43794.pdf

TUGAS AKHIR PROGRAM MAGISTER

REGULASI PENANGANAN KEJAHATAN SIBER DI LINGKUNGAN TNI ANGKATAN DARAT

Disusun Oleh :

Kaisar Bagus Purnawijaya Rhynaldie

NIM : 500804786

PROGRAM PASCASARJANA

UNIVERSITAS TERBUKA

2019

Koleksi Perpustakaan Universitas Terbuka

ABSTRACT

In the current era of cyberspace, the role of The Army is not only to deal with conventional warfare but also cyber crime that threatens national defense. The Army has a Cyber Unit tasked with monitoring and reporting content or hoax news related to the institution of The Indonesia Army. Increasingly complex types of cyber crime, it is necessary to increase the function of The Army Cyber Unit to have offensive capabilities, namely to strengthen network security and carry out cyber attacks on the enemy. This research describes The Army Cyber Unit which will be increased its function in facing the threat of cyber crime from the beginning has only defensive ability to be offensive. The approach used is a qualitative approach through purposive sampling technique. Data collection was conducted by means of interviews, literature and documentation study, whereas for the research informants, there were 55 military personnel from The The Army Cyber Unit and 4 personnel The Army Security Staff as the supervision for The Army Cyber Unit. The data analysis technique used is the technique of data triangulation by comparing the interview result obtained from each source. The results of this research are the threat of cyber crime affect the increase in the function The Army Cyber Unit to prevent sabotage, theft of military confidential data using encription systems, cyber psychological attacks and attacks on the infrastructure and information systems of The Indonesian Army. In an effort to increase there are several inhibiting factors, namely : the limited ability of human resources, facilities and infrastructure, the weakness of the law governing the mechanism of the work The Army Cyber Unit and limited cross-sectoral coordination between National Cyber units. The role of The The Army Cyber Unit in exposing cyber crime is still limited in cyber defense, media monitoring and reporting content or news hoax. The recommendations in accordance with the industrial revolution 4.0 is becoming a priority of the government, creating a security management and contingency cyber, forming a collaboration of cyber security in the sphere of international, regional and bilateral, to improve law enforcement in the field of IT/Cyber, prioritizing innovation, creativity and improving human resource capabilities in the cyber field as well as performing the approach between The Stakeholders in the field of national cyber.

Keywords **:** Cyber crime, The Army Cyber Unit, Hoaxes, Hacking.

Koleksi Perpustakaan Universitas Terbuka

ABSTRAK

Di era dunia maya saat ini, peranan TNI AD tidak hanya menghadapi peperangan secara konvensional tetapi juga kejahatan siber yang mengancam pertahanan nasional. Organisasi TNI AD telah membuat Satuan Tugas Siber (Satsiber TNI) yang bertugas memonitor dan melaporkan konten/berita *hoax* terkait institusi TNI AD. Dengan semakin kompleksnya jenis kejahatan siber, maka diperlukan peningkatan fungsi Satuan siber TNI AD yang memiliki kemampuan ofensif yaitu untuk memperkuat keamanan jaringan dan melakukan serangan siber kepada musuh. Penelitian ini mendeskripsikan Satuan Siber TNI AD yang akan ditingkatkan fungsinya dalam menghadapi ancaman kejahatan siber dari semula hanya memiliki kemampuan defensif menjadi berkemampuan *ofensif*. Pendekatan yang digunakan adalah *pendekatan kualitatif melalui teknik purposive sampling*. Pengumpulan data dilakukan dengan cara wawancara, studi literatur dan studi dokumentasi, sedangkan untuk informan penelitian adalah 55 personel Satuan Siber TNI AD dan 4 personel Spamad. Teknik analisis data menggunakan teknik trianggulasi data dengan cara membandingkan hasil wawancara yang diperoleh dari masing-masing sumber. Hasil penelitian ini adalah ancaman kejahatan siber mempengaruhi peningkatan fungsi Satuan Siber TNI AD untuk mencegah terjadinya sabotase, pencurian data rahasia militer dengan menggunakan sistem enkripsi, *hacking*, teror *digital*, serangan psikologi siber dan serangan terhadap infrastruktur dan sistem informatika TNI AD. Dalam upaya peningkatan fungsi Satuan Siber TNI AD masih terdapat beberapa faktor penghambat, yaitu : Keterbatasan kemampuan sumber daya manusia, sarana dan prasarana, masih lemahnya hukum/peraturan yang mengatur mekanisme kerja Satuan Siber TNI AD, terbatasnya koordinasi lintas sektoral antar Satuan Siber Nasional. Peran Satuan Siber TNI AD dalam mengungkap kejahatan siber masih terbatas pada *cyber defense*, monitoring media dan pelaporan konten atau berita *hoax* saja. Rekomendasi yang diajukan sesuai dengan revolusi industri 4.0 yang menjadi prioritas pemerintah yaitu membentuk arsitektur siber kontemporer, menciptakan manajemen keamanan dan kontijensi siber, membentuk kolaborasi keamanan siber dalam lingkup internasional, regional dan bilateral, meningkatkan penegakan hukum di bidang IT/siber, mengutamakan inovasi dan kreativitas dan peningkatan kemampuan SDM di bidang siber serta melakukan pendekatan antar *Stakeholder* di bidang siber nasional.

Kata Kunci : Kejahatan siber, Satuan Siber TNI AD, *Hoax, Hacking.*

Koleksi Perpustakaan Universitas Terbuka

UNIVERSITAS TERBUKA
PROGRAM PASCASARJANA
MAGISTER ADMINISTRASI PUBLIK

PERNYATAAN

TAPM yang berjudul Regulasi Penanganan Kejahatan Siber di Lingkungan TNI Angkatan Darat adalah hasil karya saya sendiri, dan seluruh sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila di kemudian hari ternyata ditemukan adanya penjiplakan (plagiat), maka saya bersedia menerima sanksi akademik.

Bogor, 04 Februari 2019

Yang Menyatakan

(Kaisar Bagus Purnawijaya Rhynaldie)
NIM. 500804786

Koleksi Perpustakaan Universitas Terbuka

UNIVERSITAS TERBUKA
PROGRAM PASCASARJANA
PROGRAM STUDI ADMINISTRASI PUBLIK

LEMBAR LAYAK UJI

Yang bertandatangan di bawah ini, Saya selaku Pembimbing TAPM dari Mahasiswa :

Nama/NIM	:	Kaisar Bagus Purnawijaya Rhynaldie/500804786
Judul TAPM	:	Regulasi Penanganan Kejahatan Siber di Lingkungan TNI Angkatan Darat

Menyatakan dengan sesungguhnya bahwa TAPM dari mahasiswa yang bersangkutan sudah/baru * selesai sekitar 85 % sehingga dinyatakan sudah layak uji/belum layak uji dalam Ujian Sidang Tugas Akhir Program Magister (TAPM).

Demikian keterangan ini dibuat untuk menjadikan periksa.

Bogor, 11 Februari 2019

Pembimbing II	Pembimbing I
Dr. Ir. Soesilo Wibowo, M.Si.	Riswanda, S.Sos., M.P.A., Ph. D.
NIP.195308271979031002	NIP. 198104122008121001

Koleksi Perpustakaan Universitas Terbuka

UNIVERSITAS TERBUKA
PROGRAM PASCASARJANA
PROGRAM MAGISTER ADMINISTRASI PUBLIK

PENGESAHAN HASIL UJIAN SIDANG

Nama	:	Kaisar Bagus Purnawijaya Rhynaldie
NIM	:	500804786
Program Studi	:	Magister Ilmu Administrasi
Judul TAPM	:	Regulasi Penanganan Kejahatan Siber di Lingkungan TNI Angkatan Darat

TAPM telah dipertahankan di hadapan Panitia Penguji Tugas Akhir Program Magister (TAPM) Administrasi Publik Program Pascasarjana Universitas Terbuka pada :

Hari/Tanggal	:	Selasa/19 Februari 2019
Waktu	:	16.00 WIB

Dan telah dinyatakan LULUS

PANITIA PENGUJI TAPM

Tandatangan

Ketua Komisi Penguji
Nama : Dr. Darmanto, M.Ed. .....

Penguji Ahli
Nama : Prof. Dr. Ngadisah, M.A. .....

Pembimbing I
Nama : Riswanda, S.Sos., M.P.A., Ph. D. .....

Pembimbing II
Nama : Dr. Ir. Soesilo Wibowo, M.Si. .....

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

PERSETUJUAN TAPM PASCA UJIAN SIDANG

Judul TAPM	:	Regulasi Penanganan Kejahatan Siber di Lingkungan TNI Angkatan Darat
Penyusun TAPM	:	Kaisar Bagus Purnawijaya Rhynaldie
NIM	:	500804786
Program Studi	:	Magister Ilmu Administrasi
Hari/Tanggal	:	Sabtu/16 Maret 2019

Menyetujui :

Pembimbing II,

Dr. Ir. Soesilo Wibowo, M.Si.
NIP. 195308271979031002

Pembimbing I,

Riswanda, S.Sos., M.P.A., Ph. D.
NIP. 198104122008121001

Penguji Ahli

Prof. Dr. Ngadisah, M.A.
NIP. 195107031979032001

Mengetahui,

Ketua Pascasarjana
Magister Administrasi Publik

Dr. Darmanto, M.Ed.
NIP. 195910271986031003

Dekan Fakultas Hukum,
Ilmu Sosial dan Ilmu politik

Dr. Sofjan Asbin, M.Si.
NIP. 196606191992031002

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

KATA PENGANTAR

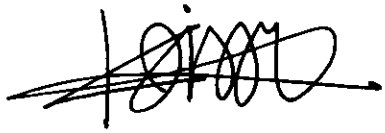
Dengan memanjatkan puji dan syukur ke hadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya kepada penulis sehingga akhirnya penulis dapat menyelesaikan Tugas Akhir Program Magister dengan judul "Regulasi Penanganan Kejahatan Siber di Lingkungan TNI Angkatan Darat" dengan baik dan lancar untuk dijadikan salah satu syarat memperoleh gelar Magister Administrasi Publik.

Penulis menyadari bahwa penulisan Tugas Akhir Program Magister ini tidak akan berhasil tanpa adanya dukungan dari berbagai pihak. Dalam kesempatan ini penulis mengucapkan terima kasih kepada:

1. Ibu Prof. DR. Ngadisah, M.A., selaku dosen penguji ahli, Bapak Riswanda Ph. D., selaku dosen pembimbing I dan Bapak Dr. Ir. Soesilo Wibowo, M.S., selaku pembimbing II yang telah menyediakan waktu, tenaga dan pikiran untuk mengarahkan penulis dalam menyusun Tugas Akhir Program Magister ini;
2. Ketua P4s;
3. Pejabat P4s-Universitas Terbuka;
4. Ketua P4s Ilmu Sosial dan Ilmu Politik;
5. Kepala UPBJJ Universitas Terbuka Bogor;
6. Jajaran Staf P4s dan UPBJJ-Universitas Terbuka
7. Jajaran Staf Satuan Siber TNI AD dan Spamad
8. Orang tua, Istri dan anak-anak serta keluarga tersayang yang selalu mendukung menyelesaikan Tugas Akhir Program Magister ini;
9. Rekan mahasiswa seangkatan Program Magister serta pihak lain yang tidak dapat disebutkan penulis dalam kesempatan ini.

Akhir kata semoga Tuhan Yang Maha Esa selalu memberikan berkat dan rahmat-Nya kepada kita semua, dan semoga Tugas Akhir Program Magister ini dapat bermanfaat bagi kita semua.

Bogor, 04 Februari 2019
Penulis,



Kaisar Bagus Purnawijaya Rhynaldie
NIM. 500804786

Koleksi Perpustakaan Universitas Terbuka

RIWAYAT HIDUP

Nama	:	Kaisar Bagus Purnawijaya Rhynaldie
NIM	:	500804786
Program studi	:	Magister Ilmu Administrasi
Tempat/Tanggal Lahir	:	Lombok Timur/25 Juni 1984

Riwayat Pendidikan :

Lulus SD di SDN 21 Mataram pada Tahun 1996
Lulus SMP di SLTPN 2 Mataram pada Tahun 1999
Lulus SMA di SMU Taruna Nusantara Magelang pada Tahun 2002
Lulus S1 di UT Palembang pada Tahun 2016

Riwayat Pekerjaan :

Tahun 2003 s/d 2006 sebagai Taruna di Akademi Militer, Magelang
Tahun 2006 s/d 2007 sebagai Perwira TNI AD di Bandung
Tahun 2007 s/d 2016 sebagai Perwira TNI AD di Palembang
Tahun 2016 s/d sekarang sebagai Pamen TNI AD di Jakarta

Bogor, 04 Februari 2019
Penulis

Kaisar Bagus Purnawijaya Rhynaldie
NIM. 500804786

Koleksi Perpustakaan Universitas Terbuka

DAFTAR ISI

Halaman

Abstract ii
Abstrak iii
Halaman Pernyataan Bebas Plagiasi iv
Halaman Persetujuan Layak Uji v
Lembar Pengesahan Hasil Ujian Sidang vi
Lembar Persetujuan TAPM Pasca Ujian Sidang vii
Kata Pengantar viii
Riwayat Hidup ix
Daftar Isi x
Daftar Tabel xi
Daftar Bagan/Gambar xii
Daftar Lampiran xiv

BAB I PENDAHULUAN 1
A. Latar Belakang Masalah 1
B. Rumusan Permasalahan 9
C. Tujuan Penelitian 9
D. Kegunan Penelitian 10

BAB II TINJAUAN PUSTAKA 11
A. Landasan Teori 11
B. Penelitian Terdahulu 100
C. Kerangka Berpikir 103
D. Operasionalisasi Konsep 106
E. Hipotesis 107

BAB III METODOLOGI PENELITIAN 109
A. Desain Penelitian 109
B. Sumber Informasi dan Penentuan Informan 110
C. Instrumen Penelitian 111
D. Prosedur Pengumpulan Data 112
E. Metode Analisis Data 114

BAB IV HASIL DAN PEMBAHASAN 116
A. Deskripsi Objek Penelitian 116
B. Hasil 117
C. Pembahasan 132

BAB V KESIMPULAN DAN SARAN 195
A. Kesimpulan 195
B. Saran 197

DAFTAR PUSTAKA xv

Koleksi Perpustakaan Universitas Terbuka

DAFTAR TABEL

Halaman

Tabel 2.1 Operasional Konsep Penelitian..... 107

Tabel 4.1 Daftar *Informan* Penelitian Analisis Faktor Kejahatan Siber Terhadap Peningkatan Fungsi Satuan Siber TNI AD.. 118

Tabel 4.2 Konsep Tren Ancaman Kejahatan Siber terhadap Institusi TNI AD 120

Tabel 4.3 Konsep Faktor Ancaman Kejahatan Siber terhadap Institusi TNI AD 125

Tabel 4.4 Konsep Pandangan Terhadap Faktor Penghambat Peningkatan Fungsi Satuan Siber TNI AD 132

Koleksi Perpustakaan Universitas Terbuka

DAFTAR BAGAN/GAMBAR

Halaman

Gambar 1.1 Jumah Pengguna Internet di Indonesia Tahun 2017 2

Gambar 1.2 Kesadaran Masyarakat Akan Keamanan Internet 3

Gambar 1.3 Tingkat Perkembangan Kejahatan Siber di beberapa Negara..... 5

Gambar 2.1 Perkembangan Revolusi Industri 53

Gambar 2.2 Tingkat Perkembangan Masyarakat Dunia 58

Gambar 2.3 Visualisasi Perubahan dalam Masyarakat 5.0 67

Gambar 2.4 Struktur Organisasi Pusintelad sesuai Perkasad 2014 95

Gambar 2.5 Struktur Organisasi PII Pusintelad sesuai Usulan Validasi 96

Gambar 2.6 Struktur Organisasi Balaksandi Pusintelad sesuai Usul Perubahan Renstra 2014-2019 97

