KOMPETENSI SUMBER DAYA MANUSIA PERTAHANAN SIBER SEBAGAI KOMPONEN KEKUATAN PERTAHANAN NEGARA

COMPETENCY OF CYBER DEFENSE HUMAN RESOURCES AS A COMPONENT OF NATIONAL DEFENSE POWER

Ruby Alamsyah[1], I Wayan Midhio[2], I Nengah Putra Apriyanto[3]

UNIVERSITAS PERTAHANAN INDONESIA
(ruby.alamsyah@idu.ac.id, midhio_2003_iwayan@yahoo.com, nengah.putra@idu.ac.id)

Abstrak – Sumber daya manusia (SDM) dengan kompetensi pertahanan siber merupakan pilar sekaligus komponen penting kekuatan pertahanan negara yang dibangun, ditingkatkan, dikelola, dan diberdayakan untuk menghadapi ancaman siber, demi kepentingan nasional Indonesia. Bagaimana kiranya wujud kompetensi SDM pertahanan siber, dan bagaimana potensi mewujudkannya ? Tujuan penelitian pada intinya untuk memperoleh gambaran wujud kompetensi SDM pertahanan siber. Penelitian menggunakan pendekatan kualitatif dan dengan analisis model interaktif terhadap data-data literatur seperti jurnal, dokumen, dan artikel dari sumber yang reliable. Analisis data dikolaborasikan dengan teori manajemen (fungsi POAC) terhadap tata kelola kompetensi SDM. Hasil analisis menunjukan bahwa kompetensi SDM TIK dan SDM keamanan siber belum cukup memenuhi standar kompetensi SDM pertahanan siber, namun perlu ditransformasikan melalui mekanisme pengelolaan sumber daya nasional untuk pertahanan negara.

Kata Kunci: Pertahanan Negara, Siber, Kompetensi, SDM, Manajemen

Abstract *– Human resources (HR) with cyber defense competence are a pillar as well as an important component of the national defense force which is built, enhanced, managed, and empowered to face cyber threats, for the national interest of Indonesia. What would the cyber defense HR competency look like, and what is the potential to make it happen? The main objective of this research is to obtain a description of the HR competency in cyber defense. This research uses a qualitative approach and an interactive model analysis of literature data such as journals, documents, and articles from reliable sources. The data analysis was collaborated with the theory of management (POAC function) on HR competency governance. The results of the analysis show that the competence of HR in ICT as well as HR in cybersecurity are not sufficient to meet the standards competency of HR for cyber defense, but needs to be transformed through a mechanism for managing national resources for national defense.*

Keywords: *National Defense, Cyber, Competency, HR, Management*

[1] Mahasiswa Program Pasca Sarjana (Magister) Universitas Pertahanan
[2] Dosen Universitas Pertahanan
[3] Dosen Universitas Pertahanan

Pendahuluan

Aspek pertahanan dan keamanan merupakan satu kesatuan faktor hakiki dalam menjamin kelangsungan hidup bangsa dan negara Indonesia dari berbagai bentuk ancaman yang datang dari dalam maupun luar negeri. Terlebih dengan adanya kemajuan teknologi informasi dan komunikasi (TIK) global, yang telah membawa Indonesia masuk ke dalam ekosistem baru ruang siber (cyberspace). TIK telah membawa manfaat bagi kehidupan umat manusia, namun juga menimbulkan berbagai ancaman siber (cyber threat) dengan motif dan tujuan beragam yang secara faktual dan potensial mengancam aspek pertahanan dan keamanan Indonesia. Ancaman siber turut berdampak signifikan terhadap perubahan paradigma dan konsep pertahanan dan keamanan, baik pada tataran strategis, operasional, maupun taktis, yang secara fundamental dinamika operasionalnya tidak lagi terbatas pada ranah (domain) fisik, namun telah bergeser ke ranah non-fisik.

Terdapat 3 (tiga) pilar/faktor penting dalam ekosistem cyberspace yang saling terhubung dan bergantung satu sama lain, yaitu: people (sumber daya manusia/SDM), process (proses), dan technology (teknologi) . Bila dijabarkan, di dalamnya meliputi, antara lain: teknologi sistem informasi, basis data, jaringan telekomunikasi data (internet), aplikasi, sistem komputer, dan perangkat prosesor berikut pengendali, termasuk operator (brainware), maupun manajemen (tata kelola) sistem elektronik, serta teknologi kecerdasan buatan atau *artificial intelligence* (AI). Dalam perspektif pertahanan, ancaman siber merupakan ancaman berdimensi teknologi yang karakteristiknya jauh lebih kompleks, canggih, penetratif, efektif, dan destruktif, menyebabkan gangguan terhadap penyelenggaraan pertahanan negara, serta kepentingan nasional maupun kedaulatan Negara Kesatuan Republik Indonesia (NKRI).

Dalam upaya mewujudkan kemampuan pertahanan dan keamanan terhadap ancaman siber, Kementerian Pertahanan (Kemhan) RI telah menerbitkan Peraturan Menteri Pertahanan (Permenhan) RI Nomor 82 tahun 2014 sebagai acuan persiapan, pembangunan, pengembangan dan penerapan pertahanan siber untuk Kemhan/TNI.

Dalam pedoman ini, pilar *people* (SDM) warga negara Indonesia (WNI) sebagai faktor utama/penting yang perlu (harus) dipersiapkan, dibangun, ditingkatkan, dan dikelola kompetensinya sebagai SDM pertahanan siber (*knowledge* dan *skill* serta kapasitas dan kapabilitas). Selanjutnya, berkenaan dengan topik kompetensi SDM pertahanan siber sebagai komponen kekuatan pertahanan negara untuk menghadapi ancaman siber, maka di dalam penelitian ini, yang menjadi fokus masalah adalah tentang bagaimana wujud kompetensi SDM pertahanan siber? dan bagaimana potensi untuk terwujudnya kompetensi SDM pertahanan siber? Beranjak dari fokus masalah tersebut, maka penelitian ini bertujuan untuk menganalisis tentang bagaimana wujud kompetensi SDM pertahanan siber, serta menganalisis tentang bagaimana potensi untuk terwujudnya kompetensi SDM pertahanan siber.

Beberapa penelitian terdahulu yang relevan dengan aspek kompetensi SDM pertahanan siber di dalam penelitian ini, antara lain: *Cybersecurity* dan Tantangan Pengembangannya di Indonesia[4], Peningkatan Peranan SDM Pertahanan Nasional Guna Menghadapi Perang Generasi ke Empat[5], Peningkatan Kualitas SDM di Bidang Industri Pertahanan Menuju Pertahanan Negara Yang Tangguh[6], Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional[7], Ancaman Siber Dalam Perspektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta)[8], dan Implementasi Manajemen Risiko Pertahanan Siber Kementerian Pertahanan Untuk Mendukung Pertahanan Negara[9].

[4] Handrini Ardiyanti, "*Cybersecurity dan Tantangan Pengembangannya di Indonesia*", Jurnal Politica, Vol.5, No.1, 2014, hlm.95-110.
[5] Elly Sebastian, "Peningkatan Peranan SDM Pertahanan Nasional Guna Menghadapi Perang Generasi Keempat", Jurnal Pertahanan, Vol.5, No.1, 2015, hlm.109-128.
[6] Budi Triyoga Prasetyo dan Sugeng Berantas, "*Peningkatan Kualitas SDM di Bidang Industri Pertahanan Menuju Pertahanan Negara Yang Tangguh*", Jurnal Pertahanan, Vol.5, No.1, 2015, hlm.175-195.
[7] Sugeng Santoso, "*Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional*", Jurnal Kajian Lemhanas RI, Edisi 34, 2018, hlm.43-48.
[8] Ratno Dwi Putra, Supartono, dan Deni D.A.R., "*Ancaman Siber Dalam Perspektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta)*", Jurnal Prodi Perang Asimetris, Vol.4, No.2, 2018, hlm.99-120.
[9] Andhika Doly Putra, Herlina J.R. Saragih, dan G.Royke Deksino, "*Implementasi Manajemen Risiko Pertahanan Siber Kementerian Pertahanan Untuk Mendukung Pertahanan Negara*", Jurnal Pertahanan, Vol.6, No.1, 2020, hlm.100-121.

