KESIMPULAN DAN REKOMENDASi

Kesimpulan

Berdasarkan langkah-langkah penelitian yang dilakukan dengan menggunakan *soft-system methodology*, maka dapat dijawab seluruh pertanyaan penelitian sebagaimana dirumuskan pada bab terdahulu. Berikut adalah kesimpulan dari jawaban penelitian dimaksud.

Pertama, ancaman serangan siber yang membayangi Indonesia meningkat secara drastis dari masa ke masa. Dari 15 (lima) belas tren serangan yang disinyalir akan terjadi dalam 5-10 tahun ke depan, terdapat 8 (delapan) jenis serangan yang perlu dicermati oleh sektor pertahanan dan militer di Indonesia, masing-masing adalah pencurian identitas *(identity theft)*, pembocoran data *(data breach),* mata-mata siber *(cyber espionage)*, software perusak *(malware)*, pelumpuhan layanan sistem *(distributed denial of services)*, serangan dari dalam *(insider threat)*, penyanderaan sistem *(ransomware)*, dan pengambilalihan/pemakaian sumber daya komputasi *(cryptojacking)*. Setiap hari-harinya disinyalir terdapat 2 hingga 2,5 juta serangan diluncurkan ke dalam situs-situs penting Indonesia, dan senantiasa meningkat setiap tahunnya. Jumlah serangan yang berasal dari dalam maupun luar negara relatif seimbang dengan berbagai motivasi, modus, pendekatan, dan kompleksitas yang berbeda-beda.

Kedua, dampak ancaman dan serangan yang terjadi berpotensi membahayakan pertahanan negara, terutama dalam konteks kedaulatan, keutuhan bangsa, keselamatan masyarakat, dan keamanan nasional. Gangguan yang membahayakan tersebut adalah sebagai berikut: (i) penyerangan terhadap infrastruktur vital/kritis nasional guna menghentikan operasional infrastruktur vital yang menguasai hajat hidup orang banyak seperti listrik, air, energi, transportasi, dsb.; (ii) penyadapan sistem komunikasi dan koordinasi pertahanan untuk mengetahui aktivitas dan kegiatan rahasia dalam sektor pertahanan dan militer, baik yang telah dan akan dilakukan; (iii) pengambilalihan kendali terhadap alutsista berbasis digital yang bertujuan untuk mengoperasikan dan mengontrol alutsista dari jarak jauh agar dapat melakukan aktivitas yang diinginkan tanpa

dapat dicegah oleh pemiliknya; (iv) penyabotan terhadap sistem pusat kendali (*command center*) dengan tujuan membuat pusat kendali pertahanan dan militer tidak bekerja sebagaimana mestinya sehingga menghambat pemantauan, pengorganisasian, dan pengambilan keputusan strategis; (v) pencurian data dan informasi penting mengenai pertahanan negara guna mendapatkan data dan informasi rahasia mengenai pertahanan negara yang dapat dipergunakan sebagai referensi dalam melakukan berbagai kegiatan yang merugikan lawan; (vi) pelumpuhan sistem informasi dan teknologi pada sektor pertahanan hingga mengakibatkan tidak dapat dipergunakan atau terganggunya operasional sistem teknologi informasi yang berada dalam sektor pertahanan; (vii) penyesatan fakta melalui disinformasi dan misinformasi (propaganda) demi mengadu-domba berbagai pihak agar saling berseteru melalui penyebaran informasi yang salah atau bohong; (viii) perusakan sistem dan fasilitas teknologi informasi pertahanan guna menghancurkan sumber daya komputasi (terutama perangkat keras, infrastruktur, jaringan, dan fasilitas sarana prasarana) secara fisik sehingga tidak dapat dipergunakan; dan (ix) penyusupan ke dalam sistem dan fasilitas rahasia pertahanan negara demi menyamarkan identitas untuk dapat memperoleh akses terhadap berbagai situs, sistem, dan perimeter yang bersifat strategis dan bernilai tinggi.

Ketiga, saat ini Indonesia memiliki kondisi pertahanan siber yang sangat lemah. Berbagai lembaga pemeringkat independen memberikan nilai rendah terhadap kinerja pertahanan dan keamanan siber di Indonesia. Sejumlah survei dan penelitian memperlihatkan pula rendahnya literasi dan kultur keamanan informasi masyarakat Indonesia, khususnya di kalangan sektor pertahanan negara dan militer. Berbagai kasus penyerangan dan kejahatan siber di masa lalu memperlihatkan bagaimana teknik *social engineering* sangat efektif dilakukan terhadap target sasaran di Indonesia. Berbagai data intelijen dari lembaga pemantau trafik dan sistem di Indonesia juga memperlihatkan begitu rawannya sistem teknologi dalam sektor pertahanan dan militer yang dimiliki. Hal ini mengandung arti bahwa sistem pertahanan siber nasional sangat rentan terhadap berbagai serangan dari dalam maupun luar negara. Pihak lawan atau peretas dapat dengan mudah melakukan penetrasi terhadap sistem pertahanan

Indonesia dan melakukan berbagai ekspoloitasi kerentanan yang sangat membahayakan kedaulatan negara.