Gambar 2.7 Struktur Organisasi Balaksandi Pusintelad Usulan Validasi 98

Gambar 2.8 Skema Kerangka Penelitian 104

Bagan 4.1 Struktur Organisasi Satuan Siber TNI AD 117

Bagan 4.2 Mekanisme *Monitoring* Berita *Online*/Medsos Dalam Fungsi *Defence* Satuan Siber TNI AD 127

Bagan 4.3 Mekanisme *Monitoring* Berita *Online*/Medsos Dalam Fungsi *Offence* Satuan Siber TNI AD 128

Bagan 4.4 Perbandingan Karakteristik Kejahatan Siber dan Kejahatan Konvensional 138

Bagan 4.5 Alur Kolaborasi/Sinergitas Satuan Siber di Indonesia 144

Bagan 4.6 Korelasi Faktor-Faktor Penghambat Peningkatan Fungsi Satuan Siber TNI AD 171

Gambar 4.1 Kerugian Akibat Pelanggaran Data Secara Global 179

Koleksi Perpustakaan Universitas Terbuka

437794.pdf

Gambar 4.2 Ancaman Siber dalam Revolusi Industri 4.0 180

Gambar 4.3 Strategi Keamanan Siber Nasional 192

Koleksi Perpustakaan Universitas Terbuka

i97794.pdf

DAFTAR LAMPIRAN

Halaman

Lampiran 1. Panduan Wawancara xvi

Lampiran 2. Transkrip Wawancara xxv

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

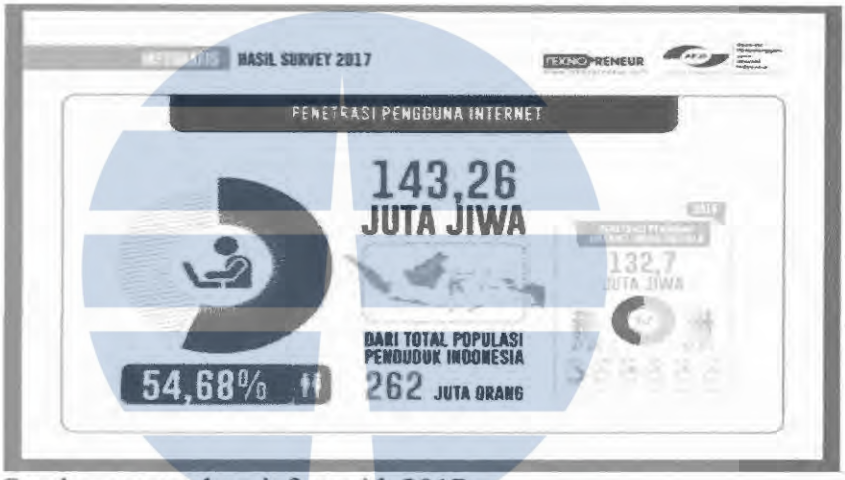
Informasi mempunyai arti dan peranan yang sangat penting bagi semua aspek kehidupan, serta merupakan salah satu kebutuhan hidup bagi semua orang baik individual maupun organisasi, sehingga dapat dikatakan dalam masyarakat bahwa informasi telah berfungsi sebagaimana layaknya aliran darah sumber kehidupan bagi tubuh manusia. Informasi menyebar begitu cepat melalui dunia maya (*cyber space*) yang menampilkan realitas yang tidak nyata, yaitu realitas virtual (*virtual reality*) yang tidak mengenal batas negara.

Internet sebagaimana yang kita kenal memiliki dua sisi mata uang, di satu sisi bernilai positif dalam membantu pekerjaan kita sehari-hari, namun di sisi yang lain menghasilkan dampak negatif yang disebut kejahatan siber. Kejahatan siber, merupakan salah satu bentuk atau dimensi baru kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Beberapa julukan diberikan kepada kejahatan jenis baru ini, antara lain kejahatan dunia maya (*cyber-space/virtual-space offence*) yang merupakan dimensi baru dari *hi-tech crime*, *transnational crime* dan *white collar crime*. Kejahatan siber meliputi: *Joy computing* (menggunakan komputer secara tidak sah atau tanpa izin), *Hacking* (menyambung dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa izin pemilik jaringan komputer), *Carding* (menyalahgunakan kartu

Koleksi Perpustakaan Universitas Terbuka

kredit), membocorkan data rahasia dan penyia-nyiaan data komputer (merusak/menghancurkan media penyimpanan data/program komputer).

Indonesia termasuk salah satu negara dengan pengguna internet atau dunia maya dengan jumlah banyak *di dunia*. Berdasarkan survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada Tahun 2017, lebih dari 50 persen atau sekitar 143 juta orang Indonesia telah terhubung jaringan internet.



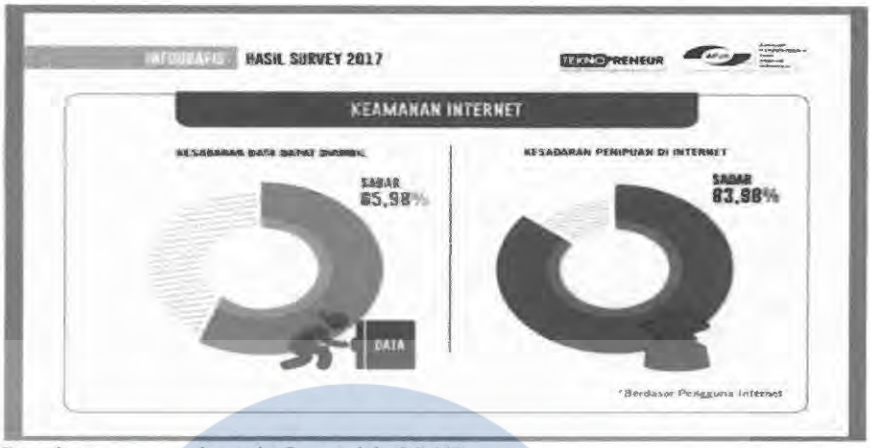
Sumber : www.kominfo.go.id, 2017

Gambar 1.1
Jumlah Pengguna Internet di Indonesia Tahun 2017

Berdasarkan Gambar 1.1, di negara Indonesia 54,68 persen penduduknya adalah pengguna internet atau sejumlah 143,26 juta jiwa dari total populasi sebanyak 262 juta orang. Seiring dengan cepat meningkatnya pengguna internet di Indonesia, satu fakta yang mengejutkan datang dari perusahaan *monitoring* internet Akamai yang mengungkap bahwa kejahatan internet di Indonesia meningkat dua kali lipat. Angka ini menempatkan Indonesia di posisi pertama negara berpotensi menjadi target *hacker*, menggantikan Tiongkok. Dari 175

Koleksi Perpustakaan Universitas Terbuka

negara yang diinvestigasi, Indonesia berkontribusi sebanyak 38 persen dari total sasaran trafik *hacking* di internet.



Sumber : www.kominfo.go.id, 2017

Gambar 1.2
Kesadaran Masyarakat akan Keamanan Internet

Pada Gambar 1.2 sebanyak 65,98 persen pengguna internet di Indonesia sadar bahwa data yang mereka miliki dapat diambil atau *hacking*. Sebanyak 83,98 persen pengguna internet di Indonesia juga sadar bahwa banyak terjadi penipuan melalui internet. Namun, meskipun adanya kesadaran yang cukup tinggi, tidak membuat kejahatan internet berkurang justru semakin bertambah banyak. Menurut David Belson dari Akamai *Research*, Indonesia memiliki kecepatan internet yang masih di bawah rata-rata dengan kecepatan maksimum hanya bisa mencapai 11,3 Mbps. Berdasarkan laporan tersebut, meskipun memiliki kecepatan internet yang terbatas, pada nyatanya Indonesia menjadi negara penghasil serangan siber di dunia selain Amerika dan Tiongkok. Dalam penelitian Akamai tersebut dikatakan juga kecepatan pertumbuhan internet tidak memiliki hubungan dengan potensi besarnya kejahatan internet yang mengancam Indonesia.

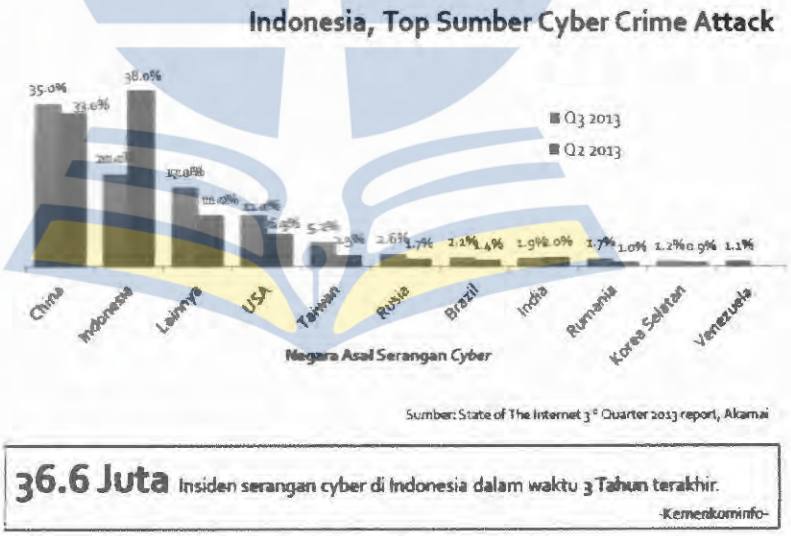
Koleksi Perpustakaan Universitas Terbuka

Aksi *hacking* lebih dikarenakan lemahnya sistem keamanan internet dan komputer di Indonesia.

Meningkatnya kejahatan siber ini adalah dampak negatif dari kemajuan dunia *digital* secara global sebagai efek negatif dari revolusi industri 4.0 yang penyebab utamanya adalah ketidakmampuan kita untuk segera beradaptasi dengan perkembangan ancaman tersebut. Sesuai dengan konsep masyarakat 5.0 yang baru-baru ini diperkenalkan oleh negara Jepang, maka dalam menghadapi kejahatan siber diperlukan sinergitas antar lembaga publik di bidang siber yang saling berkolaborasi/bekerjasama baik organisasi pemerintah, swasta maupun individu, sehingga terbentuk sistem yang terintegrasi dalam menangkal dan menghadapi kejahartan siber di Indonesia. Selain itu, dengan semakin hilangnya konsep batas-batas negara secara ***virtual***, maka kerjasama secara regional bahkan global juga perlu dilakukan, karena kejahatan jenis ini sudah merupakan ancaman nyata bagi tatanan masyarakat dunia. Langkah awal yang harus diterapkan dalam anti *cyber crime* di Indonesia adalah dengan adanya undang-undang yang mengatur kejahatan siber yaitu Undang-Undang Nomor 11 Tahun 2008 dan disempurnakan dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sebelum diundangkannya Undang - Undang Informasi dan Transaksi Elektronik tersebut, modus kejahatan dalam dunia siber memang agak sulit dimengerti oleh orang – orang yang tidak menguasai pengetahuan teknologi informasi dalam modus operandinya. Sifat ini

Koleksi Perpustakaan Universitas Terbuka

membuat *cyber crime* berbeda dengan tindak pidana lainnya, maka apabila di Indonesia ada seseorang yang melakukan perilaku kejahatan di dalam internet sebagai sasaran utama kejahatannya atau menggunakan program internet maka diterapkan Kitab Undang Hukum Pidana sebagai undang – undang pidana umum. Hal tersebut dapat dilakukan sepanjang KUHP ditemukan pasal – pasal yang pas dan tepat untuk menjatuhkan pidana, tapi nyatanya sampai saat ini belum ada teknik pelaksanaan yang jelas terkait pelaksanaan Undang-Undang Nomor 11 Tahun 2008 dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sehingga sampai saat ini Indonesia menjadi salah satu negara dengan tingkat kejahatan siber yang tinggi.



Sumber : Kemenkominfo, 2013

Gambar 1.3
Tingkat Perkembangan Kejahatan Siber di Beberapa Negara

Koleksi Perpustakaan Universitas Terbuka

Hasil studi Frost dan Sullivan yang diprakarsai oleh Microsoft mengungkapkan bahwa potensi kerugian ekonomi di Indonesia yang diakibatkan oleh insiden keamanan siber dapat mencapai nilai USD 34,2 miliar atau setara Rp 438 triliun. Angka tersebut setara dengan 3,7 persen jumlah total PDB Indonesia sebesar USD 932 miliar. Selain kerugian finansial, insiden keamanan siber mengurangi kemampuan berbagai organisasi di Indonesia untuk memanfaatkan peluang-peluang yang ada di era ekonomi digital saat ini.

Untuk menanggulangi bahaya *cyber crime* maka dibutuhkannya adanya *cyber security*. Sasaran serangan siber adalah *public-utility* yang dikendalikan secara terpusat. Baik yang berskala lokal, nasional, apalagi global. Semakin terpusat sistem kendali dari *public-utility* itu, semakin rentan untuk dilumpuhkan dalam sekali serangan, maka umumnya negara yang sadar adanya potensi perang siber akan membangun infrastruktur sistem kendali *public-utility*-nya secara eksklusif agar memiliki tingkat keamanan dan ketahanan yang tinggi. Untuk sistem pertahanan dan keamanan nasional salah satunya adalah menggunakan peranan TNI Angakatan Darat, karena TNI Angkatan Darat sebagai unsur utama kekuatan pertahanan di darat yang mempunyai tugas pokok dan fungsi sesuai Undang-Undang Nomor 34 Tahun 2004, yaitu TNI dituntut untuk berperan aktif dalam menjaga dan mempertahankan kedaulatan Negara Kesatuan Republik Indonesia dengan dilandasi kesetiaan dan ketaatan kepada Pancasila dan UUD 1945.

Koleksi Perpustakaan Universitas Terbuka

Saat era dunia maya inilah peranan TNI AD tidak hanya menghadapi peperangan secara konvensional tetapi juga kejahatan siber yang mengancam pertahanan nasional seperti timbulnya terorisme atau demonstrasi besar-besaran. Sebut saja ancaman demonstrasi besar dengan informasi yang diedarkan secara cepat melalui pesan aplikasi *whatsapp* pada 2 Desember 2016 menjadi aksi nasional di Indonesia dengan tuntutan penjarakan Gubernur DKI Jakarta atas dugaan penistaan agama. Selain itu, kasus lain adalah pada tanggal 19 Mei 2018 diperoleh informasi dari Kasandidam XIII/Merdeka bahwa adanya aplikasi penyandi (enskripsi) yang dipergunakan oleh kelompok teroris Poso untuk berkirim pesan melaui aplikasi *Whatsapp*. Setelah dilaksanakan koordinasi di lapangan, diperoleh aplikasi bernama *Amn Al Mujahid*, yang merupakan aplikasi penyandi pesan dan file sejenis *True Crypt*. Informasi hanya berukuran 1 *megabit* dan cepat. Aplikasi tersebut dipergunakan oleh para kelompok teroris yang ada di sekitar Poso untuk berkomunikasi pesan melalui aplikasi *Whatsapps*. Teroris menggunakan serangan berbasis internet karena murah, anominitas, penyangkalan yang masuk akal dan berbiaya murah kepada organisasi pemerintah dan non-pemerintah yang menjadi lawan ideologinya.

Dengan melihat dampak dari *cyber war* tersebut, maka pembangunan pertahanan siber adalah sebuah kebutuhan dan keharusan untuk melindungi pertahanan dan keamanan serta keberlangsungan hidup sebuah negara. Untuk menghadapi ancaman kejahatan siber yang mengancam pertahanan nasional, maka dibentuklah Badan Siber dan

Koleksi Perpustakaan Universitas Terbuka

Sandi Nasional (BSSN) yang merupakan suatu badan siber nasional yang mampu menjadi induk/koordinator bagi seluruh satuan siber di tanah air, menjamin terciptanya sinergitas antar organisasi siber yang meliputi organisasi *cyber defence* Kemhan dan TNI, organisasi *cyber crime* POLRI, organisasi *cyber intelligent* BIN dan organisasi siber Kemenkominfo.

