BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang peneliti dapatkan selama melakukan penelitian mengenai Strategi Pertahanan Siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia, adala dari pertanyaan penelitian dari rumusan masalah mengenai “Bagaimana faktor-faktor kendala dalam membangun sistem siber guna menghadapi ancaman sibe?” dan pertanyaan yang kedua dari rumusan masalah mengenai “Bagaimana strategi pertahanana siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia?” peneliti telah mendapatkan jawaban dari pertanyaan penelitian yang telah dijelaskan di bawah ini sebagai berikut:

5.1.1 Faktor-Faktor Kendala Dalam Membangun Sistem Siber Guna Menghadapi Ancaman Siber

Penulis telah mendapatkan hasil analisis mengenai terdapatnya faktor-faktor kendala sistem siber yang dapat menghambat kemampuan kinerja dari Pushansiber. Dapat dilihat faktor kendala yang terbesar di Pushansiber adalah anggaran dan sumber daya manusia. Pemerintah belum memberikan perhatian yang serius dalam memberikan anggaran khusus untuk siber. Dari anggaran dapat membangun dan mengembangkan sistem sibernya kembali dari sisi *hardware*, *software*, inrfrastrukutr dan *firmware* nya. Kemudian pada sumber daya manusianya juga belum terpenuhi dalam sisi kuantitas seperti pemenuhan kuota yang memiliki kemampuan siber masih belum terpenuhi dan kualitasnya seperti pemberian pendidikan, sertifikasi internasional, pelatihan dan melakukan kerja dinas.

Maka apabila dilihat dari teori yang digunakan seperti teori Ilmu pertahanan belum dapat diterapkan untuk dapat menjaga dan melindungi sepenuhnya yang dilihat belum siap dan kuat nya sistem pertahanan siber. Dari teori ilmu pertahanan yang memiliki sistem pertahanan semesta belum dapat di terapkan karena minimnya edukasi, pemahaman dan keahlian pada bidang IT. Pada regulasi juga masih terdapatnya ketimpang tindihan yang mengakibatkan belum harmonis. Seharusnya juga melakukan kerjasama juga yang baik dan jujur pada industri pertahanan agar tidak ada keberpihakan satu dengan yang lain agar anggaran juga perlu di tingkatkan.

Pada teori strategi dalam membangun sistem siber juga belum berjalan dan belum di terapkan yang dikarenakan semua ini membutuhkan perhatian serius dan khusus dari semua pihak. Untuk menjalankan suatu strategi, perlu adanya keharmonisan dari tiap pimpinan agar strategi dapat berjalan dengan semestinya dan adanya dukungan penuh dari semua pihak.

Pada teori SWNSF juga perlu dilakuakan pembangunan dan pengembangan kembali untuk dapat meningkatkan dan memperkuat sistem pertahanan siber. Posisi Pushansiber masih dalam posisi lemah dalam sektor sistem siber yang dikarenakan banyaknya faktor kendala yang dimiliki. Dan pada teori keamanan jaringan sistem juga masih sangat lemah karena belum adanya dukungan anggaran dari pemerintah untuk dapat membeli *software* untuk dapat melakukan pengamanan yang mutakhir guna menghadapi ancaman dan serangan siber yang ada.

5.1.2 Strategi Pertahanan Siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia Dalam Meningkatkan Kapabilitas Pada Sistem Siber

Berdasarkan dari hasil penelitian dan juga pembahasan yang sudah di uraikan pada Bab 4 diatas, maka dapat disimpulkan bahwa strategi pertahanan siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia dengan menjalankan Peraturan Menteri Pertahanan Republik Indonesia No. 82 Tahun 2014 terkait pedoman pertahanan siber menjadikan acuan yang bertujuan untuk meningkatkan kapabilitas dan selaras dalam membangun sistem siber pada sektor sumber daya manusia, perangkat keras, perangkat lunak, infrastruktur, frimware dan anggaran.

Dalam Peraturan Menteri Pertahanan Republik Indonesia No. 82 Tahun 2014 mengenai pedoman pertahanan siber dalam meningkatkan kapabiltas yang dirasa masih kurang dan perlu melakukan pengembangan dan peningkatan pada sumber daya manusia yang memainkan peran yang sangat penting dan menjadikan aset utama dalam *cyber security*. Ini menjadi faktor kendala yang besar.

Apabila melihat dari keadaan yang sedang dialami oleh Indonesia dalam pertahanan siber yang sangat lemah. Dari beberapa badan pemeringkat juga telah menjelaskan bahwa persentase yang rendah pada kemampuan pertahanan dan keamanan siber di Indonesia. Berbagai macam modus, pendekatan, motivasi dan lain-lain yang berbeda. Karena setipa harinya banyaknya serangan yang diberikan pada situs penting di Indonesia dan kasus tersebut setiap tahunnya selalu meningkat. Terdapat nya berbagai kasus penyerangan dan adanya kejahatan siber yang menunjukkan bagaimana dari kemampuan pada *social engineering* yang dimanfaatkan untuk dilakukan kepada target sasaran di Indonesia.