Hasil penelitian ini dapat dimanfaatkan oleh pihak-pihak terkait khususnya Kemhan RI guna menyusun konsep kompetensi SDM pertahanan siber seiring upaya membangun kemampuan baru pertahanan siber dalam kerangka pertahanan negara. Dengan demikian penelitian ini hanya terbatas pada analisis wujud kompetensi SDM pertahanan siber sebagai komponen kekuatan pertahanan negara yang diyakini di dalamnya terdapat kompetensi SDM TIK dan SDM keamanan siber.

Kompetensi

Secara estimologi, kompetensi dimaknai sebagai kemampuan yang dibutuhkan untuk melakukan atau melaksanakan pekerjaan yang dilandasi oleh pengetahuan, keterampilan dan sikap kerja[10]. Menurut kamus besar bahasa Indonesia (KBBI) *online* kompetensi didefinisikannya sebagai kewenangan (kekuasaan) untuk menentukan (memutuskan suatu)[11]. *Spencer and Spencer* mendefinisikan sebagai karakteristik yang mendasari seseorang dan berkaitan dengan efektivitas kinerja individu dalam pekerjaannya[12]. Menurut Suparno, kompetensi adalah kecakapan yang memadai untuk melakukan suatu tugas, atau memiliki keterampilan dan kecakapan yang disyaratkan[13]. Dan menurut *Stephen and Timothy*, kompetensi merupakan *ability* (kemampuan) atau kapasitas seseorang mengerjakan berbagai tugas dalam suatu pekerjaan, di mana *ability* ditentukan oleh faktor intelektual dan fisik[14]. Dari berbagai pandangan tersebut, kompetensi dapat dimaknai sebagai kemampuan dari seseorang yang dapat terobservasi mencakup pengetahuan, keterampilan dan sikap kerja dalam menyelesaikan suatu pekerjaan atau tugas sesuai dengan standar performa yang ditetapkan.

---

[10] Keputusan Menteri Ketenagakerjaan RI No.160 Tahun 2016 tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Aktivitas Profesional, Ilmiah dan Teknis Golongan Pokok Aktivitas Kantor Pusat dan Konsultasi Manajemen Bidang Produktivias.

[11] Tim Penyusun Kamus Pusat Bahasa, "*Kamus Bahasa Indonesia*", (Jakarta: Departemen Pendidikan Nasional, 2008), hlm 743.

[12] Lyle M. Spencer and Signe M. Spencer, Competence at Work: Models for Superior Performance, (New York: John Wiley & Son Inc., 1993), hlm.9.

[13] A. Suhaenah Suparno, *Membangun Kompetensi Dasar*, (Jakarta: Direktorat Jendral Pendidikan Tinggi Departemen Pendidikan Nasional, 2001), hlm.27.

[14] Stephen P.Robbins and Timothy A.Judge, *Perilaku Organisasi*, (Jakarta: Salemba Empat, 2007), hlm.38.

Secara umum, kompetensi juga dapat dipahami sebagai kombinasi dari keterampilan (*skill*), atribut personal, dan pengetahuan (*knowledge*) yang tampak pada perilaku menjalankan tugas-tugas (*job behavior*). *Spencer and Spencer* membagi kompetensi ke dalam 5 (lima) karakteristik[15], yaitu: a) *knowledge* (pengetahuan, wujud kompetensi yang kompleks), yaitu segala informasi yang dimiliki seseorang untuk bidang tertentu; b) *skills* (keterampilan/keahlian), merupakan kemampuan untuk melaksanakan suatu tugas tertentu secara mental dan fisik; c) *motives* (motivasi) merupakan sesuatu di mana manusia secara konsisten berfikir sehingga melakukan tindakan; d) *traits* (watak) adalah kepribadian yang membuat manusia perilaku atau merespon sesuatu dengan cara tertentu (misal: tahan atau tabah menerima tekanan, kontrol dan percaya diri; dan e) *Self Concept* (jati diri) merupakan sikap dan nilai-nilai yang dimiliki. Kompetensi dapat ditingkatkan dan dioptimalkan melalui berbagai kegiatan pendidikan dan pelatihan (diklat) sesuai kepentingan organisasi. Kompetensi SDM nasional di Indonesia merujuk pada dokumen peta okupasi nasional mencakup berbagai bidang (sektor) berdasarkan standar kompetensi, kualifikasi dan level kompetensi nasional[16].

Diklat dapat didefinisikan sebagai usaha terencana dari suatu organisasi untuk meningkatkan pengetahuan, keterampilan dan kemampuan. Pendidikan dapat didefinisikan antara lain sebagai sebuah aktifitas yang memiliki maksud atau tujuan tertentu yang diarahkan untuk mengembangkan potensi yang dimiliki manusia baik sebagai manusia ataupun sebagai masyarakat dengan sepenuhnya[17]. Menurut Hasibuan, pendidikan merupakan suatu proses untuk meningkatkan keahlian teoritis, konseptual, dan moral SDM[18]. SDM yang memperoleh kesempatan diklat terprogram, kompetensinya meningkat dan cenderung lebih terampil dan profesional dibanding SDM yang mengikuti diklat tidak terprogram. Oleh karenanya, diklat terprogram

[15] Lyle M. Spencer and Signe M. Spencer, *Competence at Work: Models for Superior Performance*, (New York: John Wiley & Son Inc., 1993), hlm.10.
[16] Peraturan Menteri Tenaga Kerja dan Transmigrasi RI No.5 Tahun 2012 *tentang Sistem Standardisasi Kompetensi Kerja Nasional*.
[17] Nurkholis, "Pendidikan Dalam Upaya Memajukan Teknologi", Jurnal Kependidikan, Vol. 1 No. 1, 2013, hlm. 24-44.
[18] Malayu Hasibuan, Manajemen Sumber Daya Manusia, (Jakarta: Bumi Aksara, 2009), hlm. 54.

semakin penting dalam menunjang peningkatan kompetensi seiring tuntutan peran, tugas dan fungsi organisasi terhadap tantangan perubahan situasi dan kondisi kerja, maupun kemajuan teknologi.

Sumber Daya Manusia (SDM)

Sumber daya manusia atau SDM merupakan salah satu sumber daya di dalam organisasi. Bidang pertahanan (dalam hal ini Kemhan/TNI) mendefinisikan SDM sebagai warga negara yang memberikan daya dan usahanya untuk kepentingan bangsa dan negara[19]. Bila dikaitkan dengan aspek kompetensi SDM dalam bidang TIK, bidang keamanan siber, dan bidang pertahanan siber, dapatlah diasumsikan bahwa kompetensi SDM tersebut sebagai wujud daya dan usaha yang diberikan warga negara Indonesia, baik dalam bidang TIK, bidang keamanan siber, dan bidang pertahanan siber, untuk kepentingan bangsa dan negara Indonesia.

Kompetensi SDM Bidang TIK

SDM TIK menurut Eko Indrajit, adalah para penanggung jawab perencanaan dan pengembangan teknologi informasi (TI) dalam suatu organisasi, misal: Divisi TI, Departemen Sistem Informasi (SI), atau bagian-bagian sejenis lainnya[20]. SDM menjadi aset penting dengan kompetensinya guna memecahkan permasalahan yang dihadapi, dan selalu mencari kesempatan dalam pemanfaatan TI untuk kemajuan orgaisasinya. Bila dikaitkan dengan terminologi TIK dalam ensiklopedia bebas (*wikipedia*)[21], secara umum kompetensi SDM TIK dapat dipahami sebagai *knowledge* dan *skill* serta kapasitas dan kapabilitas SDM dalam bidang teknologi informasi (teknologi komputer, baik perangkat keras maupun lunak) dan teknologi komunikasi.

Membangun kompetensi SDM TIK merupakan tugas dan fungsi pemerintah melalui Kementerian Kominfo RI, dan hal tersebut selaras dengan *roadmap*

[19] UU No.23 tahun 2019 tentang Pengelolaan Sumber Daya Nasional (PSDN) Untuk Pertahanan Negara.
[20] Richardus Eko Indrajit, Pengantar Konsep Dasar Manajemen Sistem Informasi dan Teknologi Informasi, (Jakarta: Elex Media Komputindo, 2000).
[21] Irkham Abdaul Huda, "Perkembangan Teknologi Informasi dan Komunikasi (TIK) Terhadap Kualitas Pembelajaran di Sekolah Dasar", Jurnal Pendidikan dan Konseling, Vol.1 No.2, 2020, hlm.143-149.

pembangunan TIK nasional[22], yaitu untuk memenuhi kebutuhan SDM TIK di seluruh sektor strategis nasional, dengan titik berat pada nilai tambah pertumbuhan ekonomi dan penguatan kedaulatan bangsa. Bila dikaitkan dengan tiga sasaran strategis pengembangan SDM menuju Indonesia 2045, adalah tercapainya penguasaan pasar TIK global, kapasitas produksi nasional, dan masyarakat berbudaya TIK yang tangguh. Pada intinya SDM TIK adalah SDM yang memiliki kompetensi dalam bidang TIK untuk siap mengawaki berbagai infrastruktur TIK yang ada di berbagai sektor strategis nasional.