Organisasi TNI saat ini telah membuat Satuan Siber (Satsiber TNI) yang bertugas menyelenggarakan kegiatan dan operasi siber di lingkungan TNI dalam rangka mendukung tugas pokok TNI. TNI AD sebagai bagian dari organisasi TNI sendiri telah menambahkan tugas kepada salah satu bidang intelijennya untuk melakukan deteksi alat sadap di ruangan pejabat, *jammer* kegiatan rapat pejabat, kegiatan forensik perangkat seluler, serta monitoring dan pelaporan media terbuka. Hal tersebut tidaklah cukup, dengan keterbatasan peran pokok TNI AD serta belum adanya teknis yang mengatur pelaksanaan Undang-Undang Nomor 11 Tahun 2008 dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik di lingkungan TNI AD maka perlu ditingkatkannya fungsi satuan siber menjadi suatu satuan organik yang lebih profesional guna melakukan operasi khusus dengan menggunakan kemampuan telematika dan manuver siber serta mampu mengoptimalkan jaring intel yang ada di wilayah untuk memonitor situasi dan potensi kerawanan yang mungkin timbul.

Kejahatan siber masih marak jika dilihat dari sudut pandang lemahnya hukum, namun dalam penelitian ini fokus penelitian adalah

Koleksi Perpustakaan Universitas Terbuka

kepada kejahatan siber dalam kaitannya dengan kepentingan negara khususnya peran dan fungsi Satuan Siber TNI AD dalam menghadapi kejahatan siber guna menjaga pertahanan nasional. Akibat lemahnya Undang-Undang dan juga keterbatasan sistem keamanan yang ada, bagaimana peranan dan apa saja yang dibutuhkan Satuan Siber TNI AD untuk bisa menghadapi era *cyber war*, sehingga fokus penelitian ini dirumuskan menjadi "Regulasi Penanganan Kejahatan Siber di Lingkungan TNI Angkatan Darat".

B. Perumusan Masalah

Sebagai sebuah pendekatan perencanaan dengan berbagai varian proses, maka permasalahan penelitian ini dapat dirumuskan dengan pertanyaan penelitian sebagai berikut:

1. Bagaimana ancaman kejahatan siber mempengaruhi fungsi Satuan Siber TNI AD?
2. Apa saja kendala yang dihadapi Satuan Siber TNI AD dalam mengungkap kejahatan siber?
3. Apa saja peran Satuan Siber TNI AD dalam mendukung sinergitas lembaga siber nasional untuk mengungkap kejahatan siber?

C. Tujuan Penelitian

Tujuan dilakukannya penelitian ini, yaitu:

1. Untuk mengetahui dan menganalisis bagaimana kejahatan siber mempengaruhi fungsi Satuan Siber TNI AD.
2. Untuk mengetahui dan menganalis kendala yang dihadapi Satuan Siber TNI AD dalam mengungkap kejahatan siber.

Koleksi Perpustakaan Universitas Terbuka

3. Untuk mengetahui dan menganalis peran Satuan Siber TNI AD dalam mendukung sinergitas lembaga siber nasional untuk mengungkap kejahatan siber.

D. Kegunaan Penelitian

Manfaat yang dapat dipetik dari hasil penelitian ini adalah sebagai berikut:

1. Memberikan sumbangan terhadap ilmu administrasi publik, khususnya bidang siber nasional.
2. Hasil-hasil penelitian ini dapat dijadikan masukan bagi TNI AD guna memerangi kejahatan siber.

Koleksi Perpustakaan Universitas Terbuka

BAB II

TINJAUAN PUSTAKA

A. Kajian Teori

1. Organisasi publik

a. Definisi organisasi publik.

Organisasi publik dikembangkan dari teori organisasi, oleh karena itu untuk memahami organisasi publik dapat ditinjau dari sudut pandang teori organisasi. Menurut Fahmi (2013:1) organisasi publik merupakan sebuah wadah yang memiliki multi peran dan didirikan dengan tujuan mampu memberikan serta mewujudkan keinginan berbagai pihak, dan tidak terkecuali kepuasan bagi pemiliknya. Sedangkan menurut Stephen P. Robbins dalam Fahmi (2013:2), organisasi publik merupakan kesatuan sosial yang dikoordinasikan secara sadar, dengan sebuah batasan yang relatif dapat diidentifikasi, yang bekerja atas dasar yang relatif terus menerus untuk mencapai tujuan bersama atau sekelompok tujuan. Pengertian organisasi publik berkenaan dengan proses pengorganisasian.

Menurut Handoko (2011:167) pengorganisasian merupakan proses penyusunan struktur organisasi yang sesuai dengan tujuan organisasi, sumberdaya yang

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

dimilikinya, dan lingkungan yang melingkupinya. Dengan demikian hasil pengorganisasian adalah stuktur organisasi, berkenaan dengan kesesuaian organisasi birokrasi yang menjadi penyelenggara implentasi kebijakan publik. Tantangannya adalah bagaimana agar tidak terjadi *bureaucratic fragmentation* karena struktur ini menjadikan proses implementasi menjadi jauh dari efektif. Di Indonesia sering terjadi inefektivitas implementasi kebijakan karena kurangnya koordinasi dan kerjasama diantara lembaga-lembaga negara dan pemerintah. Kebijakan yang begitu kompleks menuntut adanya kerjasama banyak organisasi, birokrasi sebagai pelaksana sebuah kebijakan harus dapat mendukung kebijakan yang telah diputuskan dengan melakukan koordinasi yang baik.

Dari penjelasan di atas dapat disimpulkan bahwa organisasi publik adalah salah suatu wadah yang menjamin penyediaan pelayanan publik sesuai dengan asas-asas umum pemerintahan dan korporasi yang baik serta untuk memberi perlindungan bagi setiap warga negara dan penduduk dari penyalahgunaan wewenang di dalam penyelenggaraan pelayanan publik, dilandasi dengan pengaturan hukum yang mendukungnya.

Koleksi Perpustakaan Universitas Terbuka

b. Tujuan organisasi publik.

Negara berkewajiban melayani setiap warga negara dan penduduk untuk memenuhi hak dan kebutuhan dasarnya dalam kerangka pelayanan publik yang merupakan amanat Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Pendirian organisasi publik merupakan upaya untuk mempertegas hak dan kewajiban setiap warga negara dan penduduk serta terwujudnya tanggung jawab negara dan korporasi dalam penyelenggaraan pelayanan publik, diperlukan norma hukum yang memberi pengaturan secara jelas.

Tujuan organisasi publik sendiri menurut Etzioni dalam Handoko (2011:109), yaitu suatu keadaan yang diinginkan di mana organisasi bermaksud untuk merealisasikan dan sebagai pernyataan tentang keadaan di waktu yang akan datang di mana organisasi sebagai kolektifitas mencoba untuk menimbulkannya. Tujuan organisasi meletakkan kerangka prioritas untuk memfokuskan arah semua program dan aktivitas lembaga dalam melaksanakan misi lembaga.

Pendirian organisasi publik bertujuan secara optimal bagi peningkatan:

1) Kesejahteraan rakyat, karena pada hakekatnya pelayanan publik merupakan infrastruktur bagi

Koleksi Perpustakaan Universitas Terbuka

setiap warga negara untuk mencapai suatu kesejahteraan.

2) Budaya dan kualitas aparat pemerintah untuk menjadi abdi bagi negara dan masyarakatnya, bukan sebagai penguasa terhadap negara dan masyarakatnya.

3) Kualitas pelayanan umum atau publik di berbagai bidang pemerintahan umum dan pembangunan terutama pada unit-unit kerja pemerintah pusat dan daerah, sehingga masyarakat diharapkan akan mendapatkan perilaku pelayanan yang lebih cepat, tepat, murah, dan memuaskan. Selain itu, era reformasi menuntut pelayanan umum harus transparan dan tidak diskriminatif dengan menerapkan prinsip-prinsip akuntabilitas dan pertimbangan efisiensi.

c. Konsep sinergitas kelembagaan.

Adanya interaksi antar ketiga *stakeholders* selain itu juga diperlukan adanya sinergi antar ketiga pemangku kepentingan tersebut. Najiyati dan Rahmat (2011), mengartikan sinergi sebagai kombinasi atau paduan unsur atau bagian yang dapat menghasilkan keluaran lebih baik dan lebih besar. Jadi sinergi dapat dipahami sebagai operasi gabungan atau perpaduan unsur untuk menghasilkan *output*

Koleksi Perpustakaan Universitas Terbuka

yang lebih baik. Sinergitas dapat terbangun melalui dua cara yaitu:

1) Komunikasi. Sofyandi dan Garniwa (2007), pengertian komunikasi dapat dibedakan atas dua bagian, yaitu:

   a) Pengertian komunikasi yang berorientasi pada sumber menyatakan bahwa, komunikasi adalah kegiatan dengan mana seseorang (sumber) secara sungguh-sungguh memindahkan stimulus guna mendapatkan tanggapan.

   b) Pengertian komunikasi yang berorientasi pada penerima memandang bahwa, komunikasi sebagai semua kegiatan di mana seseorang (penerima) menanggapi stimulus atau rangsangan.

2) Koordinasi. Di samping adanya komunikasi dalam menciptakan sinergitas juga memerlukan koordinasi. Komunikasi tidak dapat berdiri sendiri tanpa adanya koordinasi seperti yang dinyatakan oleh Hasan bahwasannya dalam komunikasi dibutuhkan koordinasi (2005, h.18). Silalahi (2011, h.217), "koordinasi adalah integrasi dari kegiatan-kegiatan individual dan unit-unit ke dalam satu

Koleksi Perpustakaan Universitas Terbuka

usaha bersama yaitu bekerja ke arah tujuan bersama". Moekijat (1994, h.39) menyebutkan ada 9 (sembilan) syarat untuk mewujudkan koordinasi yang efektif, yaitu:

a) Hubungan langsung. Koordinasi dapat lebih mudah dicapai melalui hubungan pribadi langsung.

b) Kesempatan awal. "Koordinasi dapat dicapai lebih mudah dalam tingkat-tingkat awal perencanaan dan pembuatan kebijaksanaan".

c) Kontinuitas. "Koordinasi merupakan suatu proses yang kontinu dan harus berlangsung pada semua waktu mulai dari tahap perencanaan".

d) Dinamisme. "Koordinasi harus secara terus-menerus diubah mengingat perubahan lingkungan baik *intern* maupun *ekstern*".

e) Tujuan yang jelas. "Tujuan yang jelas itu penting untuk memperoleh koordinasi yang efektif".

f) Organisasi yang sederhana. "Struktur organisasi yang sederhana memudahkan koordinasi yang efektif".

Koleksi Perpustakaan Universitas Terbuka

g) Perumusan wewenang dan tanggung jawab yang jelas. Wewenang yang jelas tidak hanya mengurangi pertentangan di antara pegawai-pegawai yang berlainan, tetapi juga membantu mereka dalam pekerjaan dengan kesatuan tujuan.

h) Komunikasi yang efektif. Komunikasi yang efektif merupakan salah satu persyaratan untuk koordinasi yang baik.

i) Kepemimpinan supervisi yang efektif. Kepemimpinan yang efektif menjamin koordinasi kegiatan orang-orang, baik pada tingkat perencanaan maupun pada tingkat implementasi.

2. Manajemen sumberdaya manusia (MSDM)

a. Definisi manajemen sumberdaya manusia (MSDM).

MSDM secara umum dapat dipahami baik dari makna sistem maupun fungsi. Dari sisi makna sistem, MSDM tidak lain merupakan suatu sistem manajemen yang sengaja dirancang untuk dapat memastikan bahwa potensi atau bakat semua individu dalam organisasi dapat diutilisasi (digunakan) secara efektif dan efisien (Mathis & Jackson 2008). Utilisasi individu tersebut dimaksudkan untuk mencapai tujuan dan target yang telah ditentukan

Koleksi Perpustakaan Universitas Terbuka

organisasi. Sistem tersebut kemudian diimplementasikan ke dalam beberapa fungsi MSDM yang akhirnya membentuk suatu rumusan definitif MSDM fungsional yaitu "semua kegiatan yang dimulai dengan perencanaan SDM sampai pada pemberhentian atau terminasi SDM". Di antara kegiatan vital lain setelah fungsi perencanaan dan sebelum terminasi SDM adalah penyusunan analisis jabatan, rekrutmen SDM yang dilanjutkan dengan seleksi dan penempatan SDM dalam jabatan yang relevan, kemudian berturut-turut fungsi penggajian, penilaian kinerja, pelatihan dan pengembangan, pengelolaan karir dalam jabatan, pembinaan hubungan antar individu (*employee relationships*), serta perancangan berbagai program kualitas kehidupan kerja (*quality of working life*).

Namun demikian, MSDM tidaklah cukup dapat dipahami hanya dari sisi sistem dan fungsi. MSDM akan memiliki arti yang lebih komprehensif bagi organisasi jika dilihat pula dari sisi kebijakan (*policy*). Dari sisi kebijakan, MSDM secara klasik sebagaimana dikembangkan oleh Guest (1987) bermakna sebagai salah satu bentuk kebijakan organisasi yang sengaja dirancang untuk memaksimalkan integrasi semua unsur organisasi (*organizational integration*), membangun komitmen pegawai terhadap organisasi (*employee commitment*), prinsip kelenturan

Koleksi Perpustakaan Universitas Terbuka

dalam pelaksanaan fungsi manajerial dan pekerjaan (*flexibility*) untuk menghindari kekakuan (*rigidity*), serta pencapaian kualitas baik dari sisi proses pelaksanaan maupun hasil dari pelaksanaan pekerjaan (*quality of work*). Dari sisi kebijakan inilah akhirnya berkembang suatu pemikiran, bahwa makna utuh dari MSDM tidak terbatasi dalam pengertian yang sekadar bersifat teknis. Lebih daripada masalah teknis, MSDM ternyata juga mengalami konvergensi peran yang sifatnya lebih substansial.

Konvergensi peran yang dialami MSDM tersebut telah terjadi sejak tahun 2000-an. Sebagaimana pernah diuraikan oleh Lengnick-Hall & Lengnick-Hall (2003: 33-43) peran MSDM yang mengalami konvergensi tersebut tidak lain dimaksudkan untuk merespon perubahan lingkungan dengan segala macam tantangan dan tuntutan yang ada di dalamnya. Dengan peran yang baru, MSDM mengemban misi dalam menyajikan layanan bagi SDM (*human capital steward*), memberi fasilitasi berupa pengetahuan bagi SDM (*knowledge facilitator*), membangun interaksi kondusif bagi semua pihak (*relationship builder*), serta memiliki keahlian yang terspesialisasi dalam mengatasi setiap masalah organisasional secara tepat dan cepat (*rapid deployment specialist*). Berbagai macam persoalan yang muncul dalam

Koleksi Perpustakaan Universitas Terbuka

48794.pdf

era yang sedang mengalami perubahan secara drastis diharapkan dapat dipecahkan melalui konvergensi peran MSDM ini. Unit fungsional MSDM tidak sekadar berputar pada penanganan masalah teknis, namun juga berkembang pada orientasi pemberian layanan dan fasilitasi bagi semua pihak dalam organisasi.

b. Prinsip dasar manajemen sumberdaya manusia (MSDM).

Sektor publik memiliki asas yang sama dengan sektor privat dalam melakukan fungsi manajerial. Sejak lingkungan organisasi berkembang dengan dinamika yang sangat intensif pada dekade 1990-an, fungsi manajerial diarahkan pada pengembangan perilaku individu dengan mengacu pada panduan umum yang oleh Wright & Rudolph (1994) ditekankan pada lima aspek yaitu:

1) *Emphasis on people*.