Banyaknya gangguan yang dapat membahayakan pertahanan negara pada lingkup kedaulatan negara, keutuhan, keselamatan dan keamanan bangsa Indonesia terhadap adanya ancaman dan serangan yang dikarenakan tidak didukung oleh infrastruktur vital/kritis nasional, *hardware, software* dan *firmware*. Untuk dapat memiliki pertahanan siber yang ideal harus memiliki anggaran khusus untuk dapat melakukan pembangunan dan pengembangan kembali dalam rangka membangun sistem pertahanan siber. Apabila belum memiliki Aaggaran juga dapat menjadi faktor kendala.

Dalam meningkatkan kapabilitas pada sistem siber dengan kondisi pertahanan siber yang masih lemah. Jumlah serangan yang berasal dari luar dan dalam relatif seimbang dengan rendahnya kultur masyarakat dan literasi memberikan bukti bahwa belum efektif pada kebijakan yang ada guna meningkatkan pada kuantitas dan kualitas yang menunjukkan bahwa permasalahan ini belum dianggap serius, penting dan *political will* dari para pemerintah dalam rangka pengembangan dan membangun sistem pertahanan siber yang kuat dan handal.

Peneliti dapat menelaah dengan menggunakan teori strategi yaitu dapat membuat alur yang pertama dengan membuat ekosistem siber atau fenomena pada *cyberwar*, *cyber crime* dan lain-lain itu seperti apa, yang kemudian memetakan ancaman dan serangan seperti: adanya data palsu, interupsi, datanya menghilang, satelit lumpuh dan lain-lain yang mana ini dapat merusal, menghambat dan menghancurkan negara. Kemudian melakukan perubahan pada pola pikir yang menjadikan pembangunan dan pengembangan sistem siber menjadi acuan sebagai pertahanan negara dalam keamanan nasional. Lalu melihat dan memahami apa saja kerentanan yang nantinya dihapadi seperti adanya ancaman, serangan siber, peretas dan lain-lain. Kemudian merubah dari kultur dari lintas generasi, kebiasaan dan literasinya. Perlunya adanya peningkatan dan memperkuat pada sektor manusia dan teknologinya yang mana nantinya dapat berkolaborasi satu sama lainnya. Tata kelola dan regulasinya harus

segera di harmoniskan agar dapat berjalan semestinya pada strateginya dalam membangun sistem siber di Pushansiber.

5.2 Saran

5.2.1 Teoritis

Berbasis dari hasil penelitian dan kesimpulan di atas, peneliti memberikan beberapa saran kepada pemerintah, masyarakat dan peneliti selanjutnya, seperti:

a. Kepada akademisi/peneliti selanjutnya disarankan untuk dapat melakukan penelitian lebih lanjut mengenai strategi pembangunan, pengembangan dan penguatan sistem siber dalam perguruan tinggi. Selain itu, hasil penelitian ini diperoleh dapat dipakai sebagai acuan untuk dapat mengembangkan ilmu pertahanan dan ilmu peperangan asimetris di Indonesia.
b. Kepada pemerintah untuk melindungi dan menjaga agar segera membuat dan menerapkan langsung dalam mengharmoniskan regulasi mengenai siber di Indonesia agar dapat selaras, melakukan dan mengadakan kerjasama pada tiap lembaga seperti BSSN atau yang lain yang memiliki kemampuan pada bidang IT dan juga melakukan kerjasama pada industri untuk dapat meningkatkan dan memperkuat pertahanan Indonesia.
c. Kepada pemerintah dan Kementerian Pertahanan Republik Indonesia agar dapat melakukan dan menerapkan pertahanan yang baik yang sesuai pada Undang-Undang No 34 tahun 2004 harus melakukan manajamen yang baik dan harmonis dalam melakukan manajemen pada regulasi pertahanan, sumber daya manusia, anggaran, industri dan teknologi pertahanan, sumber daya informasi, intelijen, potensi pertahanan dan lain-lain agar dapat pertahanan Indonesia menjadi kuat dan siap.