Gambar 1. Tiga Sasaran Strategis Pengembangan SDM
Sumber: Penyusunan Roadmap Pembangunan Sektor TIK Jangka Panjang s.d. 2045 Menuju 100 Tahun Indonesia Merdeka, 2016

Kompetensi SDM TIK tentunya diwujudkan melalui berbagai bentuk kegiatan pendidikan dan pelatihan TIK. Merujuk pada Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada TIK[23], kompetensi SDM TIK mencakup 16 (enambelas) area fungsi TIK, sebagai berikut: a) *data managemen systems*; b) *programming and software develompment*; *c) hardware and digital peripherals*; d) *network and infrastructure*; e) *operation and systems tools*; f) *information systems and technology development*; g) *IT governance and management*; h) *IT project management*;

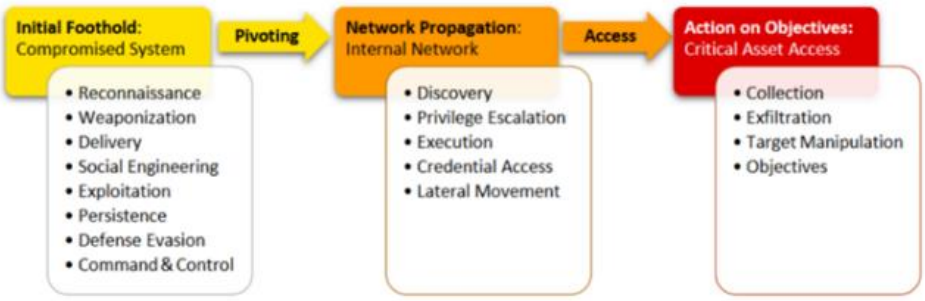
[22] Badan Litbang SDM Kominfo, Penyusunan Roadmap Pembangunan Sektor TIK Yang Mengikat Secara Jangka Panjang s.d 2045 Menuju 100 Tahun Indonesia merdeka, (Jakarta: Badan Litbang SDM Kominfo, 2016), hlm.xii.

[23] Pengesahan Kepala Badan Litbang SDM Kominfo RI, Direktur Jenderal Pembinaan Pelatihan dan Produktivitas Kementerian Ketenagakerjaan, Wakil Ketua Umum Kamar Dagang dan Industri Indonesia (Kadin) Bidang Ketenagakerjaan dan Industrial, Deputi Menteri PPN/Kepala Bappenas Bidang Kependudukan, dan ketua Badan Nasional Sertifikasi Profesi, Nomor 172/KOMINFO/ BLSDM/KS.01.07/7/2017, tanggal 27 Juli 2017 *tentang Peta Okupasi Nasional Bidang TIK tahun 2017*.

i) *IT enterprise architecture*; j) *IT security compliance*; k) *IT service management systems*; l) *IT and computing facilities management*; m) IT multimedia; n) *IT mobility and internet of things* (IoT); o) *integration application system*; dan p) *IT consultancy and advisory*.

Kompetensi SDM Bidang Keamanan Siber.

Kompetensi SDM bidang keamanan siber terwujud melalui berbagai bentuk kegiatan pendidikan dan pelatihan keamanan siber. Kompetensi tersebut merujuk pada dokumen Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber[24]. Dokumen ini juga menjadi bagian yang tidak terpisah dari Peta Okupasi Nasional TIK yang disusun dalam Kerangka Kualifikasi Nasional Indonesia (KKNI), yang memetakan berbagai jenis jabatan, okupasi, dan profesi khusus bidang keamanan siber. Kekhususan tersebut adalah dalam hal merumuskan dan mendefiniskan okupasi dan kompetensi SDM TIK aspek keamanan informasi (*information security*), dilakukan dengan pendekatan dan analisis terhadap fase-fase penanganan insiden keamanan siber yang terdiri dari tiga fase, yakni: a) fase sebelum insiden serangan siber (*before cyber attack*); b) fase ketika terjadinya insiden serangan siber (*during cyber attack*); dan c) fase setelah terjadinya insiden serangan siber (*after cyber attack*). Pendekatan dan analisis tersebut kemudian oleh BSSN dipadukan dengan *framework* "*The Unified Kill Chain*" yang dikembangkan *Cyber Security* Academy di Belanda, di mana fase-fase sebagaimana tampak pada gambar 2.



Gambar 2. Fase-Fase Pada *Framework* "*The Unified Kill Chain*"
Sumber: Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber, 2019

[24] Badan Siber dan Sandi Negara (BSSN), Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber, (Jakarta: Badan Siber dan Sandi Negara, 2019), hlm.2.

Hasil pendekatan dan analisis *framework* "*the unified kill chain*" pada peta okupasi nasional bidang TIK, teridentifikasi wujud kompetensi SDM keamanan siber mencakup 30 (tiga puluh) okupasi pada level kualifikasi 5 s.d. 9 jenjang (*level*) kualifikasi KKNI, sebagai berikut: a) kualifikasi 5, teridentifikasi 4 (empat) okupasi pada fase *before attack* dan *during attack*, yaitu: *cryptographic technician*, *cryptographic administrator*, junior cyber security, dan *cyber security operator*; b) kualifikasi 6, teridentifikasi 10 (sepuluh) okupasi pada fase *before*, *during*, dan *after attack*, yang meliputi: *ICT security product evaluator*, *cryptographic analyst*, *cryptographic module analyst*, *vulnerability assessment analyst*, *network security administrator*, *cyber security administrator*, *cyber security awareness officer*, *cyber security analyst/cyber security incident analyst*, dan *digital evidence first responder*; c) kualifikasi 7, teridentifikasi 12 (dua belas) okupasi pada seluruh fase, meliputi: *cryptographic speialist*, *cryptographic engineer*, *ICT security product lead evaluator*, *cybersecurity manager*, *network security manager*, *cybersecurity awareness lead officer*, *incident response team manager*, *information security auditor*, *threat hunter*, *penetration tester*, *cybersecurity governance officer*, dan *digital forensic analyst*; d) kualifikasi 8, teridentifikasi 5 (lima) okupasi pada fase *before attack* dan *after attack*, meliputi: *cyber risk specialist*, *security architect*, *cryptographic specialist*, *cyber incident investigation manager*, dan *cyber forensic specialist*; dan e) kualifikasi 9, teridentifikasi 1 (satu) okupasi pada seluruh fase, yaitu: *chief of information security officer*.

Secara deskriptif, kompetensi SDM keamanan siber mencakup hal-hal sebagai berikut: definisi, ruang lingkup, profil, tanggung jawab, wewenang, persyaratan, tugas utama, tugas khusus dan unit kompetensi yang dibutuhkan. Terdapat hal dari beberapa substansi deskripsi kompetensi SDM keamanan siber yang menjadikannya spesifik dibanding dengan kompetensi SDM TIK, yaitu adanya faktor dinamika dalam penyelenggaraan kegiatan operasional keamanan siber yang komprehensif meliputi *technique*, *tactic*, dan *procedure* (TTP) dalam menghadapi ancaman serangan siber; selain itu operasional keamanan siber bersifat masif (skala nasional) melibatkan

segenap pemangku kepentingan siber secara integratif; dan terkait dengan eskalasi ancaman siber, dinamika operasi keamanan siber dilaksanakan pada masa normal (damai), dan dengan tetap berpedoman pada ketentuan dan aturan hukum yang berlaku dalam kerangka keamanan nasional.

Kompetensi SDM Bidang Pertahanan Siber.