Secara alamiah, organisasi diadakan untuk memenuhi kebutuhan manusia. Sementara dalam melakukan utilisasi SDM, organisasi secara eksplisit menunjukkan adanya pemosisian manusia sebagai unsur utama di dalamnya. Dengan demikian unsur manusia dalam organisasi tidak hanya sekadar bersifat pasif, namun lebih bersifat aktif untuk menghadapi sejumlah tantangan dan siap mengembangkan diri demi kelangsungan organisasi

Koleksi Perpustakaan Universitas Terbuka

itu sendiri. Sebagaimana telah diidentifikasi oleh Jacob & Washington (2003) bahwa pengembangan kualitas SDM berdasarkan hasil sejumlah riset diyakini dapat meningkatkan kinerja organisasi.

2) *Participative leadership.*

MSDM memiliki prinsip kepemimpinan yang bersifat partisipatif. Jika mencermati prinsip MSDM pertama yang memposisikan unsur manusia sebagai pihak yang bersifat aktif, prinsip kedua ini pun juga memposisikan figur pemimpin sebagai pihak yang aktif dan tidak sekadar bersifat situasional. Secara teoritis, kepemimpinan terbaik adalah dengan menyesuaikan diri terhadap semua perubahan bentuk situasional. Namun kepemimpinan yang terbaik dari yang terbaik adalah kemampuan penyesuaian diri pemimpin secara aktif disertai tingkat pelibatan diri pada semua level organisasi secara intensif dan dengan kemampuan membentuk lingkungan yang kreatif (Amabilea 2004).

3) *Innovative workstyles.*

Prinsip dasar ketiga MSDM merujuk pada perilaku inovatif yang tidak berhenti maknanya pada hasil yang telah dapat dicapai seorang individu.

Koleksi Perpustakaan Universitas Terbuka

Prinsip ketiga ini merujuk pada kemampuan individu untuk dapat merefleksikan diri pada kinerja (Vaughan 2003) yang telah dicapai dan kemudian mempelajarinya sedemikian rupa sehingga akan dapat mencapai tingkat yang lebih baik di masa mendatang.

4) *Strong client orientation.*

Akibat tingkat persaingan yang kian intensif, orientasi organisasi lebih cenderung bersifat *outward looking*. Dalam konteks yang demikian inilah kepuasan pelanggan (untuk sektor privat) dan masyarakat (untuk sektor publik) tidak hanya merupakan tujuan namun juga sekaligus sebagai "instrumen" bagi organisasi untuk mencapai *Sustained Competitive Advantage* (SCA) atau keunggulan bersaing secara berkelanjutan (Chan et al. 2004). Prinsip keempat MSDM memegang peranan yang sangat penting dalam era *Scarcity Resources* yakni sumberdaya yang tersedia semakin terbatas sementara tuntutan masyarakat pengguna produk dan jasa organisasi semakin bervariasi sehingga kebutuhan akan sumberdaya menjadi meningkat (Wang & Lo 2003).

Koleksi Perpustakaan Universitas Terbuka

5) *A mindset that seeks optimum performance.*

Sementara prinsip kelima dalam MSDM tetap memposisikan figur sentral individu sebagai pihak yang memegang teguh sejumlah nilai luhur yang dapat mengarahkan dirinya pada berbagai upaya perbaikan. *Mindset* menjadi konsep yang sangat penting untuk menunjukkan bahwa persepsi, sikap, dan perilaku individu memiliki kejelasan arah dalam membangun kesuksesan organisasi. Pengalaman di negara lain membuktikan bahwa keunggulan organisasi dapat dicapai melalui pengembangan SDM (Pattanayak 2003) sebagai instrumen dalam memenangkan persaingan dan mencapai keberhasilan.

Kelima prinsip MSDM tersebut menjadi pelajaran penting dalam membangun organisasi bermutu yang berpusat pada pengembangan SDM. Prinsip-prinsip MSDM tersebut juga menegaskan kembali bahwa tanpa SDM bermutu, organisasi dipastikan tidak dapat mencapai keberhasilan.

Menurut Figen Cakar dan kawan-kawan terdapat tiga komponen strategi MSDM yang dapat dijelaskan sebagai berikut:

Koleksi Perpustakaan Universitas Terbuka

1) Perumusan strategi MSDM.

Dalam tahapan perumusan strategi MSDM ini ditentukan batas-batas tentang:

a) *Objective activity*, yakni melakukan intepretasi terhadap strategi dan tujuan organisasi serta berbagai proses kegiatan utama dalam organisasi dikaitkan dengan kebutuhan dan tujuan MSDM.

b) *Establish current capability activity*, yakni menentukan kapabilitas SDM yang ada dalam organisasi dikaitkan dengan berbagai proses utama dalam organisasi untuk mencapai berbagai tujuan dan sasaran yang telah ditetapkan.

c) *Plan activity*, yakni mengembangan suatu rencana, termasuk di dalamnya anggaran.

d) *Negotiate budget activity*, yakni menggunakan perencanaan untuk melakukan negosiasi dalam rangka memperoleh anggaran yang memadai yang dapat diyakini sebagai instrumen meraih keberhasilan implementaasi strategi MSDM.

e) *Set HR policies activity*, yakni menentukan jenis-jenis kompensasi, metode staffing, metode penilaian kinerja, membentuk skema pelatihan dan pengembangan, serta menciptakan situasi dan

Koleksi Perpustakaan Universitas Terbuka

kondisi kerja yang kondusif dan relevan dengan kebutuhan implementasi strategi.

2) Implementasi strategi MSDM.

Implementasi startegi akan menghasilkan *redeployment* SDM yang meliputi:

a) *Control HR*, yakni memastikan bahwa SDM sudah terencana, terlaksana dan terpantau secara tepat dan benar dalam kaitannya dengan tujuan dan sasaran yang diinginkan organisasi.

b) *Recruit activity*, yakni perhatian terhadap posisi SDM yang *in line* dengan kebutuhan organisasi baik berasal dari sumber dalam maupun luar untuk memperoleh SDM yang tepat.

c) *Train, educate, develop*, yakni kegiatan yang diarahkan untuk melakukan *upgrading* kapabilitas bagi semua SDM yang ada sesuai dengan kebutuhan organisasi.

d) *Manage HR performance*, yakni kegiatan yang diarahkan untuk menentukan berbagai target individual, pemantauan terhadap kemajuan dan perkembangan berdasarkan target yang telah ditentukan serta melakukan identifikasi tentang kebutuhan pelatihan, pengembangan, dan pendidikan sebagai respon atas hasil penilaian

Koleksi Perpustakaan Universitas Terbuka

kinerja sebelum menentukan tindakan baik dalam bentuk *reward* maupun *discipline action*.

e) *Manage redeployment*, yakni kegiatan untuk mengidentifikasi defisiensi posisi pekerjaan yang tidak dapat diatasi (*rectified*) baik melalui pelatihan, pengembangan ataupun pendidikan yang diarahkan pada *redeployment* bagi pemegang pekerjaan/jabatan baik di dalam maupun di luar organisasi.

f) *Negotiation for working conditions*, yakni kegiatan yang diarahkan untuk memenuhi kebutuhan SDM dan pencapaian tujuan organisasi.

3) Pemantauan dampak atas hasil organisasi.

Bagian ini dilakukan secara rinci yaitu dengan upaya:

a) *Monitor impact on business strategy*, yakni pemantauan dampak strategi SDM terhadap strategi serta kinerja organisasi.

b) *Monitor impact on people satisfaction*, yakni kegiatan yang dimasudkan untuk menentukan tingkat kepuasan SDM.

c) *Monitor impact on manage process*, yakni kegiatan yang berkaitan dengan *monitoring* kadar strategi MSDM dan implementasinya sehingga

Koleksi Perpustakaan Universitas Terbuka

dapat memenuhi semua kebutuhan dalam pengelolaan proses kegiatan.

d) *Monitor impact on operate process*, yakni kegiatan berkaitan dengan *monitoring* kadar kualitas strategi MSDM dan implementasinya dapat memenuhi semua kebutuhan proses kegiatan (*operate processes*) yang terdiri dari *get order, develop product, fulfil order*, dan *support product*.

e) *Monitor impact on support process*, yakni kegiatan yang berkaitan dengan *monitoring* kadar kualitas strategi MSDM dan implementasinya sehingga dapat memenuhi semua kebutuhan proses pendukung (*support processes*) yang terdiri dari keuangan dan Teknologi Informasi (TI) yang dapat mendukung berjalannya fungsi proses.

3. *Collaborative governance*

a. Definisi *collaborative governance*.

Istilah *collaborative governance* merupakan cara pengelolaan pemerintahan yang melibatkan secara langsung *stakeholder* di luar negara, berorientasi konsensus, dan musyawarah dalam proses pengambilan keputusan kolektif, yang bertujuan untuk membuat atau melaksanakan kebijakan publik serta program- program publik (Ansell & Gash, 2007, dalam Setyoko 2011: 15). Fokus dari

Koleksi Perpustakaan Universitas Terbuka

23794.pdf

collaborative governance ada pada kebijakan dan masalah publik. Institusi publik memang memiliki orientasi besar dalam pembuatan kebijakan, tujuan dan proses kolaborasi adalah mencapai drajat konsensus diantara para *stakeholder. Collaborative governance* menghendaki terwujudnya keadilan sosial dalam memenuhi kepentingan publik (Setyoko 2011: 16).

Menurut O'Leary dan Bingham dalam Sudarmo (2015: 195) kolaborasi merupakan konsep yang menggambarkan proses fasilitasi dan pelaksanaan yang melibatkan multi organisasi untuk memecahkan masalah yang tidak bisa atau tidak dengan mudah dipecahkan oleh sebuah organisasi secara sendirian. Pendapat ini didukung oleh Bardach dalam Sudarmo (2015: 195) yang mendefinisikan *collaboration* sebagai bentuk aktivitas bersama oleh dua institusi atau lebih yang bekerjasama ditujukan untuk meningkatkan *public value* ketimbang bekerja sendiri-sendiri.

Definisi *collaborative governance* menurut Ansell and Gash (2007) dalam Subarsono (2016: 175) menyatakan:

"A governing arrangement where one or more public agencies directlyengage non-state stakeholders in a collective decision-making processthat is formal, consensus- oriented, and deliberative and that aims tomake or implement public policy or manage public programs orassets". (*collaborative governance* adalah serangkaian pengaturan di mana satu atau lebih lembaga publik yang melibatkan secara langsung *stakeholders non state* di dalam

Koleksi Perpustakaan Universitas Terbuka

proses pembuatan kebijakan yang bersifat formal, berorientasi konsensus dan deliberatif yang bertujuan untuk membuat atau mengimplementasikan kebijakan publik atau mengatur program publik atau aset).

Defenisi tersebut dapat dirumuskan menjadi beberapa kata kunci yang menekankan pada enam karakteristik, yaitu:

1) Forum tersebut diinisiasi atau dilaksanakan oleh lembaga publik maupun aktor-aktor dalam lembaga publik.

2) Peserta di dalam forum tersebut juga termasuk aktor non-publik.

3) Peserta terlibat secara langsung dalam pembuatan dan pengambilan keputusan dan keputusan tidak harus merujuk kepada aktor-aktor publik.

4) Forum terorganisir secara formal dan pertemuan diadakan secara bersama-sama.

5) Forum bertujuan untuk membuat keputusan atas kesepakatan bersama, dengan kata lain forum ini berorientasi pada konsensus.

6) Kolaborasi berfokus pada kebijakan publik maupun manajemen publik.

Edward DeSeve (2007) dalam Sudarmo (2011) mendefenisikan *collaborative governance* adalah sebagai berikut:

Koleksi Perpustakaan Universitas Terbuka

"*An integrted system og relationships that is managed across formal and informal organizational boundaries with reconginezed organizational principles and clear defenition of success*". (Sebuah sistem yang terintegrasi dengan hubungan yang dikelola melintasi batas-batas organisasi formal dan informal dengan prinsip-prinsip organisasi yang direkonsepsi dan definisi kesuksesan yang jelas).

Selanjutnya Agrawal dan Lemos dalam Subarsono (2016:176) mendefinisikan *collaborative governance* tidak hanya berbatas pada *stakeholder* yang terdiri dari pemerintah dan non pemerintah tetapi juga terbentuk atas adanya *multipartner governance* yang meliputi sektor privat/swsta, masyarakat dan komunitas sipil dan terbangun atas sinergi peran *stakeholder* dan penyusunan rencana yang bersifat *hybrid* seperti halnya kerjasama publik-privat-sosial. Sejalan dengan itu Balogh dkk dalam Subarsono (2016: 176) mendefinisikan *collaborative governance* sebagai:

"*The processes and struktures of public policy decision making and mangement that engage people constructively across the boudaries of public agencies, levels of government, and or the public,privat and civic spheres in the order to carry out a public purposethet could not otherwoise be accomplished*". (Sebuah proses dan struktur dalam manajemen dan perumusan keputusan kebijakan publik yang melibatkan aktor-aktor yang secara konstruktif berasal dari berbagai level, baik dalam tatanan pemerintahan dan atau instansi publik, instansi swasta, dan masyarakat sipil dalam rangka mencapai tujuan publik yang tidak dapat dicapai apabila dilaksanakan oleh satu pihak saja).

Koleksi Perpustakaan Universitas Terbuka

Robertson dan Choi (2010: 10) mendefinisikan *collaborative governance* sebagai proses kolektif dan egalitarian dimana setiap partisipan didalamnya memiliki otoritas dalam pengambilan keputusan dan setiap *stakeholder* memiliki kesempatan yang sama untuk merefleksikan aspirasinya dalam proses tersebut.

b. Manfaat dan motivasi *collaborative governance.*

Rasionalitas dari penggunaan kemitraan antara pemerintah dengan swasta dalam penyelenggaraan tugas-tugas pemerintah menurut Slesky dan Parker dalam Dwiyanto (2011: 270-284) dibagi kedalam tiga *platform*, yaitu: *Platform* pertama, ketergantungan pada sumberdaya, isu sosial, dan pengotakan sektor. Pada dasarnya hal yang mendorong institusi memutuskan melakukan kolaborasi adalah keterbatasan akses sumberdaya yang memadai untuk menjawab permasalah publik. Dengan mengembangkan kemitraan, institusi pemerintah akan mendapatkan dukungan sumberdaya dari sektor bisnis ataupun masyarakat sipil yang menjadi mitranya untuk memenuhi kebutuhan dan kepentingan publik.

Platform kedua yang mendorong munculnya kemitraan adalah kepedulian mereka terhadap isu-isu sosial yang menjadi perhatian mereka bersama. Munculnya isu-isu tertentu, seperti kemiskinan, kerusakan lingkungan, dan

Koleksi Perpustakaan Universitas Terbuka

konflik sosial, yang dirasakan mengganggu kepentingan mereka bersama dapat mendorong mereka untuk berkolaborasi dalam mengatasinya. Menguatnya tradisi *corporate social responsibility* (CSR) dalam banyak korporasi mendorong mereka untuk berkolaborasi dengan pemrintah dan masyarakat sipil dalam rangka mengatasi masalah dan isu sosial yang cendrung semakin kompleks.

Platform ketiga, disebut sebagai *social sector platform*, menjelaskan bahwa kecendrungan semakin kaburnya ciri-ciri institusi pemerintah, masyarakat sipil, dan korporasi membuat perbedaan diantara ketiganya menjadi semakin tidak jelas. Hal ini terjadi karena apa yang sebelumnya merupakan peran sebuah institusi tertentu ternyata sekarang juga sering dimainkan oleh institusi di sektor lainnya. Ketika pemerintah mengontrakkan salah satu fungsinya dalam memberikan pelayanan publik kepada sektor swasta atau masyarakat sipil maka perbedaan peran antar ketiganya akan semakin kabur.

