34	*"Disintermediation, Counterinsurgency, and Cyber Defense"* (Aucsmith, 2017) *SSRN Electronic Journal*	Kualitatif	Penjelasan fenomena disintermediasi, pemberontakan, dan pertahanan siber yang mengemuka belakangan ini.	Pertahanan siber dipandang dari fenomena disintermediasi dan *countersurgency.*	Sangat fokus dalam mencari relasi dari ketiganya.
35	*"Cyber Security – Threat Scenarios, Policy Framework and Cyber Wargames"* (Vaseashta et al., 2014) Cyber Security Policy Review	Kualitatif	Penjelasan mengenai fenomena keamanan siber.	Strategi mengembangkan keamanan internet dalam kerangka kebijakan menghadapi perang siber.	Fokus pada berbagai skenario ancaman, kerangka kebijakan, dan perang siber.
36	*"Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policy Making"* (Shackelford et al., 2019) *University of Pennsylvania Journal*	Kualitatif berupa studi komapratif antar berbagai model penyusunan kebijakan	Ajakan untuk memikirkan kembali model pertahanan aktif.	Penyusunan kebijakan pertahanan dan keamanan siber yang bersifat proaktif, dengan melihat tren di masa mendatang.	Tawaran didasarkan pada hasil analisa komparatif berbasis pengembangan kebijakan keamanan siber.

	of International Law, 41(2)				
37	*"Rough-And-Ready: A Policy Framework to Determine if Cyber Detterence is Working or Failing"* (Healey & Jenkins, 2019) *International Conference on Cyber Conflict, CYCON, 2019-May*	Kualitatif	Pengembangan kerangka kebijakan siber untuk meningkatkan daya gentar.	Perlunya kajian terhadap kemungkinan pengembangan daya gentar berbasis siber.	Fokus pada cara menilai apakah kebijakan berhasil atau gagal.
38	*"National Cyber Security Strategies: Global Trends in Cyberspace"* (Sabillon et al., 2016) *International Journal of Computer Science and Software Engineering, 5(5)*	Kualitatif	Strategi keamanan siber nasional yang dapat menjadi referensi negara lain.	Pentingnya setiap negara memiliki strategi pertahanan dan keamanan siber yang terintegrasi dan terpadu.	Konsep disusun berdasarkan analisa terhadap tren global di dunia siber.
39	*"Cyber Operations in Department of Defense Policy and Plans: Issues for Congress"* (Theohary & Harrington, 2015)	Kualitatif	Contoh kebijakan Kementerian Pertahanan Amerika Serikat dalam mengelola operasi sibernya.	Peran dan fungsi Kementerian Pertahanan dalam konteks kegiatan operasional pengelolaan siber nasional.	Paparan berbicara mengenai perencanaan ke depan.

	Threat Landscape Review				
40	*"A Framework for Thinking about Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains"* (Lukasik, 2010) *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy*	Kualitatif	Sebuah kerangka yang menghubungkan antara konflik dalam dunia siber dengan kinerja daya gentar.	Model kebijakan publik terkait dengan tata kelola oertahanan siber berbasis ancaman terjadinya konflik yang berpengaruh pada masyarakat luas.	Arah pembicaran ditujukan pada gagasan melakukan kebijakan khusus untuk menghadapi isu keduanya.
41	*"Cyber Acquisition: Policy Changes To Drive Innovation In Response To Accelerating Threats In Cyberspace"* (Klemas et al., 2019) *The Cyber Defense Review*	Kualitatif	Memperkenalkan konsep akuisisi siber dalam dunia pengelolaan moderen.	Cara mengubah dan memutakhirkan kebijakan yang telah dimiliki agar efektif dalam mengakselerasi kemampuan bertahan dari serangan siber.	Pemaparan berdasarkan pengembangan kebijakan yang memacu terjadinya inovasi.
42	*"Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence"*	Kualitatif	Mempelajari bagaimana negara China mengembangkan kedaulatan	Pandangan China sebagai negara kuat di bidang siber terkait dengan pendekatan	Secara khusus digambarkan bagaimana negara menggunakan siber untuk meningkatkan daya