Kompetensi SDM pertahanan siber, sama sekali belum (tidak) merujuk pada dokumen peta okupasi nasional. Bidang pertahanan, dalam hal ini Kemhan dan TNI, masih merujuk pada dokumen pedoman pertahanan siber[25]. Bahwa penyediaan SDM pertahanan siber tentunya hanya dapat terwujud melalui kegiatan pendidikan dan pelatihan pertahanan siber. Hal tersebut merupakan tantangan terbesar bagi Kemhan/TNI, terutama untuk mewujudkan SDM yang kompeten dan senantiasa cepat dan sigap mengikuti dinamika perkembangan ekosistem siber seiring kemajuan teknologi dan perubahan sosial masyarakat. Kemhan/TNI memandang bahwa strategi pengembangan SDM harus didukung oleh program peningkatan kompetensi SDM yang berkesinambungan.

Secara umum, konsep (rumusan) kompetensi SDM pertahanan siber sebagaimana tercantum pedoman pertahanan siber, antara lain: a) memiliki *cybersecurity awareness*; b) memiliki pengetahuan dan keterampilan dalam hal: *information security and risk management*, *access control systems and methodology*, *cryptography*, *physical security*, *telecommunications and network security*, *security architecture and models*, *business continuity planning and disaster recovery plan*, *applications security*, *operations security*, *legal, regulations, compliance and investigations*, dan *implementasi SNI 27001*; c) memiliki pengetahuan dan keterampilan penanganan insiden sekurang-kurangnya meliputi: *digital forensic*, *incident response*, *operation system*, dan *data communication networking*; d) pengetahuan dan keterampilan melakukan *penetration test* sekurang kurangnya meliputi: *information security in general*, *using penetration testing tools*, *IT examination and reporting*, dan *web based application developing*; e) *system assurance*;

[25] Peraturan Menteri Pertahanan RI No.82 Tahun 2014 tentang Pedoman Pertahanan Siber.

f) pengetahuan dan ketrampilan sistem meliputi: *network security*, *operating systems security*, *systems infrastructure and database*, *security*, *digital control system*, dan *system development*; dan g) pengetahuan dan kemampuan merehabilitasi dan rekonstruksi kerusakan yang terjadi pada jaringan TIK dan muatannya.

Terdapat hal-hal spesifik dalam konteks pertahanan siber, dan itu menjadi tantangan tuntutan standar kompetensi SDM pertahanan siber, yaitu penyelenggaraan pertahanan siber yang dilaksanakan dengan merujuk pada suatu strategi penangkalan, penindakan dan pemulihan bidang pertahanan siber, yang tentunya didukung oleh kesiapan infrastruktur sistem berikut sarana dan prasarana pertahanan siber yang memadai. Dalam banyak hal, terdapat persamaan maupun perbedaan antara konsep pertahanan siber dengan keamanan siber, salah satunya adalah aspek strategi, tentu akan sangat berbeda konsep srategi dalam pertahanan siber dengan keamanan siber. Perbedaan konsep strategi merupakan tantangan spesifikasi yang tidak mungkin teratasi hanya dengan mengandalkan kompetensi SDM TIK maupun SDM keamanan siber, terutama terhadap fakta ketika penyelenggaraan pertahanan siber diproyeksikan tujuan melindungi dan mempertahankan kedaulatan negara dalam *theatre* perang siber (*cyber war*) dan/atau peperangan siber (*cyber warfare*), di mana prinsip-prinsip yang berlaku bagi para pihak yang bertikai adalah prinsip-prinsip hukum internasional yang berlaku untuk konflik bersenjata (*the international law of armed conflict*), sementara ironisnya belum ada satupun hukum internasional yang mengatur dinamika TTP untuk konflik yang terjadi di ruang siber.

Pemerintah telah menerbitkan UU No.23/2019 tentang PSDN untuk hanneg, sejatinya bertujuan untuk bagaimana mentransformasikan segenap warga negara Indonesia sebagai SDM nasional yang memiliki potensi kompetensi dalam bidang TIK dan keamanan siber untuk menjadi komponen kekuatan pertahanan negara yang siap digunakan untuk kepentingan hanneg. Harapannya adalah melalui mekanisme PSDN untuk hanneg, tantangan dalam membangun dan mempersiapkan kompetensi SDM pertahanan siber dapat teratasi.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan pertimbangan bahwa keseluruhan data merupakan situasi sosial (*social situation*) non angka (*non-numeric data*), yaitu berupa tulisan dan gambar. Penyaringan terhadap data dilakukan untuk membuat interpretasi dari tinjauan pustaka (*literature review*)[26]. Kajian dilakukan merujuk pada sumber literatur seperti jurnal, dokumen, maupun artikel dari berbagai sumber yang *reliable*. Terkait penyaringan data atau kondensasi data, menggunakan teknik analisis data kualitatif model interaktif (*interactive model*)[27], dan langkah-langkah analisis dikolaborasikan menggunakan teori manajemen George R. Terry terkait fungsi dasar manajemen (POAC)[28]. Analisis dimulai dari memetakan eksistensi setiap kompetensi SDM (TIK, keamanan siber, dan pertahanan siber), di mana setiap kompetensi tentu relevan dengan peran, tugas, dan fungsi instansi penyelenggara tata kelola kompetensi SDM terkait. Selanjutnya hasil pemetaan ketiga kompetensi SDM tersebut, dilakukan komparasi dan identifikasi, lalu analisis dilakukan untuk memperoleh gambaran umum tentang wujud kompetensi SDM pertahanan siber sekaligus bagaimana potensi yang ada untuk mewujudkannya. Selain itu disampaikan juga rekomendasi untuk dapat diaktualisasikan.

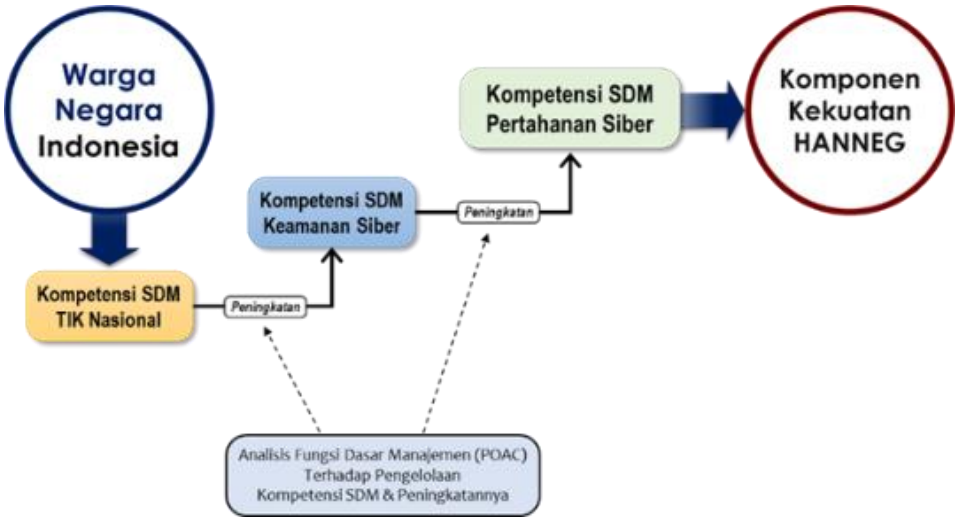
Teori Manajemen

Menurut George R. Terry[29], manajemen adalah pencapaian tujuan-tujuan yang telah ditetapkan melalui dan/atau bersama-sama usaha orang lain. Terry membagi empat fungsi manajemen, meliputi: *Planning* (Perencanaan), *Organizing* (Pengorganisasian), *Actuating* (Pelaksanaan) dan *Controlling* (Pengawasan), disingkat menjadi POAC. Manajemen penting bagi setiap aktivitas guna mencapai tujuan. Manajemen berorientasi pada proses sehingga membutuhkan SDM, *knowledge* dan *skill*, agar aktivitas efektif dalam mencapai sukses. Organisasi tidak akan sukses bila mengabaikan fungsi manajemen. Berdasarkan pandangan tersebut, peneliti

[26] John W. Creswell, *Penelitian Kualitatif & Desain Riset*, (Yogyakarta: Pustaka Pelajar, 2015), hlm.5.
[27] Matthew B. Miles dan A. Michael Huberman, *Analisis Data Kualitatif: Buku Sumber Tentang Metode-Metode Baru*, (Jakarta: UI-Press, 2014), hlm.15.
[28] George Robert Terry, *Prinsip-Prinsip Manajemen*, (Jakarta: Bumi Aksara, 2006), hlm.342.
[29] Sukarna, *Dasar-Dasar Manajemen*, (Bandung: CV. Mandar Maju, 2011), hlm.3.