Disamping pendapat Slesky dan Parker, Gazley dan Brudney dalam Dwiyanto (2011: 275-281) menjelaskan tentang manfaat kolaborasi yaitu para eksekutif pemerintah dapat melakukan penghematan biaya penyelenggaraan dalam pelayanan publik, mengurangi kompetisi memperebutkan sumberdaya, dan menigkatkan akses

Koleksi Perpustakaan Universitas Terbuka

terhadap relawan dan sumberdaya lainnya. Selanjutnya temuan Gazley dan Brudney adalah 65 persen eksekutif dari kelompok masyarakat sipil mengatakan bahwa melalui kemitraan mereka dapat menghemat pengeluaran dalam penyelenggaraan layanan. Kemitraan juga dapat menigkatkan kepercayaan diantara institusi yang bermitra. Para eksekutif di sektor publik yang terlibat dalam kemitraan pada umumnya merasa bahwa kepercayaan terhadap mitranya dari masyarakat sipil menjadi semakin tinggi setelah mereka berkolaborasi. Nilai-nilai dan kepercayaan bersama dapat menjadi sumber motivasi mereka untuk menyelenggarakan barang dan jasa. Selanjutnya kemitraan juga dapat mengubah sikap para aktor dan personel dari institusi yang bermitra untuk menjadi lebih terbuka dan bersahabat. Kerjasama juga akan mendorong adanya pertukaran nilai, tradisi, dan keahlian antara birokrasi pemerintah dan lembaga non-pemerintah.

Terdapat sejumlah literatur yang menjelaskan apa yang mendorong inovasi untuk dilakukan. McGuire dalam Sudarmo (2015: 205) mengatakan alasan dilakukannya kolaborasi adalah:

1) Perubahan dalam hal ketersediaannya sumber informasi mendorong perlunya struktur-struktur yang lebih adaptif dan mengalir dan sehingga

Koleksi Perpustakaan Universitas Terbuka

memungkinkan orang-orang untuk lebih mudah bekerja melalui lintas batas organisasi.

2) Sifat masalah yang kompleks seperti lingkungan, kemiskinan, perawatan kesehatan, bencana alam yang tidak bisa ditangani secara efektif melalui birokrasi tradisional.

3) Harapan warga negara untuk memiliki banyak pilihan tersedia.

Selanjutnya Eppel dalam Sudarmo (2015: 205) menjelaskan hasil penelitiannya tentang alasan dilakukannya kolaborasi, dimana ada empat alasan, yaitu:

1) Kebutuhan untuk melibatkan komunitas dalam keputusan-keputusan yang berdampak kepada mereka.

2) Kebutuhan untuk memperoleh legitimasi dan nilai efektivitas.

3) Secara sosial sifat masalah yang dipecahkan sangat kompleks.

4) Keterbatasan informasi dan sumberdaya yang diperlukan dari masing-masing organisasi.

c. Kendala *collaborative governance.*

Loffler dalam Dwiyanto (2011: 282) mengidentifikasi beberapa resiko dan kendala dari kemitraan pemerintah dan swasta, diantaranya yaitu

Koleksi Perpustakaan Universitas Terbuka

kecenderungan kemitraan menciptakan fragmentasi struktur dan proses pelayanan publik yang dapat berpotensi menimbulkan masalah akuntabilitas. Ketika kemitraan dilaksanakan maka institusi pemerintah akan menyerahkan sebagian otoritasnya kepada mitranya dari masyarakat sipil atau korporasi, begitu juga dengan yang dilakukan oleh institusi mitra lainnya. Pertanyaan yang kemudian muncul adalah siapa yang harus mempertanggungjawabkan penyelenggaraan pelayanan ketika kegiatan-kegiatan penyelenggaraan tersebut dibagi ke dalam berbagai institusi yang otonom? Ketidakjelasan dalam hal pertanggungjawaban akan menimbulkan masalah baru dalam *governance*.

Selanjutnya kendala yang mungkin terjadi ketika mengenalkan kemitraan adalah munculnya kekhawatiran dari pada politisi dan elite yang merasa akan kehilangan kekuasaan untuk mengontrol pengambilan kebijakan dan manajemen pelayanan (Bovaird dalam Dwiyanto 2011: 283). Di sisi lain, tepatnya kalangan warga sebagai pengguna pelayanan tentang kemungkinan kemitraan membuat pelayanan pubik lebih banyak didorong oleh etos mencari keuntungan daripada etos pelayanan. Ketika institusi pemerintah berkolaborasi dengan institusi non-pemerintah dalam penyelenggaraan layanan, terutama

Koleksi Perpustakaan Universitas Terbuka

dengan korporasi, maka kekhawatiran adanya pergeseran orientasi pelayanan publik menjadi *profit oriented* tidak terhindarkan. Kendala lainnya dapat muncul dari miskonsepsi yang sering terjadi dalam hubungan antara pemerintah dengan masyarakat sipil.

Salah satu *studi* di Kanada tahun 2008 dalam Sudarmo (2011: 117) terhambatnya jalannya suatu kolaborasi (dan juga partisipsai) adalah juga disebabkan oleh banyak faktor, terutama faktor budaya, faktor institusi, dan faktor politik. Terkait dengan faktor budaya bahwa kolaborasi bisa gagal karena adanya kecenderungan budaya ketergantungan pada prosedur dan tidak berani mangambil terobosan dan resiko. Untuk terciptanya kolaborasi yang efektif mensyaratkan para pelayan publik untuk memiliki *skills* dan kesediaan untuk masuk ke kemitraan secara pragmatik, yakni berorientasi pada hasil. Dengan kata lain, ketergantungan pada prosedur dan tidak berani mengambil resiko merupakan salah satu hambatan bagi terselenggaranya efektivitas kolaborasi.

Terkait dengan faktor institusi, kolaborasi bisa gagal karena adanya kecenderungan institusi-institusi yang terlibat dalam kerjasama atau kolaborasi (terutama dari pihak pemerintah) cenderung menerapkan struktur yang hirarkis terhadap institusi-institusi lain yang ikut terlibat

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

dalam kerjasama atau kolaborasi tersebut. Institusi yang masih terlalu ketat mengadopsi struktur vertikal, yang dengan demikian akuntabilitas institusi dan arah kebijakan juga vertikal, tidak cocok dengan kolaborasi karena kolaborasi mensyaratkan cara-cara kerja atau pengorganisasian secara horizontal antara pemerintah dengan non pemrintah. Bahkan betapapun pemerintah mengadopsi sistem pemerintahan demokrasi yang biasanya bersifat *representative democracy* belum tentu cocok bagi kolaborasi karena demokrasi seperti ini mensyaratkan tingkat proses dan derajat formalisme yang begitu besar dibandingkan dengan kemitraan horizontal.

Selanjutnya pada sisi politik, kolaborasi bisa gagal karena kurangnya inovasi pemimpin dalam mencapai tujuan-tujuan politik yang kompleks dan kontradiktif. Kepemimpinan yang inovatif (*forward-looking*) adalah pemimpin yang bisa memperkenalkan berbagai macam nilai- nilai dan tujuan politis yang bisa menjadikan sebagai inti pemerintahan yang kolaboratif, dan memberikan inspirasi terhadap agenda yang ditentukan tetapi bisa mengarahkan pada pencapaian hasil- hasil yang positif melalui kemitraan (Goverment of Canada 2008 dalam Sudarmo 2011: 120)

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

d. Prinsip *collaborative governance*.

Memulai sebuah kerjasama dalam bentuk kemitraan dibutuhkan panduan dan landasan berupa prinsip agar seluruh pihak memahami tanggung jawab dan perannya masing-masing. Adapun prinsip kolaborasi atau kemitraan Suharyanto dalam Subarsono (2016: 185-186) yaitu:

1) Keserasian dan keterpaduan antara kebijkaan fiskal dan moneter.

Keserasian dapat mendorong peningkatan efisien, produktifitas, stabilitas, pemerataan alokasi, dan pemanfaatan sumberdaya ekonomi. Dengan kebijkan fiskal dan moneter yang tepat maka dapat mensukseskan agenda pemberdayaan, pemerataan, dan pertumbuhan ilmu pengetahuan dan teknologi, termasuk sistem manajemen modern seiring dengan peningkatan sumberdaya manusia dan kesejahteraan masyarakat, pengentasan kemiskinan serta untuk mengatasi kesenjangan dalam berbagai aspek. Dalam setiap aspek dan perkembangannya perlu adanya evaluasi dan pembelajaran yang bisa dikembangkan.

2) Pemberdayaan.

Kelompok masyarakat tidak sedikit yang memiliki potensi atas kemampuan yang dimiliki.

Koleksi Perpustakaan Universitas Terbuka

Namun terhalang pada keterbatasan modal, pemasaran, dan teknologi. Kelemahan tersebut harus diakui dan diubah dengan adanya program pemberdayaan oleh pemerintah dan pihak swasta, sehingga masyarakat dapat berperan dan berkontribusi secara luas dalam proses perencanaan, pelaksanaan, dan pengawasan pembangunan. Dalam kegiatan pemberdayaan masyarakat, pemerintah dapar berperan melalui:

a) Pengurangan hambatan dan kendala partisipasi masyarakat.

b) Menyusun program yang lebih memberi kesempatan kepada masyarakat untuk belajar dan berperan aktif dalam pemanfaatkan dan mendayagunakan sumberdaya produktif yang tersedia guna memenuhi kebutuhan.

e. Ukuran keberhasilan kolaborasi.

DeSeve (2007:50) dalam Sudarmo (2011:110-116) menyebutkan bahwa terdapat item penting yang bisa dijadikan untuk mengukur keberhasilan sebuah *network* atau kolaborasi dalam *governance*, yang meliputi:

1) *Networked strucuture type* (jenis struktur jaringan) menjelaskan tentang deskripsi konseptual suatu keterkaitan antara elemen yang satu dengan elemen

Koleksi Perpustakaan Universitas Terbuka

yang lain yang menyatu secara bersama-sama yang mencerminkan unsur-unsur fisik dari jaringan yang ditangani.

2) *Commitment to a common purpose* (komitmen terhadap tujuan). *Commitment to common purpose* mengacu pada alasan mengapa sebuah jaringan harus ada. Alasan mengapa sebuah *network* harus ada adalah karena perhatian dan komitmen untuk mencapai tujuan-tujuan positif. Tujuan-tujuan ini biasanya terartikulasikan di dalam misi umum suatu organisasi pemerintah.

3) *Trust among the participants* (adanya saling percaya di antara para pelaku/peserta yang terangkai dalam jaringan). Hal ini didasarkan pada hubungan profesional atau sosial keyakinan bahwa para partisipan mempercayakan pada informasi-informasi atau usaha-usaha dari *stakeholder* lainnya dalam suatu jaringan untuk mencapai tujuan bersama.

4) Adanya kepastian *governance* atau kejelasan dalam tata kelola. Hal ini termasuk:

   a) *Boundary and exlusivity*, yang menegaskan siapa yang termasuk anggota dan siapa yang bukan termasuk anggota, ini berarti bahwa

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

jika sebuah kolaborasi dilakukan, harus ada kejelasan siapa saja yang termasuk dalam jaringan dan siapa yang diluar jaringan.

b) *Rules* (aturan-aturan) yang menegaskan sejumlah pembatasan-pembatasan perilaku anggota komunitas dengan ancaman bahwa mereka akan dikeluarkan jika perilaku mereka menyimpang (tidak sesuai atau bertentangan dengan kesepakatan yang telah disetujui bersama), dengan demikian ada aturan main yang jelas tentang apa yang seharusnya dilakukan, apa yang seharusnya tidak dilakukan, ada ketegasan apa yang dinilai menyimpang dan apa yang dipandang masih dalam batas-batas kesepakatan. Hal ini menegaskan bahwa dalam kolaborasi ada aturan main yang disepakati bersama oleh seluruh *stakeholder* yang menjadi anggota dari jaringan tersebut, hal-hal apa saja yang harus dilakukan dan hal-hal apa saja yang seharusnya tidak dilakukan sesuai aturan main yang disepakati.

c) *Self determination*, yakni kebebasan untuk menentukan bagaimana *network* akan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

dijalankan dan siapa saja yang diijinkan untuk menjalankannya. Hal ini berarti bahwa model kolaborasi yang dibentuk akan menentukan bagaimana cara kolaborasi ini berjalan. Dengan kata lain cara kerja sebuah kolaborasi ikut ditentukan oleh model kolaborasi yang diadopsi.

d) *Network management* yakni berkenaan dengan resolusi penolakan/tantangan, alokasi sumberdaya, kontrol kualitas dan pemeliharaan organisasi. Ini untuk menegaskan bahwa ciri sebuah kolaborasi yang efektif adalah jika kolaborasi itu didukung sepenuhnya oleh semua anggota *network* tanpa konflik dan pertentangan dalam pencapaian tujuan, ketersediaan sumberdaya manusia yang memiliki kompetensi yang memenuhi persyaratan yang diperlukan dan ketersediaan sumber keuangan/kondisi finansial secara memadai dan berkesinambungan, terdapat penilaian kinerja terhadap masing-masing anggota yang berkolaborasi, dan tetap mempertahankan eksistensi masing-masing

Koleksi Perpustakaan Universitas Terbuka

anggota organisasi untuk tetap adaptif dan berjalan secara berkesinambungan sesuai dengan visi dan misinya masing-masing tanpa mengganggu kolaborasi itu sendiri.

5) *Access to authority* (Akses terhadap Kekuasaan) yaitu tersedianya standar-standar (ukuran-ukuran) ketentuan prosedur-prosedur yang jelas yang diterima secara luas. Bagi kebanyakan *network*, *network* tersebut harus memberi kesan kepada salah satu anggota *network* untuk memberikan otoritas guna mengimplementasikan keputusan-keputusan atau menjalankan pekerjaannya.

6) *Distributive accountability / responsibility* (pembagian akuntabilitas / responsibilitas), yaitu berbagi *governance* (penataan, pengelolaan, manajemen secara bersama-sama dengan *stakeholder* lainya) dan berbagi sejumlah pembuatan keputusan kepada seluruh anggota jaringan dan dengan demikian berbagi tanggung jawab untuk mencapai hasil yang diinginkan. Jika para anggota tidak terlibat dalam menentukan tujuan *network* dan tidak berkeinginan membawa sumberdaya dan otoritas ke dalam *network*, maka kemungkinan *network* itu akan gagal mencapai tujuan.

Koleksi Perpustakaan Universitas Terbuka

7) *Information sharing* (berbagi informasi), yaitu kemudahan akses bagi para anggota, perlindungan privasi (kerahasiaan identitas pribadi seseorang) dan keterbatasan akses bagi yang bukan anggota sepanjang bisa diterima oleh semua pihak. Kemudahan akses ini bisa mencakup sistem, *software* dan prosedur yang mudah dan aman untuk mengakses informasi.

8) *Access to resources* (akses terhadap sumberdaya), yaitu ketersediaan sumber keuangan, teknis, manusia dan sumberdaya lainnya yang diperlukan untuk mencapai tujuan *network*.

4. *Cosmopolitan governance*

a. Definisi *cosmopolitan governance*.

Cosmopolitan adalah pengertian manusia dan semua unsur dunia merupakan satu kesatuan yang memiliki pengetahuan atau wawasan yang luas. Sementara itu, menurut Colin Wight, kosmopolitanisme merupakan sebuah doktrin yang percaya bahwa kesetiaan politik kedaerahan harus dihilangkan demi identifikasi etik yang lebih tinggi dengan kemanusiaan dan masyarakat internasional harus dikorbankan dalam prosesnya. Salah satu alasan utama kemunculan kosmopolitanisme dalam dunia internasional adalah akibat meningkatnya kesadaran antar negara dalam

Koleksi Perpustakaan Universitas Terbuka

berbagai isu atau masalah internasional yang tidak dapat mereka selesaikan sendiri, meskipun itu adalah bagian dari agenda politik internasional mereka. Misalnya saja masalah kemanusiaan, kejahatan transnasional, dan lingkungan. Selain itu, munculnya individu-individu atau tingkatan non-state yang memiliki kelebihan daripada negara dalam menghadapi berbagai persoalan dunia internasional ikut menguatkan kehadiran kelompok *cosmopolist*. Mengingat bahwa individu tidak perlu memiliki sikap atau formalitas yang dimiliki oleh negara, membuat mereka bisa lebih cepat dan reaksioner dalam sebuah isu atau wacana. Selain itu, adanya beberapa aktor yang memang telah memiliki kedekatan dalam masalah tersebut, baik melalui orang atau jaringan, tempat dan waktu, atau kebudayaan yang ikut mendukung kesiapan mereka dibandingkan dengan negara.