	(Kolton, 2017) *The Cyber Defense Review, 2(1)*		sibernya.	kedaulatan dan daya gentar yang dikembangkannya.	gentarnya.
43	*"Securing the Internet of Battlefield Things while Maintaining Value to the Warfighter"* (Miller et al., 2019) *The 14th International Conference on Cyber Warfare and Security, ICCWS 2019*	Kualitatif	Strategi mengamankan internet dalam konteks peperangan siber.	Pendekatan mengamankan internet sambil memelihara manfaat yang diberikannya secara ofensif.	Pada saat yang sama diperhatikan pula keselamatan dan manfaat bagi para serdadu siber.
44	*"Decentralizing Cyber Command and Control"* (FitzGerald & Wright, 2014) *Disruptive Defense Papers, April*	Kualitatif	Pendekatan pengawasan dan pengendalian siber yang terdesentralisasi.	Model pengelolaan siber secara desentralisasi mengikuti sistem negara.	Tawaran ini diperuntukkan bagi sejumlah negara yang memiliki beberapa karakteristik tertentu.
45	*"Challenges to Cyber Sovereignty and Response Measures"* (Xu, 2020)	Kualitatif	Tantangan kedaulatan siber dalam dunia peperangan moderen.	Ragam tantangan dalam mempertahankan kedaulatan siber serta aksi terhadap mereka yang melanggarnya.	Fokus pembahasan pada bagaimana membalas serangan yang terjadi.

	World Economy and International Relations, 64(2)				
46	*"Sovereignty Over Cyber Territories"* (Dilisen, 2018) *International Journal of Interdisciplinary Civic and Political Studies, 13(3–4)*	Kualitatif	Diskursus mengenai isu kedaulatan dalam konteks perbatasan teritori fisik.	Teknik mengamankan teritori siber yang berada di luar wilayah negara.	Pembahasan lebih bersifat deskripsi dibandingkan dengan pemberian rekomendasi (preskripsi).
47	*"Research on Cyberspace Sovereignty"* (Shen, 2016) *Chinese Political Science Review, 1(1)*	Kualitatif	Kumpulan hasil penelitian mengenai kedaulatan siber.	Berbagai pandangan mengenai strategi dan kiat mengembangkan sistem kedaulatan siber yang efektif, efisien, dan terkendali.	Contoh lebih banyak diberikan dari negara barat.
48	*"Against Sovereignty in Cyberspace"* (Mueller, 2019)	Kualitatif	Paparan mengenai perlawanan berbagai pihak terkait dengan isu kedaulatan siber.	Tantangan berbagai negara terhadap konsep kedaulatan siber yang mengancam prinsip-prinsip demokrasi.	Perdebatan bersifat terbuka tanpa ada kesimpulan yang tegas mengenai solusi yang ditawarkan.

	International Studies Review				
49	*"Enabling Cyber Sovereignty: With Knowledge, Not with National Products"* (Schläger et al., 2017) *Digital Marketplaces Unleashed*	Kualitatif	Suatu kritik terhadap bagaimana negara-negara mencoba membangun kedaulatan siber melalui penggunaan produk dalam negeri.	Kesalahan pandangan terhadap pendekatan kedaulatan dengan melakukan blokade terhadap produk-produk teknologi dari negara luar.	Dijelaskan bagaimana unsur paling penting adalah terkait dengan pengetahuan, bukan pada kemandirian produk sistem dan teknologi informasi.
50	*"A Review of Major Viewpoints on Cyber Sovereignty around the World"* ("A Review of Major Viewpoints on Cyber Sovereignty around the World," 2016) *Chinese Journal of Engineering Science, 18(6)*	Kualitatif dan kuantitatif melalui pendekatan komparatif antara berbagai model kedaulatan siber	Kajian utuh terhadap sejumlah pandangan mengenai kedaulatan siber di seluruh dunia.	Mempelajari kesamaan pandangan negara-negara yang bersepakat mengenai prinsip perlunya menjaga kedaulatan siber.	Mendeskripsikan secara esensial berbagai pandangan dan prinsip yang dipakai sebagai landasan dalam berfikir dan membuat kebijakan.
51	*"Adapting the Current National Defence Doctrine to Cyber Domain"*	Kualitatif	Tawaran menselaraskan doktrin pertahanan negara dengan aktivitas pada domain siber.	Teknik memutakhirkan doktrin pertahanan negara dengan mengintegrasikan arena siber ke dalamnya.	Preposisi yang dipergunakan adalah didefinisikannya domain siber sebagai ranah strategis.