berpendapat bahwa manajemen adalah ilmu yang mengatur proses mencapai tujuan yang telah ditetapkan untuk mencapai tujuan sesuai rencana. Dalam penelitian ini, fungsi dasar manajemen (POAC), digunakan peneliti untuk menganalisis adanya upaya-upaya (sebagai proses manajemen yang setidaknya dianggap memenuhi prinsip-prinsip POAC) peningkatan kompetensi SDM TIK dan keamanan siber hingga kompetensi SDM pertahanan siber. Analisis POAC tersebut sekaligus untuk membuktikan pandangan dan asumsi bahwa kompetensi SDM dapat ditingkatkan dan dioptimalkan melalui berbagai kegiatan diklat sesuai bidang kepentingan organisasi. Analisis POAC dilakukan secara sederhana terhadap data awal aspek-aspek kompetensi SDM TIK nasional, keamanan siber, dan pertahanan siber, guna menjawab fokus rumusan masalah, yaitu: bagaimana wujud kompetensi SDM pertahanan siber, dan bagaimana potensi dalam mewujudkannya.

Kerangka Berpikir



Gambar 3. Kerangka Berpikir Penelitian
Sumber: diolah peneliti, 2020

Warga negara Indonesia (WNI) merupakan SDM yang dalam konsep pertahanan negara merupakan salah satu komponen kekuatan pertahanan negara. Dalam hal kompetensi SDM pertahanan siber, terdapat kompetensi SDM TIK dan kompetensi SDM keamanan siber yang pengelolaannya diselenggarakan oleh Kominfo untuk SDM TIK

nasional, dan BSSN untuk SDM keamanan siber. Tata kelola SDM TIK merupakan *basic* (awal) kebutuhan kompetensi TIK nasional oleh Kominfo, yang kemudian ditata kelola kembali oleh BSSN untuk ditingkatkan kompetensinya menjadi SDM keamanan siber. Selanjutnya kompetensi SDM keamanan siber ditata kelola oleh bidang pertahanan (Kemhan/TNI) untuk ditingkatkan kompetensinya melalui mekanisme pengelolaan sumber daya nasional untuk hanneg (UU No.23/2019), dalam hal ini ditransformasi menjadi komponen pertahanan negara dengan kemampuan pertahanan siber guna menghadapi ancaman siber. Analisis dilakukan pada setiap bidang tata kelola peningkatan kompetensi SDM, yang setidaknya memenuhi prinsip-prinsip fungsi dasar manajemen (POAC).

Hasil dan Pembahasan

Prinsip POAC Pada Kompetesi SDM Bidang TIK

Pembangunan kompetensi SDM TIK nasional merupakan peran tugas dan tanggung jawab pemerintah melalui Kemenkominfo RI, yang merujuk pada *Roadmap* Pembangunan TIK Nasional di mana fokus pembangunan infrastruktur TIK nasional menitikberatkan pada pembangunan SDM TIK yang memiliki nilai tambah bagi pertumbuhan ekonomi dan meneguhkan kedaulatan bangsa. Terdapat 3 (tiga) sasaran strategis pembangunan SDM TIK, yaitu penguasaan pasar TIK global, kapasitas produksi nasional, dan masyarakat berbudaya TIK yang tangguh. Sangat jelas bahwa kompetensi SDM bidang TIK lebih menitikberatkan kepada sektor ekonomi dan cenderung diproyeksikan untuk siap bersaing di dunia industri.

Tabel 1. Kompetensi SDM TIK Nasional

No	Area Fungsi TIK	Keterangan / Aspek Manajemen (POAC)
1.	*data managemen systems*	• Merujuk pada Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi TIK • Melalui berbagai bentuk program kegiatan pendidikan dan pelatihan spesifik TIK
2.	*programming and software develompment*	
3.	*hardware and digital peripherals*	
4.	*network and infrastructure*	
5.	*operation and systems tools*	

No	Area Fungsi TIK	Keterangan / Aspek Manajemen (POAC)
6.	*information systems and technology development*	• Pembangunan Kompetensi menitikberatkan kepada sektor ekonomi dan cenderung untuk bersaing di dunia Industri • Untuk memenuhi kebutuhan pembangunan, pengembangan, dan pengawakan infrastruktur TIK di berbagai sektor strategis nasional (aspek ketenagakerjaan) • Aspek keamanan bersifat keamanan informasi (*information security*) terbatas pada kepentingan sektoral organisasi • Strategi → untuk kepentingan/sesuai *roadmap* pembangunan TIK nasional
7.	*IT governance and management*	
8.	*IT project management*	
9.	*IT enterprise architecture*	
10.	*IT security compliance*	
11.	*IT service management systems*	
12.	*IT and computing facilities management*	
13.	*IT multimedia*	
14.	*IT mobility and internet of things (IoT)*	
15.	*integration application system*	
16.	*IT consultancy and advisory*	

Sumber: diolah peneliti, 2020

Kominfo telah menyusun rencana pengembangan SDM TIK melalui sertifikasi Standar Kompetensi Kerja Nasional Indonesia (SKKNI) bidang Kominfo (Puslitbang SDPPI Balitbang SDM Kominfo), di mana secara umum kompetensi SDM TIK adalah meliputi bidang-bidang: Telekomunikasi Satelit, Instalasi Fiber Optik, Perencanaan dan Perekayasaan Jaringan Seluler, *Operation and Maintenance* Jaringan Seluler, Optimasi Jaringan Seluler, Jaringan Komputer, Pengembangan Perangkat Lunak (*Software Development*) Sub Bidang Pemrograman, *Computer Technical Support*, Manajemen Layanan TI, Pengoperasian Komputer, Desain Grafis atau Desain Komunikasi Visual, Kehumasan (*Public Relations*). Pada dasarnya kompetensi SDM TIK tersebut masih standar dan *basic*.

Prinsip POAC Pada Kompetesi SDM Bidang Keamanan Siber

Membangun kompetensi SDM keamanan siber nasional, merupakan peran tugas dan tanggung jawab pemerintah melalui BSSN. Dalam hal tersebut BSSN merujuk pada *Roadmap* Pembinaan SDM Keamanan Siber dan Sandi 2020-2024, menuju keamanan siber yang terpercaya, profesional dan berdaya saing. Hal spesifik dari kompetensi SDM keamanan siber adalah tuntutan *knowledge* dan *skill* serta kapasitas dan kapabilitas operasional keamanan siber sebagai dampak dari pesatnya pemanfatan TIK pada setiap aspek kehidupan, yang disertai dengan meningkatnya ancaman siber sehingga menjadi

tantangan yang harus dihadapi sesuai tugas BSSN yaitu melaksanakan keamanan siber secara efektif dan efisien memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur terkait keamanan siber. Secara umum. Bila merujuk pada dokumen peta okupasi nasional dalam kerangka kualifikasi nasional Indonesia pada fungsi keamanan siber, maka kompetensi SDM keamanan siber adalah meliputi, antara lain: *cybersecurity*, *chief of information security*, *cyber risk specialist*, *cybersecurity manager*, *network security manager*, *incident response team manager*, *threat hunter*, *cybersecurity governance oficer*, *cybersecurity operator*, *forensic computer*, digital *forensic analyst*, *digital evidence first responder*, *IT security*, *penetration tester*, *security architect*,