d. Kepada pemerintah dan terutama pada Kementerian Pertahanan Republik Indonesia disarankan untuk melakukan strategi dan langkah untuk dapat membangun sistem siber yang baik, seperti: membuat alur ekosistem siber, memetakan ancaman dan serangan, membuat perubahan pada pola pikir yang menjadikan pembangunan dan pengembangan sistem siber, memberikan pemahaman mengenai apa saja kerentanan yang nantinya dihapadi, melakukan perubahan dari kultur dari lintas generasi, kebiasaan dan literasinya. Kemudian memberikan pelatihan, pendidikan dan lain-lain untuk dapat meningkatkan kualitas pada sektor manusia. Melakukan pemeliharaan, melengkapi dan membeli teknologi yang baru agar dapat melakukan tugas dengan baik. Kemudian merekrut mahasiswa di seluruh Indonesia dari berbagai perguruan tinggi yang memiliki kecerdasan dan kemampuan di bidang IT agar dapat di pekerjakan di Pushansiber dan dijadikan Pegawai Negeri Sipil (PNS). Atau bahkan dapat melakukan perekrutan dari masyarakat yang memang memiliki kemampuan pada IT agar dapat di pekerjakan sebagai PNS dan maka dari itu pemerintah harus merubah peraturan agar sumber daya manusia yang memiliki kemampuan khusus di bidang IT dapat di pekerjakan sebagai PNS.
e. Kepada pemerintah terutama Kementerian Pertahanan Republik Indonesia untuk dapat membeli *renewal signature* agar dapat melakukan *update* pada *principal* nya ini dalam keamanan sistem jaringannya.
f. Untuk Universitas Pertahanan RI sebagai kampus bela negara yang nanti nya dapat membuat kajian, mata kuliah dan penelitian terkait ancaman asimetris dalam hal ini ancaman siber.

5.2.2 Praktis

a. Saran untuk Pemerintah terutama Kementerian Pertahanan memberikan perhatian yang serius dan khusus pada pentingnya sistem siber segera guna mengantisipasi berbagai macam ancaman dan serangan yang mana dapat mengganggu kemanan dan kedaulatan nasional.
b. Strategi pada Pusat Pertahanan Siber dalam upaya membangun sistem siber sudah mempunyai rencana, sistematis dan terpadu. Akan lebih baik apabila pemerintah melakukan pembangunan pada konsep doktrin pertahanan negara yang komprehensif yang dikarenakan negara memberikan dukungan dan memperdalam kemampuan sumber daya manusia, melakukan mengadopsi dan kajian kembali pada ekosisem pertahanan siber nasional. Membuat kerangka model pertahanan siber yang baik untuk dapat menyempurnakan teori pada pengembangan kebijakan terhadap sulitnya kebijakan untuk dapat menyesuaikan diri namun perkembangan pada teknologi semakin cepat.
c. Saran untuk pemerintah terutama Kementerian Pertahanan Republik Indonesia pada regulasi yang dimiliki yang memiliki keterkaitan dengan ruang siber seharusnya diharmoniskan, selaras dan seimbang agar tidak memperlemah dari sisi kedaulatan dan memberikan hambatan dalam memperkuat sistem pertahanan siber.
d. Saran untuk pemerintah terutama pada Kementerian Pertahanan Republik Indonesia harus dapat memberikan anggaran khusus dalam sistem siber guna memiliki pertahanan siber yang kuat dan siap.

e. Saran untuk pemerintah terutama pada Kementerian Pertahanan Republik Indonesia dan Pusat Pertahanan Siber pada sumber daya manusia untuk dapat memberikan pelatihan dan pendidikan nasional dan internasional, pemberian sertifikasi internasional, dan lain-lain.
f. Saran untuk pemerintah agar dapat menyalaraskan regulasi dan peraturan untuk dapat menerima sumber daya manusia yang non organik dan bukan anggota TNI. Agar dapat memperkerjakan masyrakat yang memiliki kemampuan di bidang IT untuk dapat di PNS kan guna meningkatkan dan menguatkan pertahanan siber di Indonesia.
g. Saran untuk pemerintah terutama pada Kementerian Pertahanan Republik Indonesia merekrut mahasiswa di seluruh Indonesia dari berbagai instansi yang memiliki kecerdasan dan kemampuan di bidang IT agar dapat di pekerjakan di Pushansiber dan dijadikan PNS.
h. Saran untuk pemerintah terutama pada Kementerian Pertahanan Republik Indonesia dapat membeli, melakukan pemelihaaran dan melengkapi kekurangan pada bidang *hardware*, *software*, infrstruktur dan *firmware*. Ini dilakukan untuk pertahanan negara menjadi kuat dan keamanan pada jaringan sistem juga tidak mudah rentan dirusak atau di hancurkan oleh para penjahat siber.
i. Saran untuk pemerintah terutama Kementerian Pertahanan Republik Indonesia dan Pusat Pertahanan Siber untuk melakukan identifikasi dan memetakan resiko yang nantinya dapat memberikan gambaran mengenai adanya serangan dan ancaman terhdap sistem pertahanan siber di Indonesia.

j. Saran untuk pemerintah terutama Kementerian Pertahanan Republik Indonesia dan Pusat Pertahanan Siber Melakukan mitigasi risiko dan aset strategis pertahanan yang menjadi incaran dan rentan terhadap adanya serangan dan ancaman yang dihasilkan dari *penetration test*.
k. Saran untuk pemerintah terutama Kementerian Pertahanan Republik Indonesia dan Pusat Pertahanan Siber Perlu nya membentuk ekosistem pertahanan siber bersama dengan pihak lainnya guna mendapatkan dukungan dari semua pihak yang nantinya dapat melakukan kolaborasi, koordinasi dan kooperasi dengan mudah, efisien dan tepat.