Keempat, kebijakaan dan regulasi terkait dengan pertahanan siber di Indonesia masih sangat jauh dari efektif. Begitu lemahnya situasi dan kondisi pertahanan siber negara sebagai salah satu bukti manifestasi akan kurangnya beragam regulasi yang dibutuhkan untuk membangun sistem yang kuat dan kokoh. Dibandingkan dengan negara berkembang dan maju lainnya, sangat sedikit regulasi dan kebijakan terkait dengan pertahanan siber yang disusun, dimiliki, diterapkan, dan dikembangkan di Indonesia. Disamping itu, kebijakan yang selama ini disusun dan dikembangkan dinilai memiliki kualitas yang relatif rendah – karena tidak mengalami pemutakhiran sesuai dengan kemajuan jaman dan perkembangan teknologi. Rendahnya literasi dan kultur masyarakat juga merupakan bukti tidak efektifnya kebijakan yang ada dalam meningkatkan pertahanan siber secara holistik. Buruknya kebijakan dari sisi kualitas dan kuantitas ini menunjukan tidak adanya *sense of urgency* dan *political will* dari para penyelenggara negara untuk membangun sistem pertahanan siber yang handal.

Kelima, Indonesia perlu membangun model ekosistem pertahanan siber yang kokoh, kuat, mandiri, dan berdaulat sesuai dengan postur dan karakteristik ancaman, serangan, dan karakteristik bangsa. Ekosistem yang dibangun harus terdiri dari sebelas komponen penting yang terhubung antara satu dan lainnya, yaitu: (i) regulasi atau tata kelola yang efektif, efisien, dan *agile* – atau mampu beradaptasi cepat terhadap perubahan; (ii) infrastruktur telekomunikasi dan internet yang berkulalitas serta menjangkau seluruh wilayah NKRI; (iii) sumber daya manusia yang kompeten, terampil, dan berpengetahuan luas di bidang pertahanan siber; (iv) teknologi komputasi beserta perangkat keras dan perangkat lunak (aplikasi) yang beroperasi untuk menjaga pertahanan siber; (v) anggaran yang tersedia untuk membangun sistem teknologi pertahanan siber secara berkesinambungan; (vi) industri teknologi informasi dan komunikasi dalam negeri yang berpihak pada kepentingan nasional; (vii) sektor pertahanan dan militer yang teritegrasi satu dan lainnya dalam ruang siber; (viii) dukungan politik dan berbagai lembaga tinggi negara terhadap usaha membangun sistem

pertahanan siber yang kuat, mandiri, dan berdaulat; (ix) peran serta masyarakat dan komunitas dalam membela negara Indonesia di ruang siber; (x) peran strategis perguruan tinggi dalam menghasilkan SDM, ilmu pengetahuan, dan beragam produk inovatif hasil penelitian dan pengembangan; serta (xi) peran media terutama dalam meningkatkan keperdulian dan literasi warganegara terhadap pertahanan dan keamanan siber.

Keenam, rancangan model kebijakan pertahanan dan kedaulatan siber yang ideal dan fleksibel terhadap perubahan jaman paling tidak harus terdiri dari delapan komponen yang sifatnya adalah modular. Kedelapan komponen itu dibedakan dalam 3 (tiga) tahapan kebijakan, yaitu: (i) Kebijakan Nasional - berpusat pada Undang-Undang Dasar Republik Indonesia beserta Undang-Undang dan Ketetapan MPR yang berkaitan dengan pertahanan negara; (ii) Kebijakan Umum: berpusat pada Doktrin Pertahanan Negara yang telah dimutakhirkan dimana arena siber merupakan bagian dari “semesta” kedaulatan Indonesia sebagaimana dimaksud dalam sishankamrata; dan (iii) Strategi Kebijakan: yang terdiri dari dua domain besar, yaitu domain utama (ragam kebijakan terkait dengan domain perlindungan siber, pertahanan siber, penyerangan siber, dan peperangan siber) dan domain pendukung (ragam kebijakan terkait tata kelola pertahanan siber berorientasi pada *people, process,* dan *technology*). Strategi pengembangan kebijakan yang direkomendasikan adalah bersifat modular, dimana terdiri dari sistem dan sub-sistem kebijakan pertahanan siber yang terkait satu dan lainnya, namun dapat dengan mudah dimutakhirkan sesuai perkembangan jaman tanpa harus membutuhkan waktu lama untuk menyusun, mengembangkan, dan menerapkannya. Perlu diperhatikan bahwa Kebijakan Nasional adakah kumpulan dari regulasi yang mengikat seluruh institusi di Indonesia, sementara Kebijakan Umum berpusat pada Doktrin Pertahanan Siber Negara yang disusun, dikembangkan, dan dikeluarkan secara kolektif oleh seluruh kementerian koordinator dalam bentuk *omnibus law*. Sementara Strategi Kebijakan yang meliputi perlindungan, pertahanan, penyerangan, dan pertahanan siber disusun oleh Kementerian Pertahanan Republik Indonesia.