Tabel 2. Kompetensi SDM Keamanan Siber

Level Kualifikasi	Area Fungsi Keamanan Siber	Keterangan / Aspek Manajemen (POAC)
1	–	• Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber. Dokumen ini juga menjadi bagian yang tidak terpisah dari Peta Okupasi Nasional TIK yang disusun dalam KKNI. • Melalui berbagai bentuk program kegiatan pendidikan dan pelatihan spesifik keamanan siber. • Pembangunan Kompetensi menitikberatkan kepada terwujudnya keamanan siber nasonal • Aspek keamanan siber (*cybersecurity*) bersifat terkoordinasi dan integratif antar pemangku kepentingan siber nasional demi kepentingan nasional • Terdapat dinamika penyelenggaraan kegiatan operasional keamanan siber yang komprehensif meliputi *technique*, *tactic*, dan *procedure* (TTP) dalam menghadapi ancaman serangan siber • Operasional keamanan siber bersifat masif (skala nasional) melibatkan segenap pemangku kepentingan siber secara integratif • Terkait eskalasi ancaman siber, dinamika operasi keamanan siber dilaksanakan pada masa normal (damai), dan dengan tetap
2	–	
3	–	
4	–	
5	**Fase *before & during attack*** *cryptographic technician, cryptographic administrator, junior cyber security, dan cyber security operator*	
6	**Fase *before, during & after attack*** *ICT security product evaluator, cryptographic analyst, cryptographic module analyst, vulnerability assessment analyst, network security administrator, cyber security administrator, cyber security awareness officer, cyber security analyst/cyber security incident analyst, dan digital evidence first responder*	
7	**Seluruh Fase** *cryptographic speialist, cryptographic engineer, ICT security product lead evaluator, cybersecurity manager, network security manager, cybersecurity awareness lead officer, incident response team manager, information security auditor, threat hunter, penetration tester, cybersecurity governance officer, dan digital forensic analyst*	

Level Kualifikasi	Area Fungsi Keamanan Siber	Keterangan / Aspek Manajemen (POAC)
8	**Fase *before & after attack*** *cyber risk specialist, security architect, cryptographic specialist, cyber incident investigation manager, dan cyber forensic specialist*	berpedoman pada ketentuan dan aturan hukum yang berlaku dalam kerangka keamanan nasional • Strategi adalah strategi keamanan siber dalam kerangka keamanan nasional
9	**Seluruh Fase** *Chief of information security officer*	

Sumber: diolah peneliti, 2020

Prinsip POAC Pada Kompetesi SDM Bidang Pertahanan Siber

Upaya membangun kompetensi SDM pertahanan siber, menjadi peran tugas dan tanggung jawab pemerintah melalui Kemhan. Dalam hal tersebut Kemhan belum ada rumusan *roadmap* pembangunan kompetensi SDM pertahanan siber, namun demikian merujuk pada dokumen Pedoman Pertahanan Siber. Hal yang spesifik dari kompetensi SDM pertahanan siber, yaitu diproyeksikan di berbagai tugas-tugas pertahanan negara guna menghadapi ancaman siber sesuai dengan fungsi penangkalan, penindakan, dan penanggulangan. Oleh karena itu maka *knowledge* dan *skill* serta kapasitas dan kapabilitas SDM pertahanan siber mutlak memiliki kemampuan untuk melaksanakan fungsi-fungsi tersebut dalam bentuk praktik-praktik kegiatan operasi militer untuk perang (OMP) maupun operasi militer selain perang (OMSP), termasuk operasional dalam bentuk perang siber.

Tabel 3. Kompetensi SDM Pertahanan Siber

No	Uraian Kompetensi	Keterangan / Aspek Manajemen (POAC)
1.	Memiliki *cybersecurity awarness*	• Kompetensi SDM tidak merujuk pada Peta Okupasi Nasional melainkan pada dokumen pedoman pertahanan siber • Melalui berbagai bentuk program kegiatan pendidikan dan pelatihan spesifik pertahanan siber. • Pembangunan Kompetensi menitikberatkan kepada terwujudnya SDM sebagai bagian dari komponen kekuatan pertahanan negara
2.	**Memiliki pengetahuan dan keterampilan** *information security and risk management, access control systems and methodology, cryptography, physical security, telecommunications and network security, security architecture and models, business continuity planning and disaster recovery plan, applications security, operations security, legal, regulations, compliance and investigations, dan implementasi SNI 27001*	

No	Uraian Kompetensi	Keterangan / Aspek Manajemen (POAC)
3.	**Memiliki pengetahuan dan keterampilan penanganan insiden, sekurang-kurangnya meliputi** *digital forensic, incident response, operation system, dan data communication networking*	• Aspek keamanan siber (*cybersecurity*) dalam hal ini adalah pertahanan siber yang bersifat terkoordinasi dan integratif antar pemangku kepentingan siber nasional sebagai bagian dari sumberdaya nasional untuk pertahanan negara • Penyelenggaraan pertahanan siber merujuk pada suatu strategi penangkalan, penindakan dan pemulihan bidang pertahanan siber, yang tentunya didukung oleh kesiapan infrastruktur sistem berikut sarana dan prasarana pertahanan siber yang memadai. • terkait eskalasi ancaman siber, dinamika operasi pertahanan siber dilaksanakan pada masa konflik (perang), ironisnya belum ada aturan internasional yang mengatur konflik berdimensi *cyberspace* • strategi adalah strategi pertahanan siber dalam kerangka pertahanan negara
4.	**Memiliki pengetahuan dan keteramnpilan melakukan penetatrion test sekurang-kurangnya meliputi** *information security in general, using penetration testing tools, IT examination and reporting, dan web based application developing*	
5.	*System assurance*	
6.	**Pengetahuan & keterampilan sistem meliputi** *network security, operating systems security, systems infrastructure and database, security, digital control system, dan system development*	
7.	Pengetahuan dan kemampuan merehabilitasi dan rekonstruksi kerusakan yang terjadi pada jaringan TIK dan muatannya	

Sumber: diolah peneliti, 2020

Di dalam dokumen Pedoman Pertahanan Siber, belum secara spesifik menguraikan kualifikasi kompetensi SDM pertahanan siber yang menjadi harapan bidang pertahanan. Bahkan bila mencermati ilustrasi pada gambar 4 (kajian kebutuhan kompetensi SDM pertahanan siber yang berkorelasi dengan jenjang karir), hal itu semakin memperjelas bahwa kompetensi SDM pertahanan sama sekali tidak (belum) merujuk pada Peta Okupasi Nasional untuk kualifikasi kriteria kompetensi SDM TIK nasional maupun SDM keamanan siber. Di sisi lain, dalam perspektif bidang pertahanan, baik kompetensi SDM TIK maupun SDM keamanan siber, keduanya merupakan awal (*basic*) dan baru mampu memenuhi sebagian besar kualifikasi kriteria kompetensi SDM pertahanan siber. Untuk dapat memenuhi kualifikasi kriteria kompetensi SDM pertahanan siber, maka terhadap SDM dengan kompetensi TIK + keamanan siber, padanya dilakukan upaya transformasi (pengelolaan) melalui mekanisme PSDN untuk hanneg, sehingga menjadi SDM pertahanan siber

Gambar 4. Kajian Kebutuhan Kompetensi SDM Pertahanan Siber Berkorelasi Dengan Jenjang Karir
Sumber: Pedoman Pertahanan Siber, 2014

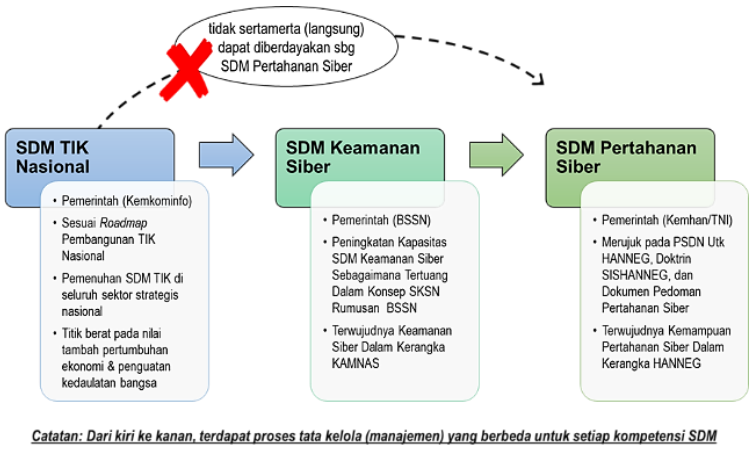
Prinsip POAC Pada Potensi Mewujudkan Kompetesi SDM Pertahanan Siber

Dalam membangun kompetensi SDM pertahanan siber, di dalamnya terdapat potensi, yaitu: bahwa kompetensi SDM TIK dan kompetensi SDM keamanan siber telah memenuhi hampir sebagian besar kriteria kualifikasi SDM pertahanan siber. Selain itu pada kompetensi SDM keamanan siber terdapat *knowledge* dan *skill* serta kapasitas dan kapabilitas SDM yang secara spesifik telah memenuhi sebagian besar kualifikasi kriteria kompetensi SDM pertahanan siber, misalnya untuk aspek *knowledge*, antara lain secara umum menguasai konsep dan teoritis tentang jaringan komputer dan komunikasi, keamanan informasi, dan intelijen; sedangkan untuk aspek *skill* antara lain memiliki kemampuan dalam rekayasa keamanan jaringan komputer dan komunikasi dengan menggunakan metodologi tertentu, rekayasa keamanan informasi, merencanakan dan merancang pengelolaan keamanan siber, serta mengoperasikan fitur-fitur keamanan perangkat jaringan yang meliputi sistem operasi, perangkat lunak dan perangkat keras.