Bagi beberapa ahli teori, kosmopolitanism mengacu kepada kemungkinan-kemungkinan yang melingkupi demokrasi global dan masyarakat dunia atau sebuah kerangka kerja bagi kerjasama antara gerakan sosial antar bangsa. Dengan meningkatnya publikasi mengenai kosmopolitanisme, juga ikut terbuka tiga cara untuk memahami dan mempelajari lebih jauh apa yang dimaksud kosmopolitanisme. Tiga cara itu adalah:

Koleksi Perpustakaan Universitas Terbuka

1) Kosmopolitanisme mengacu kepada kondisi sosiokultural sesuai dengan tujuan sebuah dunia kosmopolitan. Seiring jalan, semakin banyak manusia yang akan melakukan perjalanan jauh yang melintasi batas negara, politik dan budaya, yang berarti mereka akan merasakan berbagai macam makanan, adat, busana, dll. Namun demikian, paham ini hanya membatasi lingkupannya kepada kelompok elit yang memiliki kemampuan untuk melakukannya, misalnya saja orang-orang kaya, akademisi, ilmuwan, atlet, dan semua tipe manusia seperti ini yang tidak terikat dalam kepentingan politik tertentu. Jadi kosmopolitanisme adalah masalah konsumerisme, bagaimana seorang elit memiliki kekayaan dibanding yang lainnya dan menggunakannya untuk menuju berbagai tempat di dunia.

2) Kosmopolitanisme mengacu kepada ideologi dan filosofi. Dalam hal ini, filsuf politik kontemporer mencoba membagi dan memasukkan diri mereka sebagai komunitarian, yaitu mereka yang percaya bahwa prinsip moral dan tanggungjawab harus ditempatkan terpisah dan terkotak-terkotak dan juga secara konstektual, dan *cosmopolitan*, yaitu mereka

Koleksi Perpustakaan Universitas Terbuka

yang melihat diri mereka sebagai bagian dari masyarakat dunia, lalu berusaha menciptakan sebuah lingkungan beradab dengan pengakuan segala hak azasi manusia secara ideal.

3) Kosmopolitanisme adalah sebuah proyek politik bagi aturan baru struktur politik transnasional yang disebut juga sebagai *cosmopolitan democracy*. Konsep ini berusaha menciptakan *global governance* yang memiliki kemampuan dalam membatasi kedaulatan negara. Sehingga pada akhirnya kekuasaan sebuah negara dalam beberapa sektor akan dapat dicampuri oleh kehadiran para *cosmopolitan* ini. dua wilayah yang telah menjadi lokasi potensial untuk menciptakan kondisi ini adalah Amerika Serikat dan Uni Eropa.

Hingga saat ini dalam beberapa konsep, kosmopolitanisme masih menjadi sebuah hal yang abstrak. Beberapa ahli yang meneliti dan mengkaji kosmopolitanisme antara lain Martha Nussbaum yang sedang mengkaji visi yang lebih detail tentang pendidikan kosmopolitan, kemudian David Held yang mempelajari demokrasi kosmopolitan. la bahkan mampu membagi kosmopolitanisme menjadi tiga tipe, yaitu: politik, legal, dan liberal. David Held bertujuan untuk mengkaji lebih

Koleksi Perpustakaan Universitas Terbuka

dalam mengenai tugas, prerogatif institusional, hak moral, dan faktor politik etis para kosmopolitan yang bertujuan menciptakan tatanan konstitusional dunia baru.

b. Konsep *cosmopolitan governance*.

Munculnya aktor-aktor baru dalam hubungan internasional menggeser kekuasaan yang dimiliki negara atau *states*. Negara semakin kehilangan perannya dalam mengendalikan kekuatan pasar. Hal ini berpengaruh kuat terhadap perubahan tatanan politik global. Dalam kondisi seperti ini dibutuhkan sebuah aturan baru untuk menampung dan mengatur aktivitas para aktor baru tersebut. Kebutuhan untuk menciptakan sebuah tatanan atau mekanisme yang menjalankan fungsi yang ekuivalen dengan pemerintah menjadi sangat besar. Konsep *cosmopolitan governance* menjadi gagasan untuk menjawab kebutuhan tersebut. Para ahli hubungan internasional melihat gagasan ini sebagai jawaban yang lebih efektif dalam menyelesaikan masalah.

Rosenau dan Czempiel mengungkapkan konsep *cosmopolitan global governance* sebagi *governance without government*. Pandangan ini merujuk pada tatanan atau aturan- aturan global tanpa adanya susunan hierarki sebagaimana yang terdapat dalam sebuah institusi formal. Akan tetapi konsep tersebut masih dilihat sebagai hal yang

Koleksi Perpustakaan Universitas Terbuka

bias dan masih diperdebatkan. Oleh *The Comission on Global Government* mendefinisikannya sebagai:

"...the sum of the many ways individuals and institutions, public and private, manage their common affairs. ...Governance has been viewed primarily as intergovernmental relationships, but it must now be understood as also involving non- governmental organizations, citizens' movements, multinational corporations, and the global capital market. ... It is continuing process through which conflicting or diverse interests may be accommodated and co-operative action may be taken (1995: 2)".

Leon Gordenker dan Thomas Weiss memberikan definisi *cosmopolitan/global governance* sebagai "...efforts to bring more orderly and reliably responses to social and political issues that go beyond capacities of states to address individually' (1996: 17)".

Argumen ini mengungkapkan bahwa *cosmopolitan/global governance* lebih mengacu pada individu dalam merespon isu-isu sosial dan politik. Individu secara moral memiliki nilai-nilai dan hak-hak yang tidak terikat atau diberikan oleh intitusi manapun. Nilai-nilai moral ini yang dijadikan landasan dalam *cosmopolitan/global governance*. Dalam proyek normatif, *cosmopolitan/global governance* mengindikasikan adanya tujuan bersama yang bersifat lintas negara dan ditujukan untuk kebaikan individu- individu, bukan negara. *cosmopolitan/global governance* menghendaki sebuah tatanan atas perilaku- perilaku aktor dalam hubungan internasional melalui penerapan norma-norma yang diterima secara global.

Koleksi Perpustakaan Universitas Terbuka

Berangkat dari paparan di atas, *cosmopolitan/global governance* dapat didefinisikan sebagai sebuah struktur regulasi yang dapat berupa organisasi atau sebuah tatanan yang dibentuk dengan kesepakatan, yang diberi kewenangan untuk mengkoordinasikan tiap aktor, mengontrol dan memiliki otoritas penuh atas bidang yang disepakati dan melaksanakan kebijakan. Dapat dikatakan juga sebagai regulasi yang mengatur hubungan inter-dependen dalam ketiadaan otoritas dominan. Ada pula yang mengatakan 'administrasi yang mengontrol proses global dalam ketiadaan pemerintahan global atau tindakan bersama untuk mengidentifikasi, memahami, masalah dunia yang pemecahannya membutuhkan kapabilitas yang melebihi kapasitas individu atau negara.

Cosmopolitan/global governance mendasarkan asumsinya bahwa semua aktor baik negara maupun non-negara termasuk di dalamnya individu harus terakomodasi dalam penciptaan norma-norma internasional. Semua warga dunia tanpa kecuali harus diikutsertakan dalam penciptaan suatu tatanan yang berlaku dan sesuai untuk semua. Konsep yang demikian ini sangat sesuai dengan *cosmopolitan*. Pengambilan keputusan berdasarkan pemikiran *cosmopolitan* tidak perlu mempertimbangkan perhitungan *cost and benefit* namun lebih melihat pada

Koleksi Perpustakaan Universitas Terbuka

nilai-nilai moral yang dimiliki manusia karena tujuannya adalah menjamin kepentingan individu bukan negara.

Prinsip *cosmopolitan/global governance* adalah bahwa di dalam dunia dengan hubungan regional dan global yang makin intensif, ditandai dengan "takdir komunitas" yang tumpang tindih, prinsip otonomi memerlukan pertahanan jaringan regional, global, nasional dan juga pemerintahan lokal.

Secara jangka pendek dalam konteks pemerintah, *cosmopolitan/global governance* dicirikan sebagai berikut:

1) Mempersatukan kembali institusi pemerintah PBB seperti Dewan Keamanan guna memberikan negara-negara berkembang suatu suara yang penting dan kapasitas pengambilan keputusan yang efektif.
2) Pembentukan Dewan Keamanan PBB yang kedua mengikuti konvensi undang-undang internasional.
3) Meningkatkan politik regional (Masyarakat Uni Eropa dan lainnya) dan penggunaan referendum antar bangsa.
4) Pembentukan suatu pengadilan internasional hak asasi manusia yang baru yang bertanggungjawab secara yuridis terhadap pengadilan internasional.
5) Menertibkan kekuatan militer internasional yang efektif dan bertanggungjawab.

Koleksi Perpustakaan Universitas Terbuka

Secara jangka panjang dalam konteks pemerintah, *cosmopolitan global governance* dicirikan sebagai berikut:

1) Piagam hak dan kewajiban yang baru dan sesuai dengan perbedaan kekuatan di bidang politik, sosial dan ekonomi.
2) Parlemen yang bersifat global (dengan pembatasan kapasitas peningkatan pendapatan) berhubungan dengan daerah, bangsa dan lokal.
3) Pemisahan kepentingan politik dan ekonomi, kumpulan pembiayaan publik dan proses pemilihan.
4) Sistem hukum global yang saling berhubungan yang mencakup hukum sipil dan kriminal.
5) Peralihan secara tetap wewenang dan kapasitas negara-bangsa kepada institusi regional dan global.

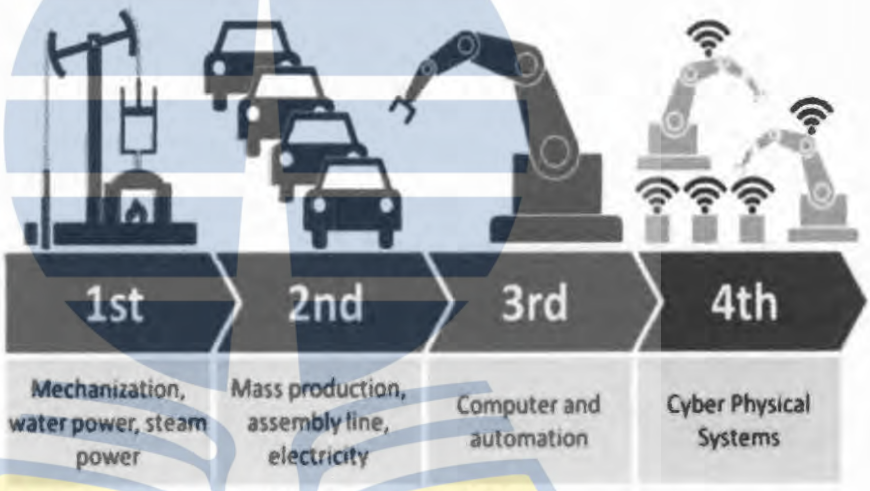
5. Revolusi Industri 4.0

a. Definisi Revolusi Industri 4.0.

Pada awalnya, istilah Revolusi Industri 4.0 berasal dari sebuah proyek strategis teknologi canggih Pemerintah Jerman yang mengutamakan komputerisasi pada semua pabrik di negeri itu. Saat ini, Revolusi Industri 4.0 adalah nama tren otomasi dan pertukaran data terkini dalam teknologi pabrik. Istilah ini mencakup sistem siber-fisik, internet untuk segala, komputasi awan, dan komputasi kognitif. Revolusi Industri 4.0 menghasilkan "pabrik

Koleksi Perpustakaan Universitas Terbuka

cerdas". Di dalam pabrik cerdas berstruktur moduler, sistem siber-fisik mengawasi proses fisik, menciptakan salinan dunia fisik secara *virtual*, dan membuat keputusan yang tidak terpusat. Melalui Internet untuk segala (*IoT*), sistem siber-fisik berkomunikasi dan bekerja sama dengan satu sama lain dan manusia secara bersamaan serta pada akhirnya dapat dimanfaatkan dengan menggunakan komputasi awan, layanan internal dan lintas organisasi yang disediakan.



Sumber : www.serambinews.com, 2018

Gambar 2.1
Perkembangan Revolusi Industri

Pada bulan April 2013, Prof Krugman mencatat beberapa hal tentang perkembangan revolusi industri yang terjadi sejak abad ke-17:

1) Revolusi Industri Pertama (1750-1830), ditandai dengan penemuan mesin uap dan kereta api. Penggunaan mesin uap pada waktu itu dimaksudkan

Koleksi Perpustakaan Universitas Terbuka

untuk menggantikan tenaga manusia dan hewan dalam produksi. Revoluasi industri ini pada saat itu juga berguna untuk melaksanakan mekanisasi sistem produksi. Mekanisasi di sini bermakna penggunaan tenaga mesin dan sarana-sarana teknik lainnya untuk menggunakan tenaga manusia dan hewan dalam proses produksi.

2) Revolusi Industri Kedua (1870-1900), ditandai dengan penemuan listrik, alat komunikasi, bahan-bahan kimia, dan minyak. Revolusi industri pada tahap ini dapat digunakan untuk melaksanakan konsep produksi massal.

3) Revolusi Industri Ketiga (1960 hingga sekarang), ditandai dengan penemuan komputer, internet, dan telepon genggam. Revolusi industri ketiga ini dapat digunakan untuk otomatisasi proses produksi dalam kegiatan industri.

4) Saat ini kita memasuki era baru, yaitu Revolusi Industri Keempat atau sering disebut dengan istilah populer Revolusi Industri 4.0. Revolusi industri gelombang keempat ini tetap bertopang pada Revolusi Industri Ketiga. Namun, Revoluasi Industri 4.0 mulai ditandai dengan bersatunya beberapa teknologi, sehingga kita melihat dan merasakan

Koleksi Perpustakaan Universitas Terbuka

suatu era baru yang terdiri atas tiga bidang ilmu yang independen, yaitu fisika, *digital*, dan biologi.

Dengan komposisi yang demikian, maka Revolusi Industri 4.0 mempunyai potensi memberdayakan individu dan masyarakat, karena revolusi industri fase ini dapat menciptakan peluang baru bagi ekonomi, sosial, maupun pengembangan diri pribadi. Tetapi Revolusi Industri 4.0 juga bisa menyebabkan pengerdilan dan marginalisasi (peminggiran) beberapa kelompok dan ini dapat memperburuk kepentingan sosial bahkan kohesi sosial, juga dapat menciptakan resiko keamanan dan dapat pula merusak interelasi (hubungan) antarmanusia. Kombinasi antara pertumbuhan ekonomi yang tidak bertambah dengan cepat dan menurunnya peran manufaktur, menyisakan pertanyaan tentang kehebatan Revolusi Industri 4.0. Belum lagi, misalnya, Revolusi Industri 4.0 ini masih menyisakan sisi gelapnya, yakni dampak negatifnya terhadap penciptaan lapangan kerja.

b. Prinsip rancangan dalam revolusi industri 4.0.

1) Interoperabilitas (kesesuaian).

Kemampuan mesin, perangkat, sensor, dan manusia untuk berhubungan dan berkomunikasi dengan satu sama lain lewat internet untuk segala (IoT) atau internet untuk khalayak (IoP). IoT akan

Koleksi Perpustakaan Universitas Terbuka

mengotomatisasikan proses ini secara besar-besaran.