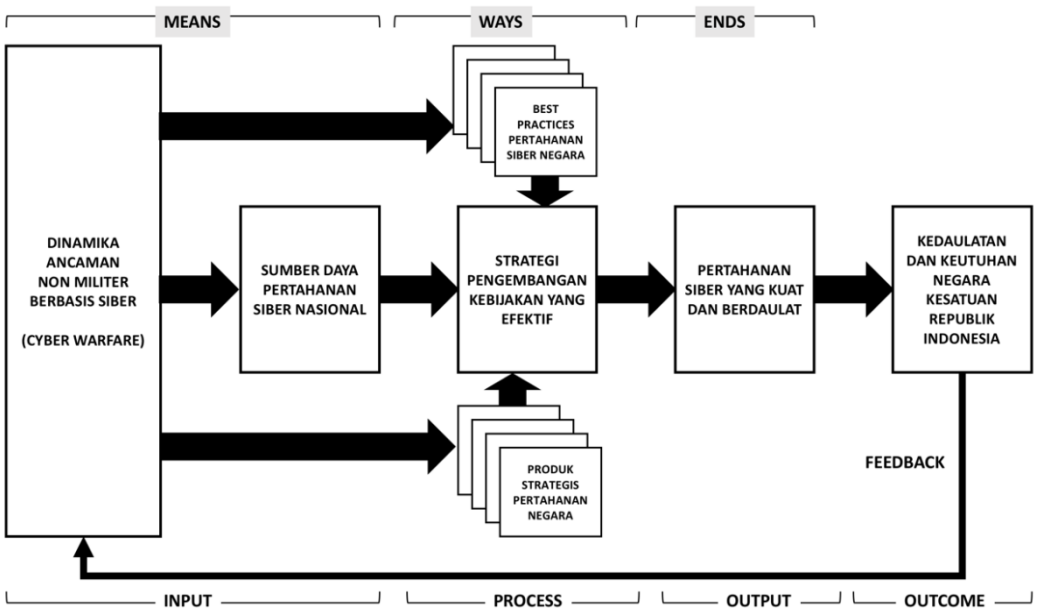
	(Tuukkanen, 2013) *International Journal of Cyber Warfare and Terrorism, 1(4)*				
52	*"Generals in Cyberspace: Military Insights for Defending Cyberspace"* (Campbell, 2018) *Orbis, 62(2)*	Kualitatif	Pendekatan mempertahankan arena siber dengan menggunakan model militer.	Pandangan militer dan beragam kementerian pertahanan terhadap keberadaan ranah siber.	Teori kepemimpinan militer menjadi cara yang dipergunakan sebagai tawaran.
53	*"Cyber War and Cyber Power - Issues for NATO Doctrine"* (Hunker, 2010) *Reseach Division. NATO Defense College, 62*	Kualitatif	Diskursus dan debat seputar doktrin yang dikeluarkan NATO.	Doktrin NATO dalam menyeimbangkan kekuatan antar negara anggotanya di bidang pertahanan siber.	Fokus perdebatan terletak pada aspek perang siber dan kekuatan siber.
54	*"The Role of Effects, Saliencies and Norms in U.S. Cyberwar Doctrine"*	Kualitatif	Peran strategis doktrin siber Amerika Serikat dalam era moderen.	Doktrin perang siber Amerika Serikat dalam konteks tata kelola arena siber dunia.	Pembahasan fokus pada norma-norma yang berlaku.