Rekomendasi

Berbasis pada hasil penelitian yang telah dilakukan yang direfleksikan pada kondisi termutakhir, dapat disampaikan sejumlah rekomendasi terhadap pimpinan dan penyelenggara negara selaku pembuat kebijakan sebagaimana disampaikan berikut ini.

Rekomendasi Teoritis

Hasil penelitian ini menghasilkan sejumlah temuan dan artefak yang memberikan kontribusi pada dunia ilmu pengetahuan, terutama dalam bidang strategi pertahanan, pertahanan siber, kebijakan kontemporer, dan teknologi informasi. Temuan tersebut diperoleh ketika peneliti melakukan pendalaman untuk menjawab keenam pertanyaan penelitian. Berikut adalah rekomendasi teoretis yang direkomendasikan:

1. Klasifikasi dan taksonomi jenis ancaman serangan siber pada sektor pertahanan yang dihasilkan pada penelitian ini dapat menjadi referensi bagi berbagai penelitian pengembangan model dalam dunia pertahanan dan keamanan siber.

2. Penggabungan model Bayesian Network, teori *Graph*, dan *Cause-Effect* dalam menilai dampak yang dihasilkan oleh beragam serangan siber dapat dijadikan model dalam menilai tingkat risiko yang dihadapi sebuah institusi.

3. Tingkat pertahanan siber sebuah negara dapat diukur dengan menggunakan pendekatan triangulasi antara hasil *penetration test, vulneability analysis, intelligence analysis,* pemeringkatan lembaga, dan survei – sehingga memberikan gambaran yang utuh bagi mereka yang ingin mengetahui kekuatan pertahanan perimeter siber.

4. Perlunya pemutakhiran terhadap konsep doktrin pertahanan siber negara yang holistik dan komprehensif, mengingat wilayah negara

di dunia dalam persepektif moderen secara *de facto* maupun *de jure* dapat meliputi darat, laut, udara, antariksa, dan siber.

5. Kajian terhadap berbagai *good practices* pertahanan siber beragam negara bermuara pada pengembangan ekosistem pertahanan siber yang terintegrasi dengan postur dan karakteristik pertahanan negara – sehingga adalah tugas pemerintahan negara dalam melakukan kajian terhadap ekosistem pertahanan siber nasional yang perlu diadopsi.

6. Kerangka model pertahanan siber yang komprehensif dan holistik sebagaimana dihasilkan dalam penelitian ini dapat melengkapi teori seputar pengembangan kebijakan yang *agile* sebagai jawaban terhadap sulitnya kebijakan menyesuaikan diri dengan perkembangan teknologi yang sedemikian pesat.

Rekomendasi Praktis

Berdasarkan hasil kajian empiris yang dilakukan dalam penelitian ini, sejumlah inisiatif perlu dilakukan oleh penyelenggara negara guna memastikan terbangunnya sistem pertahanan siber yang kuat, kokoh, mandiri dan berdaulat. Rekomendasi yang perlu untuk dilakukan adalah sebagai berikut:

1. Sudah saatnya pemerintah terutama Kementerian Pertahanan dan Panglima TNI memberikan perhatian khusus terhadap pentingnya mengantisipasi beragam ancaman serangan siber yang berpotensi mengganggu kedaulatan negara dan keamanan nasional.

2. Berbagai aset digital siber strategis dalam lingkungan pertahanan dan militer harus diidentifikasi dan dilakukan asesmen risiko terhadapnya, agar dapat diperoleh gambaran holistik mengenai dampak serangan siber terhadap sistem pertahanan negara.

3. Hasil *penetration test* dan *vunerability analysis* maupun kajian lembaga independen dunia merupakan sinyal perlunya negara

melakukan mitigasi risiko terhadap beragam sistem dan aset strategis pertahanan yang sangat rentan dan lemah – sebab jika tidak akan sangat membahayakan bangsa dan negara.

4. Seluruh regulasi yang secara langsung maupun tidak langsung berhubungan dengan ruang siber harus diharmonikasikan satu dan lainnya, agar keberadaannya justru memperkuat satu dan lainnya, bukan sebaliknya yang justru dapat memperlemah kedaulatan dan kemandirian pertahanan siber nasional.

5. Ekosistem pertahanan siber negara perlu dibentuk dan dikembangkan bersama secara kolektif oleh berbagai pemangku kepentingan dalam wilayah NKRI, agar keberadaannya mendapatkan dukungan dari semua pihak – sehingga koordinasi, kolaborasi, dan kooperasi dapat dijalankan dengan mudah.

6. Model penyusunan regulasi terkait pertahanan siber harus dimutakhirkan agar dapat menyesuaikan diri dengan kecepatan perkembangan teknologi dan dinamika lingkungan strategis pada era revolusi industri 4.0.