2) Transparansi informasi.

Kemampuan sistem informasi untuk menciptakan salinan dunia fisik secara *virtual* dengan memperkaya model pabrik *digital* dengan data sensor. Prinsip ini membutuhkan pengumpulan data sensor mentah agar menghasilkan informasi konteks bernilai tinggi.

3) Bantuan teknis.

a) Kemampuan sistem bantuan untuk membantu manusia dengan mengumpulkan dan membuat visualisasi informasi secara menyeluruh agar bisa membuat keputusan bijak dan menyelesaikan masalah genting yang mendadak.

b) Kemampuan sistem siber-fisik untuk membantu manusia secara fisik dengan melakukan serangkaian tugas yang tidak menyenangkan, terlalu berat, atau tidak aman bagi manusia.

4) Keputusan mandiri.

Kemampuan sistem siber-fisik untuk membuat keputusan sendiri dan melakukan tugas

Koleksi Perpustakaan Universitas Terbuka

semandiri mungkin. Bila terjadi pengecualian, gangguan, atau ada tujuan yang berseberangan, tugas didelegasikan ke atasan.

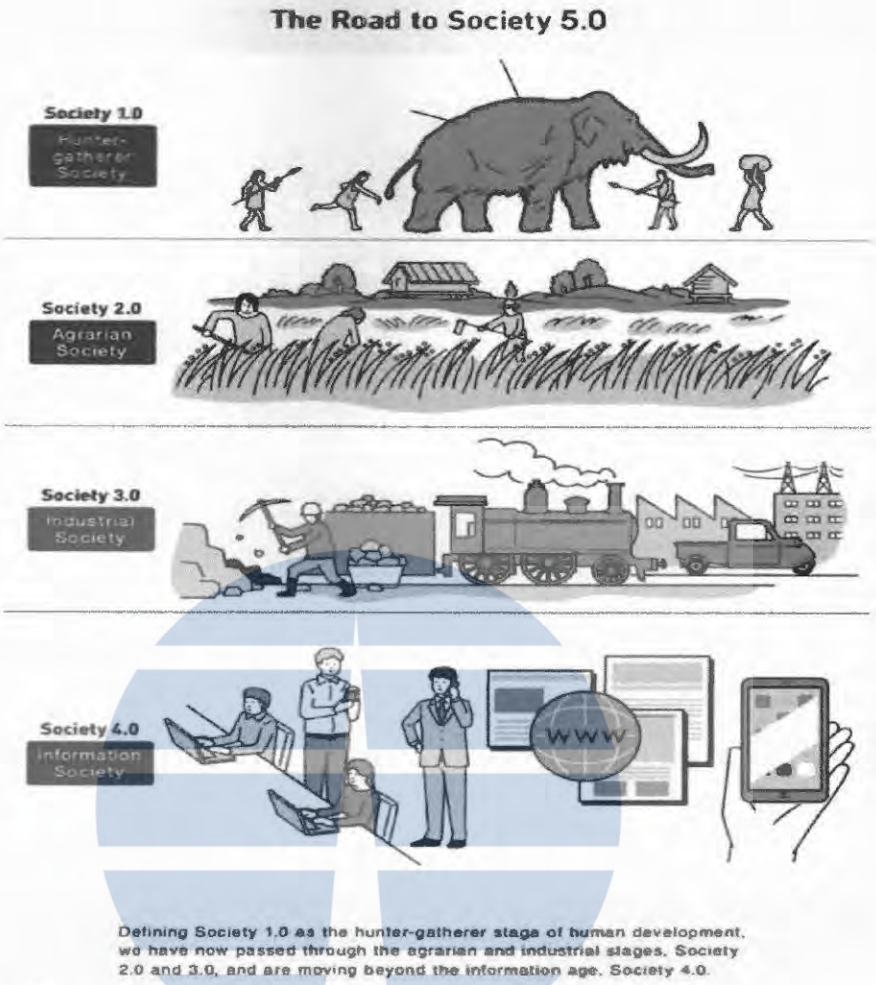
6. Masyarakat 5.0

a. Definisi Masyarakat 5.0.

Masyarakat 5.0 dimaksudkan untuk menyebut sebuah masa di mana masyarakat berpusat pada manusia yang menyeimbangkan kemajuan ekonomi dengan penyelesaian masalah sosial oleh sistem yang sangat mengintegrasikan ruang dunia maya dan ruang fisik. Konsep ini lahir sebagai pengembangan dari revolusi industri 4.0 yang dinilai berpotensi mendegradasi peran manusia. Masyarakat atau *Society* 5.0 diusulkan dalam Rencana Dasar Sains dan Teknologi ke-5 sebagai masyarakat masa depan yang ingin dicita-citakan Jepang. Sebagaimana kita ketahui, sebelumnya masyarakat pemburu digunakan untuk menyebut generasi 1.0, masyarakat pertanian digunakan untuk menyebut masyarakat 2.0, masyarakat industri digunakan untuk menyebut generasi 3.0, dan masyarakat informasi digunakan untuk menyebut generasi 4.0.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf



Sumber : www.cao.go.jp, 2018

Gambar 2.2
Tingkat Perkembangan Masyarakat Dunia

Melalui Masyarakat 5.0, kecerdasan buatan (*artificial intelligence*) akan mentransformasi *big data* yang dikumpulkan melalui internet pada segala bidang kehidupan (*the Internet of Things*) menjadi suatu kearifan baru, yang akan didedikasikan untuk meningkatkan kemampuan manusia membuka peluang-peluang bagi kemanusiaan. Transformasi ini akan membantu manusia untuk menjalani kehidupan yang lebih bermakna.

Koleksi Perpustakaan Universitas Terbuka

Masyarakat 5.0 mencapai tingkat konvergensi yang tinggi antara *cyberspace* (ruang *virtual*) dan ruang fisik (ruang nyata). Dalam masyarakat informasi masa lalu (*Society* 4.0), orang akan mengakses layanan *cloud* (*database*) di dunia maya melalui internet dan mencari, mengambil, dan menganalisis informasi atau data. Sementara itu, di Masyarakat 5.0, sejumlah besar informasi dari sensor di ruang fisik terakumulasi di dunia maya. Di dunia maya, data besar ini dianalisis oleh kecerdasan buatan atau *artificial intelligence* (AI), dan hasil analisisnya diumpankan kembali ke manusia dalam ruang fisik dalam berbagai bentuk. Di Masyarakat 4.0, praktik umum adalah mengumpulkan informasi melalui jaringan dan menganalisisnya oleh manusia. Namun, dalam Masyarakat 5.0, orang, benda, dan sistem semuanya terhubung di dunia maya dan hasil optimal yang diperoleh oleh AI melebihi kemampuan manusia diberi *feedback* ke ruang fisik. Proses ini membawa nilai baru bagi industri dan masyarakat dengan cara yang sebelumnya tidak mungkin.

Dalam menghadapi perubahan besar seperti di dunia, teknologi baru seperti IoT (*internet of things*), robotika, AI, dan data besar, yang semuanya dapat mempengaruhi jalannya masyarakat, terus mengalami kemajuan. Jepang berusaha menjadikan Masyarakat 5,0

Koleksi Perpustakaan Universitas Terbuka

sebagai sebuah masyarakat baru yang menggabungkan teknologi baru ini di semua industri dan kegiatan sosial dan mencapai perkembangan ekonomi dan solusi untuk masalah sosial secara paralel. Di Masyarakat 5.0, nilai baru yang diciptakan melalui inovasi akan menghilangkan kesenjangan regional, usia, jenis kelamin, dan bahasa dan memungkinkan penyediaan produk dan layanan yang dirancang untuk beragam kebutuhan individu dan kebutuhan umum. Dengan cara ini, akan mungkin untuk mencapai masyarakat yang dapat mempromosikan pembangunan ekonomi dan menemukan solusi untuk masalah sosial.

b. Contoh penerapan Masyarakat 5.0 (*Society* 5.0).

1) Bidang mobilitas.

Dalam Masyarakat 5.0, nilai baru dapat dihasilkan dengan cara melalui analisis AI dari *big data* dalam basis data yang mencakup beragam jenis informasi termasuk data sensor dari mobil, informasi waktu nyata mengenai cuaca, lalu lintas, akomodasi, serta makanan dan minuman, dan riwayat pribadi dengan aplikasi sebagai berikut:

a) Mudah dalam menentukan rute jalan sesuai kebutuhan dengan penyajian optimal tentang cuaca, kemacetan, dan lain-lain.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

b) Diciptakannya pengemudi otonom.

c) Adanya layanan *online* terintegrasi terkait transportasi umum, dan lain-lain.

d) Diciptakannya kursi roda otonom untuk membantu lansia dan penyandang cacat untuk bergerak sendiri.

e) Mengurangi emisi CO2 oleh transportasi publik.

2) Bidang kesehatan.

Dalam Masyarakat 5.0, nilai baru dapat dihasilkan melalui analisis AI dari *big data* yang mencakup beragam jenis informasi, termasuk data fisiologis *real-time* pribadi, informasi situs perawatan kesehatan, informasi perawatan/infeksi, dan informasi lingkungan dengan aplikasi sebagai berikut:

a) Penggunaan robot sebagai tenaga medis.

b) Pemeriksaan kesehatan otomatis secara *real-time.*

c) Memberikan perawatan optimal di mana saja melalui pembagian data fisiologis dan medis.

d) Membantu mengurangi biaya sosial yang terkait dengan perawatan kesehatan dan pengasuhan dan memecahkan masalah

Koleksi Perpustakaan Universitas Terbuka

kekurangan tenaga kerja di lokasi perawatan kesehatan.

3) Bidang industri.

Dalam Masyarakat 5.0, nilai baru dapat dihasilkan melalui analisis AI dari *big data* yang mencakup beragam jenis informasi, termasuk permintaan pelanggan dan konsumen, informasi inventaris pemasok, dan informasi pengiriman dengan aplikasi sebagai berikut:

a) Melaksanakan perencanaan produksi dan manajemen persediaan yang fleksibel.

b) Menggunakan AI dan robot dalam koordinasi antar-pabrik untuk membuat produksi lebih efisien dan hemat tenaga kerja.

c) Membuat distribusi lebih efisien dengan pengiriman kooperatif lintas industri.

d) Pengiriman barang lebih tepat waktu.

e) Membantu memperkuat daya saing industri, meningkatkan daya tanggap terhadap bencana, mengurangi masalah kekurangan tenaga kerja, menangani berbagai kebutuhan, mengurangi emisi dan pengeluaran gas rumah kaca, meningkatkan kepuasan pelanggan, dan merangsang konsumsi.

Koleksi Perpustakaan Universitas Terbuka

4) Bidang pertanian.

Dalam Masyarakat 5.0, nilai baru dapat dihasilkan melalui analisis AI dari *big data* yang terdiri dari beragam informasi, seperti data meteorologi, data pertumbuhan tanaman, kondisi pasar, dan tren dan kebutuhan makanan dengan aplikasi sebagai berikut:

a) Mengotomatisasi pekerjaan pertanian dan menghemat tenaga kerja melalui traktor robot, mengotomatisasi pengumpulan data tanaman melalui *drone*, serta mengotomatisasi dan mengoptimalkan pengelolaan air berdasarkan prediksi cuaca, data sungai, dan lain-lain.

b) Merumuskan rencana pertanian dengan menetapkan hasil panen yang disesuaikan dengan kebutuhan, mengoptimalkan rencana kerja bersama dengan prediksi cuaca, berbagi pengalaman dan pengetahuan, dan memperluas basis pelanggan.

c) Mengirim hasil pertanian ke konsumen melalui kendaraan pengiriman yang otonom.

d) Membantu meningkatkan produksi pangan dan menstabilkan pasokan, mengatasi

Koleksi Perpustakaan Universitas Terbuka

masalah kekurangan tenaga kerja di daerah pertanian, mengurangi limbah makanan, dan merangsang konsumsi.

5) Bidang pangan atau produk makanan.

Di Masyarakat 5.0, nilai baru dapat dihasilkan melalui analisis AI dari *big data* yang terdiri dari beragam informasi, seperti alergi pribadi, informasi tentang produk makanan, produk makanan yang disimpan di kulkas keluarga, inventaris toko ritel, dan kondisi pasar dengan aplikasi sebagai berikut:

a) Tersedianya produk makanan yang disesuaikan dengan informasi alergi pribadi.

b) Mengotomasikan manajemen makanan yang disimpan di lemari es.

c) Memungkinkan produsen pertanian dan toko ritel untuk mengelola produksi, pesanan, dan inventaris sesuai dengan kebutuhan pelanggan.

d) Membantu mengurangi limbah makanan dan membuat industri makanan lebih kompetitif.

6) Bidang pencegahan bencana.

Dalam Masyarakat 5.0, nilai baru dapat dihasilkan melalui analisis AI dari *big data* yang

Koleksi Perpustakaan Universitas Terbuka

terdiri dari beragam informasi, seperti pengamatan daerah yang terkena bencana oleh satelit, radar cuaca terestrial, atau oleh *drone*, informasi kerusakan berdasarkan struktural sensor, dan informasi kerusakan jalan dari mobil dengan aplikasi sebagai berrikut:

a) Menyediakan data tempat tinggal dan tempat penampungan yang aman melalui *smartphone* individu dan perangkat lain berdasarkan kondisi bencana alam.

b) Temukan korban segera melalui pakaian pembantu, robot penyelamat, dan lain-lain.

c) Melakukan pengiriman bahan bantuan secara optimal melalui *drone*, kendaraan pengiriman *self-driving*, dan lain-lain.

d) Membantu mengurangi kerusakan dan mencapai pemulihan awal.

7) Bidang energi.

Dalam Masyarakat 5.0, nilai baru dapat dihasilkan melalui analisis AI dari *big data* yang terdiri dari beragam informasi seperti data meteorologi, status operasi pembangkit listrik, status debit / muatan kendaraan listrik (EV), dan kondisi

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

penggunaan energi setiap rumah tangga dengan aplikasi sebagai berikut:

a) Menyediakan pasokan energi yang stabil melalui beragam sarana energi berdasarkan perkiraan permintaan yang akurat dan prediksi cuaca.

b) Mencapai produksi lokal untuk konsumsi lokal dengan menggunakan EV dan produksi hidrogen dan mempromosikan akomodasi antar-regional.

c) Terciptanya penghematan energi rumah tangga dengan mengoptimalkan penggunaan energi berdasarkan prediksi persediaan.

d) Membantu menyediakan pasokan energi yang stabil dan mengurangi beban lingkungan kita dengan mengurangi emisi gas rumah kaca.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Sumber : www.cao.go.jp, 2018

Gambar 2.3
Visualisasi Perubahan dalam Masyarakat 5.0

7. Kejahatan siber (*Cyber Crime)*

a. Definisi kejahatan siber.

Berdasarkan hasil penelusuran, pengertian *cyber crime* belum terdefinisi secara baku. Mengingat pengertian yang dikemukakan oleh para pakar sangat beraneka ragam, tetapi pengertian yang satu dengan yang lain saling melengkapi. Oleh karena itu, penting untuk dipaparkan pengertiannya. Secara etimologi *cyber crime* berasal dari dua rangkaian kata, yaitu *cyber* dan *crime*. Menurut Kamus Bahasa Inggris-Indonesia *cyber* berarti maya, sedangkan *crime* diartikan dengan kejahatan. Menurut *Dictionary of Contemporary English*, *crime* adalah *an offence which is punishable by law* (suatu kejahatan yang dihukum oleh

Koleksi Perpustakaan Universitas Terbuka

hukum), *illegal activity in general* (kegiatan ilegal pada umumnya), atau *a bad, immoral, or dishonourable act* (tidak terhormat, tidak bermoral, atau tindakan yang buruk). Secara kebahasaan *cyber crime* semakna dengan "kejahatan dunia maya" atau "kejahatan mayantara".