	(Farrell & Glaser, 2016) *SSRN Electronic Journal*				

Sumber : Daftar Penelitian Relevan Terdahulu (hasil kompilasi berbagai sumber)

Kerangka Pemikiran

Berdasarkan tujuan penelitian beserta literatur yang terkait dengannya, didukung oleh sejumlah riset pendahuluan, maka dikembangkan kerangka berpikir sebagaimana terlihat pada diagram berikut.



Gambar 2. 10 Kerangka Berpikir Penelitian

Sumber : Kerangka Berpikir Penelitian (dikembangkan oleh peneliti)

Outcome

Manfaat akhir yang ingin dicapai dari penerapan hasil penelitian adalah terjaganya kedaulatan dan keutuhan Negara Kesatuan Republik Indonesia. Kondisi ini selaras dengan tujuan negara yaitu melindungi segenap bangsa

Indonesia dan seluruh tumpah darah Indonesia – melalui kemampuan bertahan dari berbagai ancaman dari dalam maupun luar negeri.

Output | Ends

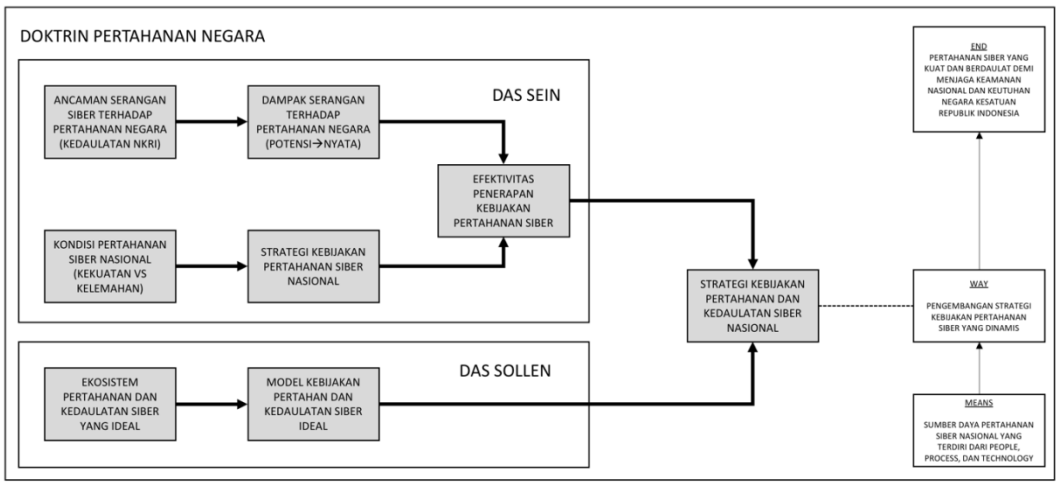
Obyektif akhir tersebut hanya bisa tercapai apabila di era moderen ini Indonesia memiliki pertahanan siber yang kuat dan berdaulat. Perang dan pertempuran siber terjadi setiap hari dalam berbagai skalanya, sehingga hanya dengan pertahanan yang kuatlah maka Indonesia dapat terhindar dari segala marabahaya. Oleh karena itulah maka penerapan hasil penelitian secara efektif diharapkan memperkuat pertahanan siber di Indonesia.

Input | Means

Ancaman siber bukan lagi merupakan potensi tapi telah menjelma menjadi situasi aktual yang mengglobal. Perang siber telah terjadi di mana-mana dan semakin intens serta kompleks keberadaannya. Sejumlah negara besar telah mengalami banyak gangguan terhadap keutuhan dan kedaulatan negara akibat jenis serangan abad ke-21 dimaksud. Indonesia telah berusaha sekuat tenaga merancang dan mengembangkan sistem pertahanan sibernya agar dapat terhindar dari kehancuran akibat dampak dari perang siber ini.