Baik Kompetensi SDM TIK maupun kompetensi SDM keamanan siber, peningkatan kompetensinya ditempuh melalui berbagai bentuk program kegiatan pendidikan dan pelatihan (diklat) yang spesifik. Oleh karena itu program diklat merupakan potensi dan penting untuk diselenggarakan secara terencana dan berkesinambungan, mulai dari awal (*basic*), yaitu: kompetensi SDM bidang TIK (melalui program diklat bidang TIK),

kemudian ditingkatkan menjadi SDM keamanan siber (melalui program diklat bidang keamanan siber), lalu kemudian melalui proses dan tata kelola yang lebih spesifik ditingkatkan kembali sehingga terpenuhi kriteria kompetensi sebagai SDM pertahanan siber (melalui semacam program diklat spesifik/khusus bidang pertahanan siber).

Pada gambar 5 menunjukan bahwa SDM TIK nasional didudukan sebagai kompetensi *basic* dalam mengawali proses pembangunan (pengelolaan) kompetensi SDM keamanan siber maupun pertahanan siber. *Requirement* SDM kompetensi keamanan siber dan pertahanan siber sangat mensyaratkan adanya *knowledge* dan *skill* serta kapasitas dan kapabilitas *basic* bidang TIK. Kompetensi SDM keamanan siber maupun pertahanan siber, juga mensyaratkan kualifikasi SDM yang memiliki kriteria *knowledge* dan *skil* serta kapasitas dan kapabilitas bidang keamanan siber maupun bidang pertahanan siber yang mampu (dapat) diproyeksikan dalam menyelenggarakan dan melaksanakan berbagai dinamika tugas, peran, dan fungsi khusus, yaitu untuk menghadapi dan menanggulangi berbagai bentuk ancaman siber terhadap kepentingan nasional Indonesia dan/atau bersifat kontijensi nasional. Dan kekhususan yang ada pada kompetensi SDM keamanan siber tersebut sekaligus menjadi potensi yang diperlukan memenuhi kualifikasi dan kriteria kompetensi SDM pertahanan siber yang *intake*-nya (*input* SDMnya) sangat bergantung atau bersumber kepada kompetensi SDM keamanan siber.



Gambar 5. Model Proses Tata Kelola SDM TIK Ke SDM Pertahaan Siber
Sumber: diolah peneliti, 2020

Deskripsi Area Fungsi Kompetensi SDM Pertahanan Siber Dengan Tolok Ukur Pada Kompetensi SDM TIK dan SDM Keamanan Siber.

Kompetensi SDM pertahanan siber sebagaimana tercantum dalam dokumen Pedoman Pertahanan Siber (Permenhan RI No.82/2014), belum mengacu kepada Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada TIK maupun Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber, malah sebaliknya tidak lebih hanya dipahami sebagai konsep kompetensi SDM yang sekedar "memiliki kemampuan". Peneliti berpandangan bahwa kompetensi SDM pertahanan siber seyogyanya dibangun secara lebih spesifik dan fokus pada *knowledge* dan *skill* serta kapasitas dan kapabilitas SDM yang sedemikian rupa mampu mengaktualisasikan fungsi-fungsi pertahanan negara (dalam hal ini fungsi penangkalan, dan fungsi penindakan, serta fungsi perbantuan).

Berikut ini matrik area fungsi kompetensi pertahanan siber yang dimungkinkan sebagai referensi untuk bidang pertahanan dalam merumuskan kembali konsep kompetensi SDM pertahanan siber yang lebih mampu dalam penyelenggaraan fungsi-fungsi pertahanan negara.

Tabel 4. Matrik Deskripsi Area Fungsi Kompetensi SDM Pertahanan Siber Bertolok Ukur Pada Kompetensi SDM TIK Dan SDM Keamanan Siber

<table>
<tr><td></td><td colspan="4">Kompetensi SDM</td></tr>
<tr><td></td><td colspan="2">SDM TIK</td><td colspan="2">SDM Keamanan Siber</td><td colspan="2">SDM Pertahanan Siber</td></tr>
<tr><td rowspan="9">Level KKNI</td><td>①</td><td rowspan="9">Meliputi 16 (Enambelas) Area Fungsi Teknologi Informasi & Komunikasi</td><td colspan="2" rowspan="4"></td><td>①</td><td rowspan="9">Area Fugsi Pertahanan Siber</td></tr>
<tr><td>②</td><td>②</td></tr>
<tr><td>③</td><td>③</td></tr>
<tr><td>④</td><td>④</td></tr>
<tr><td>⑤</td><td>⑤</td><td rowspan="5">Area Fungsi Keamanan Siber</td><td>⑤</td></tr>
<tr><td>⑥</td><td>⑥</td></tr>
<tr><td>⑦</td><td>⑦</td></tr>
<tr><td>⑧</td><td>⑧</td></tr>
<tr><td>⑨</td><td>⑨</td></tr>
</table>

		Kompetensi SDM		
		SDM TIK	**SDM Keamanan Siber**	**SDM Pertahanan Siber**
***Knowledge & Skill* Serta Kapasitas & Kapabilitas Yang Mampu Menyelenggarakan Fungsi Khusus**	**Operasional Keamanan**		• Kemampuan SDM untuk menyelenggarakan fungsi keamanan informasi yang memenuhi fase-fase penanganan insiden keamanan siber yang terdiri dari 3 (tiga) fase, yaitu: a) fase sebelum insiden serangan siber (*before cyber attack*); b) fase ketika terjadinya insiden serangan siber (*during cyber attack*); dan c) fase setelah terjadinya insiden serangan siber (*after cyber attack*) • Kemampuan SDM untuk melaksanakan fungsi keamanan siber yang diselenggarakan dalam bentuk/wujud kegiatan terorganisir (strategi, taktis, operasional, dan bersifat kontjensi) secara terintegrasi melibatkan seluruh pemangku kepentingan siber nasional.	Kemampuan SDM untuk mampu melaksanakan fungsi-fungsi keamanan informasi maupun fungsi keamanan siber sebagaimana berlaku pada kompetensi SDM keamanan siber
	Operasional Pertahanan			Kemampuan SDM untuk mampu melaksanakan fungsi-fungsi pertahanan negara yang terdiri dari 3 (tiga) fungsi, yaitu: fungsi penangkalan, fungsi penindakan, dan fungsi penanggulangan, serta sebagai tambahan adalah fungsi perbantuan.
Keterangan		• *Leading Sector* adalah Kemenkominfo RI • Merujuk pada Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada TIK	• *Leading Sector* adalah BSSN, merujuk pada SKSN • Kemampuan SDM sesuai fungsi ke-10 Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonsia Pada TIK (Fungsi ke 10 area fungsi TIK), yang kemudian dijabarkan kembali melalui Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber	• *Leading Sector* adalah Kemhan/TNI • Kompetensi SDM merujuk pada Permenhan No.82/2014 (Pedoman Pertahanan Siber) sebagai pedoman yang perlu penyesuaian terhadap Peta Okupasi TIK maupun Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber • Peningkatan dan penguatan kompetensi SDM fungsi keamaan siber menjadi pertahanan siber perlu selaras dengan SKSN • dalam hal pemberdayaan, harus ditrasnformasikan menjadi SDM pertahanan siber melalui mekanisme PSDN untuk Hanneg.

Sumber: diolah peneliti, 2020

Kesimpulan Rekomendasi dan Pembatasan

Berdasarkan uraian hasil dan pembahasan tersebut di atas, maka diperoleh kesimpulan sebagai berikut:

Wujud Kompetensi SDM Pertahanan Siber

Pada dasarnya wujud kompetensi SDM bidang pertahanan siber, adalah meliputi seluruh kualifikasi dan kriteria kompetensi SDM TIK nasional ditambah kualifikasi dan kriteria kompetensi SDM keamanan siber, yang kemudian ditingkatkan *knowledge* dan *skill* serta kapasitas dan kapabilitasnya melalui mekanisme PSDN untuk hanneg sehingga menjadi SDM dengan kompetensi pertahanan siber sebagai bagian dari komponen kekuatan pertahanan negara untuk mampu menghadapi berbagai bentuk ancaman siber.