Process | Ways

Belajar dari peristiwa dan pengalaman negara maju, dibutuhkan strategi penyusunan regulasi dan kebijakan yang efektif agar negara dapat mempertahankan dirinya dari berbagai katastrofi maupun kehancuran yang berpotensi diakibatkan oleh serangan siber. Di sinilah diperlukan studi mendalam karena mengembangkan kebijakan pertahanan siber yang berdaulat berhadapan dengan sejumlah tantangan kompleks. Jika kerangka berpikir tersebut difokuskan lebih lanjut hingga memiliki relasi prosedural dengan rumusan dan tujuan penelitian yang telah diformulasikan, maka dapat dilihat langkah-langkah logis rancangan tahapan penelitian sebagai berikut.



Gambar 2. 11 Kerangka Prosedural Penelitian

Sumber : Kerangka Prosedural Penelitian (dikembangkan oleh peneliti)

Das Sein

Pemicu utama dari dilakukannya penelitian ini adalah adanya ancaman siber terhadap pertahanan negara, yang berpengaruh secara langsung terhadap kedaulatan NKRI. Adanya ancaman riil yang telah memporak-porandakan sejumlah negara lain ini perlu dianalisa dampaknya terhadap pertahanan negara Indonesia. Pada saat yang sama, perlu dilakukan pula kajian terhadap kondisi pertahanan siber nasional yang dimiliki saat ini serta strategi kebijakan pertahanan siber yang diberlakukan. Hasilnya adalah tingkat efektivitas penerapan kebijakan pertahanan siber yang dimiliki Indonesia sebagai negara berdaulat.

Das Sollen

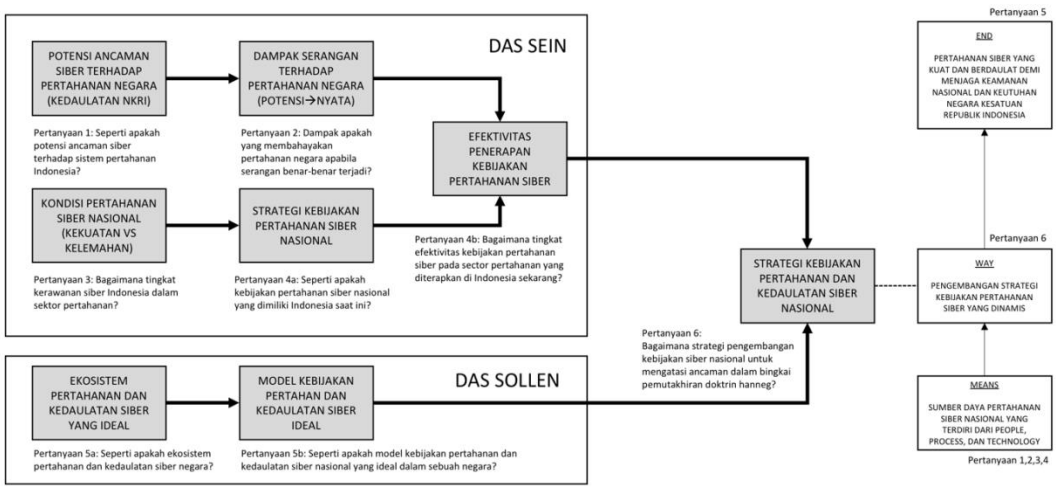
Simultan dengan melakukan kajian terhadap kondisi yang ada saat ini, dipelajari pula situasi ideal yang seharusnya terjadi dalam sebuah negara terkait dengan pertahanan siber. Melalui studi literatur, *benchmarking*, dan *best practices* dari negara-negara lain, dipelajarilah ekosistem pertahanan dan kedaulatan siber yang ideal dengan menggunakan pendekatan sistem dinamis. Berbasis pada hasil studi tersebut dikembangkanlah model kebijakan pertahanan dan kedaulatan siber ideal yang harus dimiliki oleh Indonesia.

Kajian terhadap *Das Sein* dan *Das Sollen* ini akan melahirkan sebuah gap yang perlu menjadi dasar pembuatan strategi kebijakan pertahanan dan kedaulatan siber nasional yang diusulkan untuk diadopsi oleh Indonesia sebagai sebuah negara kesatuan.

Tujuan akhir atau *end* yang diinginkan pada dasarnya adalah rasa aman dari negara karena memiliki pertahanan siber yang kuat dan berdaulat penuh. Pada saat ini, Indonesia telah memiliki sejumlah sumber daya, kebijakan, infrastruktur, dan suprastruktur (baca: *people, process, technology*) yang tersebar di seluruh wilayah tanah air demi menjaga pertahanan dan kedaulatan siber. Seluruh aset *tangible* maupun *intangible* yang merupakan *means* ini harus dikelola dan dikembangkan sedemikian rupa agar dapat mencapai target akhir yang diinginkan. Oleh karena itulah dibutuhkan sebuah *way* atau strategi penyusunan kebijakan pertahanan siber yang efektif, efisien, dan berdaulat penuh.

Keseluruhan rangkaian proses di atas dijalankan dalam bingkai Doktrin Pertahanan Negara yang dilahirkan yang dilahirkan dari Tujuan Negara Kesatuan Republik Indonesia dalam lingkungan strategis yang dinamis (Indonesia, 2015; Riana Nugraha, 2017). Dalam konteks ini diharapkan terjadi pemutakhiran doktrin pertahanan negara dimana di dalamnya secara eksplisit dinyatakan doktrin terkait dengan pertahanan siber (baca: rezim siber) sebagai basis pengembangan model kedaulatan siber yang menjadi salah satu komponen dalam sektor pertahanan negara (Chotimah, 2019; Sutrisno, 2016). Adapun strategi negara yang harus disusun dan dikembangkan agar obyektif dimilikinya pertahanan siber yang kuat tercapai, dengan berbekal sumber daya kolektif yang dimiliki segenap bangsa Indonesia (Arganata, 2019). Terlihat dalam

diagram bagaimana kedaulatan siber menjadi *ends* atau target akhir dari pengembangan strategi yang ada (Corn & Taylor, 2017). Kebijakan-kebijakan publik yang dikembangkan harus bersifat holistik dan komprehensif, sehingga tidak terjadi tumpang tindih peran dan tanggung jawab berbagai institusi negara maupun masyarakat dalam mengimplementasikannya (Islami, 2018).



Gambar 2. 12 Pertanyaan Penelitian dalam Kerangka Prosedural

Sumber : Pertanyaan Penelitian dalam Kerangka Prosedural

(dikembangkan oleh peneliti)

Gambar di atas memperlihatkan bagaimana kerangka berpikir yang dikembangkan akan dipergunakan sebagai tahapan prosedural dalam menjawab keseluruhan pertanyaan penelitian. Kerangka berpikir ini pula yang akan menjadi basis dalam penetapan metoda dan instrumen yang tepat dipergunakan selama proses penelitian berlangsung.

Melalui kerangka ini dapat dilihat bahwa secara simultan, fokus pertama yang dilakukan dalam penelitian adalah menjawab pertanyaan 1,

pertanyaan 3, dan pertanyaan 5a – karena sifatnya yang klaster, tidak saling berkaitan secara prosedural.

Langkah berikutnya adalah menjawab pertanyaan 2, pertanyaan 4a, dan pertanyaan 5b. Sebagaimana terlihat pada diagram, jawaban pertanyaan 5a dan pertanyaan 5b berasal dari studi pustaka dan literatur, sehingga menggambarkan kondisi ideal yang diinginkan (*das sollen*). Sementara setelah pertanyaan 2 dan pertanyaan 4a dijawab, akan menjadi input untuk menjawab secara detil pertanyaan 4b – yang merupakan kondisi terkini dan termutakhir (*das sein*).

Melalui kajian analisa gap dari hasil menjawab pertanyaan 4b dan pertanyaan 5b, maka dapat dikembangkan strategi penyusunan kebijakan pertahanan siber yang pada dasarnya merupakan jawaban terhadap pertanyaan penelitian 6.