Potensi Mewujudkan Kompetensi SDM Pertahanan Siber

Potensi-potensi yang mendukung upaya mewujudkan kompetensi SDM pertahanan siber, antara lain: a) bahwa kompetensi SDM TIK (oleh Kominfo) dan SDM keamanan siber (oleh BSSN) merupakan esensi kompetensi yang *basic* dan awal yang dinilai mampu memenuhi sebagian besar kualifikasi kriteria kompetensi SDM pertahanan siber, sehingga bidang pertahanan hanya perlu mempersiapkan dan mengelola semacam diklat khusus bidang pertahanan siber sehingga terwujud kompetensi SDM pertahanan siber yang mampu menghadapi berbagai ancaman siber; dan b) Bahwa UU No.23/2019 tentang PSDN untuk Hanneg sangat potensial sebagai payung legitimasi bagi perlunya program pendidikan dan pelatihan (diklat) spesifik bidang pertahanan siber, karena program kegiatan diklat memiliki peran sekaligus selaras dengan upaya transformasi/pengelolaan sumber daya nasional untuk kepentingan pertahanan negara.

Sebagai rekomendasi, Kemhan RI perlu merevisi dokumen Pedoman Pertahanan Siber untuk disempurnakan sehingga menjadi semacam *roadmap* pembangunan kemampuan pertahanan siber yang di dalamnya tercantum upaya mewujudkan

kompetensi SDM pertahanan siber. Upaya mewujudkan kompetensi SDM pertahanan dalam *roadmap* tersebut perlu selaras sekaligus komprehensif dengan: *roadmap* pengembangan kompetensi SDM TIK nasional, *roadmap* pembinaan SDM keamanan siber dan sandi 2020-2024 (BSSN), peta okupasi nasional dalam KKNI pada TIK, peta okupasi nasional dalam KKNI pada area fungsi keamanan siber, dan tentunya UU No.23/2019 tentang PSDN untuk pertahanan negara.

Daftar Pustaka

Peraturan

Undang-Undang Republik Indonesia Nomor 23 tahun 2019 tentang Pengelolaan Sumber Daya Nasional Untuk Pertahanan Negara.

Peraturan Menteri Tenaga Kerja dan Transmigrasi RI No.5 Tahun 2012 tentang Sistem Standardisasi Kompetensi Kerja Nasional.

Peraturan Menteri Pertahanan RI No.82 Tahun 2014 tentang Pedoman Pertahanan Siber.

Keputusan Menteri Ketenagakerjaan RI No.160 Tahun 2016 tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Aktivitas Profesional, Ilmiah dan Teknis Golongan Pokok Aktivitas Kantor Pusat dan Konsultasi Manajemen Bidang produktivias.

Pengesahan Kepala Badan Litbang SDM Kominfo RI, Direktur Jenderal Pembinaan Pelatihan dan Produktivitas Kemnaker, Wakil Ketua Umum Kamar Dagang dan Industri Indonesia (Kadin) Bidang Ketenagakerjaan dan Industrial, Deputi Menteri PPN/Kepala Bappenas Bidang Kependudukan, dan ketua Badan Nasional Sertifikasi Profesi, Nomor 172/KOMINFO/ BLSDM/KS.01.07/7/2017, tanggal 27 Juli 2017 tentang Peta Okupasi Nasional Bidang TIK tahun 2017.

Jurnal

Ardiyanti, Handrini. "Cybersecurity dan Tantangan Pengembangannya di Indonesia", Politica, Vol.5, No.1, 2014, hlm.95-110.

Huda, Irkham Abdaul. "Perkembangan Teknologi Informasi dan Komunikasi (TIK) Terhadap Kualitas Pembelajaran di Sekolah Dasar", Jurnal Pendidikan dan Konseling, Vol.1, No.2, 2020, hlm.143-149.

Nurkholis. "Pendidikan Dalam Upaya Memajukan Teknologi", Jurnal Kependidikan, Vol.1, No.1, 2013, hlm.24-44.

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

Putra, Andhika Doly, Herlina J.R. Saragih, dan G.Royke Deksino. "Implementasi Manajemen Risiko Pertahanan Siber Kementerian Pertahanan Untuk Mendukung Pertahanan Negara", Jurnal Pertahanan, Vol.6, No.1, 2020, hlm.100-121.

Prasetyo, Budi Triyoga, dan Sugeng Berantas. "Peningkatan Kualitas SDM di Bidang Industri Pertahanan Menuju Pertahanan Negara Yang Tangguh", Jurnal Pertahanan, Vol.5, No.1, 2015, hlm.175-195.

Santoso, Sugeng. "Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional", Jurnal Kajian Lemhanas RI, Edisi 34, 2018, hlm.43-48.

Sebastian, Elly. "Peningkatan Peranan SDM Pertahanan Nasional Guna Menghadapi Perang Generasi Keempat", Jurnal Pertahanan, Vol.5, No.1, 2015, hlm.109-128.

Buku

Badan Litbang SDM Kominfo. Penyusunan Roadmap Pembangunan Sektor TIK yang Mengikat Secara Jangka Panjang s.d 2045 Menuju 100 Tahun Indonesia merdeka, (Jakarta: Badan Litbang SDM Kominfo, 2016).

Badan Siber dan Sandi Negara (BSSN). *Roadmap* Pembinaan SDM Keamanan Siber dan Sandi 2020 – 2024 (Menuju SDM Keamanan Siber & Sandi Yang Terpercaya, Profesional, dan Berdaya Saing), (Jakarta: Direktorat Pengendalian SDM, Deputi IV, Badan Siber dan Sandi Negara, 2019).

Badan Siber dan Sandi Negara (BSSN). Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber, (Jakarta: Badan Siber dan Sandi Negara, 2019).

Creswell, John W. Penelitian Kualitatif & Desain Riset, (Yogyakarta: Pustaka Pelajar, 2015), hlm.5.

Hasibuan, Malayu. Manajemen Sumber Daya Manusia, (Jakarta: Bumi Aksara, 2009), hlm.54.

Indrajit, Richardus Eko. Pengantar Konsep Dasar Manajemen Sistem Informasi dan Teknologi Informasi, (Jakarta: Elex Media Komputindo, 2000).

Tim Penyusun Kamus Pusat Bahasa. Kamus Bahasa Indonesia, (Jakarta: Departemen Pendidikan Nasional, 2008), hlm.743.

Miles, Matthew B., dan A. Michael Huberman. Analisis Data Kualitatif: Buku Sumber Tentang Metode-Metode Baru, (Jakarta: UI-Press, 2014), hlm.15.

Puslitbang SDPPI Balitbang SDM Kominfo. Rencana Pengembangan SDM TIK di Indonesia Melalui Sertifikasi SKKNI Bidang Kominfo, (Jakarta: Puslitbang SDPPI Balitbang SDM Kominfo, 2018).

Robbins SP, dan Judge. Perilaku Organisasi, (Jakarta: Salemba Empat, 2007), hlm.38.

Spencer, N.Lyle and Spencer, M. Signe. Competence at Work: Models for Superior Performance, (New York: John Wiley & Son Inc., 1993), hlm.9-10.

Suparno, A. Suhaenah. Membangun Kompetensi Dasar, (Jakarta: Direktorat Jendral Pendidikan Tinggi Departemen Pendidikan Nasional, 2001), hlm.27.

Terry, George Robert. Prinsip-Prinsip Manajemen, (Jakarta: Bumi Aksara, 2006), hlm.342.

Website

Flowers, Angelyn., Sherali Zeadally. "*Cyberwar: The What, When, Why, and How*", dalam https://technologyandsociety.org/cyberwar-the-what-when-why-and-how/, 29 Juni 2017, diakses pada 20 Oktober 2020.

Opdebeeck, Jean Sebastien. "*People, Processes dan Technology are the pillars of CyberSecurity*", dalam https://www.vulpoint.com/people-processes-technology-cybersecurity/#page-content, 1 Desember 2018, diakses pada 20 Juni 2020.