Menurut terminologi, akan dikemukakan berdasarkan pendapat para pakar sebagai berikut:

Cyber crime adalah kejahatan yang lahir sebagai dampak negatif dari perkembangan aplikasi internet. Berdasarkan pengertian tersebut terlihat bahwa *cyber crime* mencakup semua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif aplikasi internet. Definisi ini tidak menyebutkan secara spesifik dari karakteristik *cyber crime*. Definisi ini mencakup segala kejahatan yang dalam modus operandinya menggunakan fasilitas internet.

Dalam dua dokumen Kongres PBB yang dikutip oleh Barda Nawawi Arief, mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada Tahun 1990 dan di Wina Austria pada Tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian *cyber crime*, yaitu *cyber crime* dan *computer related crime*. Dalam *back ground paper* untuk lokakarya Kongres PBB X/2000 di Wina Austria, istilah *cyber crime*

Koleksi Perpustakaan Universitas Terbuka

dibagi dalam dua kategori. Pertama, *cyber crime* dalam arti sempit *(in a narrow sense)* disebut *computer crime*. Kedua, *cyber crime* dalam arti luas *(in a broader sense)* disebut *computer related crime*. Lengkapnya sebagai berikut:

1) *Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed byh them.*
2) *Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network.*
3) Pengertian komputer dalam *The Proposed West Virginia Computer Crimes Act* adalah *"an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typewriter or typesetter, a portable handheld calculator, or other similar device".*

b. Jenis-jenis kejahatan siber berdasarkan motif.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada , antara lain:

1) *Unauthorized access to computer system and service.*

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem

Koleksi Perpustakaan Universitas Terbuka

jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet.

2) *Illegal contents.*

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya.

Koleksi Perpustakaan Universitas Terbuka

3) *Data forgery.*

Merupakan kejahatan dengan memalsukan data pada dokumen dokumen penting yang tersimpan sebagai *scripless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalahgunakan.

4) *Cyber espionage.*

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system)* pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (*data base*) tersimpan dalam suatu sistem yang *computerized* (tersambung dalam jaringan komputer).

5) *Cyber sabotage and extortion.*

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan

Koleksi Perpustakaan Universitas Terbuka

komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

6) *Offense against intellectual property.*

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh, peniruan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya

7) *Infringements of privacy.*

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun non materil, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

Koleksi Perpustakaan Universitas Terbuka

c. Jenis-jenis kejahatan siber berdasarkan sasaran kejahatan.

1) Kejahatan siber yang menyerang individu (*againts person*).

Jenis kegiatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. contoh : pornografi, *cyberstalking, cyber-tresspass.*

2) Kejahatan siber menyerang hak milik (*againts property*).

Siber yang dilakukan untuk mengganggu atau menyerang hak milik orang lain. Beberapa contoh kejahatan ini misalnya pengaksesan komputer secara tidak sah melalui dunia siber, pemilikan informasi elektronik secara tidak sah/pencurian informasi, *carding, cybersquatting, hijacking, data forgery* dan lain-lain.

3) Kejahatan siber menyerang pemerintah (*againts government*).

Cyber crime againts government dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan ini misalnya *cyber terorrism* sebagai tindakan yang mengancam pemerintah

Koleksi Perpustakaan Universitas Terbuka

termasuk juga *cracking* ke situs resmi, pemerintah atau situs militer.

8. Ancaman kejahatan siber terhadap negara dan institusi militer

a. Tren ancaman.

1) *Cyberwarfare.*

Merupakan kegiatan *hacking* atau pencurian data melalui jaringan internet/komputer/dunia maya berdasarkan motivasi politik dengan tujuan sabotase atau spionase terhadap kepentingan tertentu. Sedangkan menurut Richard A. Clarke dalam bukunya *Cyber War* (Mei 2010) adalah "tindakan oleh negara/bangsa untuk menembus komputer atau jaringan bangsa lain untuk tujuan menyebabkan kerusakan atau gangguan".

2) Jaringan masyarakat atau *social networking.*

Merupakan layanan elektronik *online* yang menghubungkan masyarakat dan sekarang menjadi bagian penting dari kehidupan masyarakat, perbankan, komunikasi, media dan belanja yang semuanya berada di dunia maya. Kondisi ini menyebabkan banyak pemerintah modern sekarang menjadi tergantung pada keamanan komputer dan jaringan untuk menjaga kebutuhan masyarakat tersebut. Bahkan, *trend* terbaru menunjukkan bahwa

Koleksi Perpustakaan Universitas Terbuka

e) Modus eksploitasi pendapat masyarakat pada media sosial dengan mengambil momen isu sensitif.

Kasus yang aktual pada Tahun 2017 adalah *postingan* provokatif terhadap Panglima TNI dan Institusi TNI terkait isu senjata standar TNI yang dimiliki Polri, protes kepada Kebijakan Panglima TNI tentang HUT TNI 2017, dan elektabilitas Panglima TNI sebagai bursa Pemilu Presiden 2019.

f) Modus bagi tautan melalui media sosial.

Pengunggahan tautan alamat situs atau video dan alamat akun media sosial menjadi sarana ampuh yang menggerakkan pemakai perangkat *gadget* yang terkoneksi dengan internet. Modus ini mampu meningkatkan sentimen negatif masyarakat atas dasar substansi berita yang telah dimanipulasi.

2) Serangan terhadap infrastruktur sistem informatika.

Bentuk serangan ini mengarah kepada infrastruktur informatika yang jika tidak diberikan respon secara cepat akan berdampak kepada

Koleksi Perpustakaan Universitas Terbuka

eksistensi institusi TNI AD. Beberapa modus ancaman yang dilakukan antara lain adalah:

a) *Hacking* mengambil kontrol kendali terhadap Alat Utama Sistem Persenjataan (Alutsista).

Era teknologi telah menghubungkan setiap unit Alutsista ke jaringan internet sehingga sangat rentan terhadap pengambilan alih kendali secara sistem jarak jauh.

b) Serangan virus jahat terhadap sistem informasi.

Pengiriman program jahat terhadap sistem informasi sehingga dapat diambil alih kendalinya.

c) Perusakan fisik terhadap infrastruktur sistem informasi.

Ancaman ini merupakan bentuk aksi kekerasan nyata dan bertujuan merusak sistem informasi secara permanen.

d) Penggalangan personel pengawak sistem informasi.

Penggalangan lawan atau musuh dapat diarahkan kepada personel pengawak sistem informasi. Karenanya perlu

Koleksi Perpustakaan Universitas Terbuka

diamankan agar tidak bocor mulut terhadap setiap personel.

e) Serangan *presition guided munition* (PGM).

Teknologi PGM merupakan bentuk tandingan dari teknologi *suicied bomb* (bom bunuh diri). Teknologi ini menjadi tren kontra gerilya Amerika Serikat dan Barat melawan kelompok *Al Qaeda* di Afghanistan dan ISIS di Suriah. Namun seiring dengan perkembangan teknologi telah dikuasai oleh masyarakat sipil dan menjadi senjata presisi yang dimiliki oleh kelompok penggiat teror dalam melaksanakan aksinya.

9. Faktor penghambat peningkatan fungsi Satuan Siber TNI AD

a. Sarana dan prasarana terbatas.

Ancaman siber yang mulai menyerang institusi militer telah direspon dengan pembentukan Satuan Siber TNI dan Satuan Tugas Siber TNI AD. Saat ini tugas pokok dari kedua satuan tersebut adalah melakukan fungsi pertahanan siber dan *monitoring* aktif terhadap media sosial/*online*. Namun, dengan adanya keterbatasan sarana dan prasarana seperti piranti lunak/aplikasi, perangkat komputer anti sadap dan peralatan *tracking digital* serta lainnya menyebabkan pelaksanaan fungsi pertahanan dan

Koleksi Perpustakaan Universitas Terbuka

monitoring pun menjadi *low respond*. Sebagai contoh dalam mengungkap berita *hoax* terkait TNI AD membutuhkan waktu penelusuran yang cukup lama sampai dengan mengungkap pelakunya, sehingga akibat dari hal tersebut adalah pemberitaan telah menjadi viral sebelum dilakukan pemblokiran.

b. Sumberdaya manusia terbatas.

Pembentukan Satuan Siber TNI AD membutuhkan banyak personel berkualifikasi intelijen dan persandian serta Informasi dan Teknologi (IT) dengan tujuan agar adaptasi satuan baru tersebut dalam melaksanakan fungsinya dapat berjalan dengan cepat, namun kenyataan di lapangan rekruitmen personel TNI AD yang berkualifikasi intelijen, sandi dan menguasai IT dengan baik banyak menemui kendala. Saat ini memperoleh prajurit yang menguasai IT tingkat lanjut merupakan hal yang langka, sehingga perlu dilaksanakan pelatihan/penataran/kursus untuk membekali personel tersebut sebelum bertugas di Satuan Siber TNI AD, namun di sisi lain hal ini justru menghambat peningkatan fungsi satuan tersebut, karena proses pembekalan itu sendiri memakan waktu yang tidak sebentar.

Koleksi Perpustakaan Universitas Terbuka

c. Hukum perundang-undangan lemah.

Sebagaimana telah disinggung di atas, bahwa penerapan Undang – Undang No.11 Tahun 2008 dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam tindak pidana siber dinilai masih banyak kelemahan dan kekurangan di dalam mengatur tindak pidana siber serta menimbulkan banyak permasalahan baru. Terkait dengan semakin canggihnya modus kejahatan tindak pidana siber yang semakin berkembang pesat, para pembuat Undang-Undang dan penegak hukum belum melakukan perubahan sama sekali kualitas dan kuantitas Undang-Undang ini malah cenderung Undang-Undang ini menuai banyak pro dan kontra yang dianggap tidak dapat menurunkan tingkat kejahatan tindak pidana siber secara signifikan sehingga memunculkan tudingan bahwa Undang-Undang ini tidak berjalan secara efektif terutama dari aspek pidananya. Undang-Undang No.11 Tahun 2008 dan Undang-Undang Nomor 19 Tahun 2016 masih membutuhkan penambahan kesempurnaan khususnya tentang Procedural Law dan hal yang masih menjadi persoalan dan perlu dicarikan solusinya adalah mengenai sifat khusus dari bidang teknologi informasi, yang penanganannya harus dilakukan oleh orang

Koleksi Perpustakaan Universitas Terbuka

yang memahami teknologi informasi dan komunikasi serta perlunya pembaharuan Undang-Undang atau menerbitkan Peraturan Pemerintah yang mengakomodir sifat kekhususan dari bidang teknologi informasi dan komunikasi.

d. Birokrasi lambat.

Selain ketiga hal di atas, faktor penghambat lainnya adalah adanya jalur birokrasi yang lambat dalam mekanisme penanganan kejahatan siber yang menyerang institusi TNI AD. Saat ini, untuk penanganan berita *hoax* saja, Satuan Siber TNI AD yang telah menemukan pelaku berita *hoax* tidak dapat menangani atau menyelesaikan masalah tersebut, melainkan harus membuat laporan tertulis dan permohonan pemblokiran ke Kementerian Komunikasi dan Informasi serta Kepolisian. Masalah muncul karena mekanisme pemblokiran tidak dapat dilaksanakan dengan segera, tetapi membutuhkan waktu paling tidak selama I minggu, sehingga pemberitaan tersebut telah menjadi konsumsi publik. Langkah antisipasi awal adalah dengan melakukan *press realease* dan klarifikasi melalui akun resmi TNI AD di media sosial/*online*.

10. Kejahatan siber terhadap peningkatan fungsi Satuan Siber TNI AD

a. Analisis potensi TNI AD dalam merespon siber.

TNI AD belum memiliki institusi dalam bidang siber. Namun dalam doktrin Kartika Eka Paksi telah

Koleksi Perpustakaan Universitas Terbuka

ditetapkan adanya siber sebagai fungsi khusus dengan kemampuan *defensif* dengan memberikan perlindungan terhadap sumberdaya telematika dan melakukan serangan *ofensif* dengan teknik telematika. Jika hendak dibentuk sebuah institusi siber di lingkungan Angkatan Darat perlu diperhatikan adanya wilayah urusan yang diperdebatkan oleh beberapa Badan Pelaksana Pusat (Balakpus), sementara itu terdapat adanya urusan keluasan siber yang sama-sama belum tertangani, namun seluruh institusi sepakat untuk tidak menggarapnya. Beberapa institusi yang memiliki irisan dalam medan garapan siber adalah:

1) Komando Pasukan Khusus (Kopassus).

Kopassus telah memiliki satuan siber yang dipimpin oleh seorang Perwira Menengah (Pamen) TNI AD berpangkat Letnan Kolonel. Komposisi terdiri atas dua puluh prajurit berkemampuan pasukan khusus sehingga berpotensi dikembangkan menjadi tim penindakan siber (*ofensif*).

2) Direktorat Perhubungan Angkatan Darat (Dithubad).

Dithubad sebagai salah satu kecabangan di lingkungan TNI AD memiliki kapasitas dalam kegiatan perang elektronika. Kapasitas yang dimiliki dapat menjadi cikal bakal bagi pembentukan satuan siber yang memiliki kemampuan *ofensif*

Koleksi Perpustakaan Universitas Terbuka

sebagaimana diamanahkan oleh doktrin Kartika Eka Paksi (doktrin tertinggi di TNI Angkatan Darat). Selain alat yang dimiliki, kapasitas perwira perhubungan yang memperoleh bekal pengetahuan elektronika, komunikasi dan komputer dari prajurit terbawah sampai tingkat perwira pertama menjadi bekal dalam pembangunan satuan siber untuk kapasitas *ofensif*. Hal lain yang patut diberikan apresiasi terhadap Dithubad adalah kemampuan *ofensif* yang dapat dikembangkan untuk melakukan kegiatan peperangan siber. Karenanya menjadikan Dithubad sebagai penjuru pembangunan Satuan Siber TNI AD yang dapat dilakukan dengan mempertimbangkan aspek *defensif* siber sebagai amanah doktrin Kartika Eka Paksi dan kualifikasi persandian yang tidak dimiliki. Perlu disadari bahwa medan siber adalah sistem komputer yang memiliki pengamanan tipologi dan enkripsi. Apapun kemampuan teknis yang dimiliki tanpa kemampuan pemecahan kode (Sandiman) akan berhenti bekerja tanpa menemukan informasi yang cukup bagi penyiapan informasi untuk kegiatan *ofensif*. Di sisi lain, kesiapan *ofensif* harus diimbangi dengan kemampuan *defensif* dalam pemeliharaan dan

Koleksi Perpustakaan Universitas Terbuka

pemulihan sistem informasi yang diperkirakan akan menjadi potensi dilakukannya serangan siber. Kapasitas prajurit perhubungan dalam hal ini harus ditambahkan dengan kemampuan *defensif* yang diperoleh dari pelatihan *ethical hacking* yang perlu ditambahkan. Kemampuan ini dapat dilakukan dengan pendidikan kursus Bintara dan Perwira Siber yang sedang menunggu pelaksanaan uji teori II di Kodiklat. Peran Dithubad dalam pembentukan Satuan Siber bagi TNI AD adalah penyediaan alat Pernika seperti pencari frekuensi radio pita lebar dan *direction finder*, dan personel yang telah memiliki kualifikasi sebagai prajurit yang mengerti tentang elektronika, komunikasi dan informatika. Gelar Satuan Perhubungan di lingkungan TNI AD dari tingkat Pusat, Komando Daerah Militer (Kodam) dengan Perhubungan Daerah Militer (Hubdam) dan Detasemen Perhubungan di Kodam/Korem/Divisi, dan Tim Perhubungan Komando Resor Militer (Korem), Kompi Perhubungan (Kihub) Brigade Infanteri (Brigif), serta Peleton Komunikasi di setiap batalyon.

Koleksi Perpustakaan Universitas Terbuka

3) Pusat Intelijen Angkatan Darat (Pusintelad).

Pusintelad sebagai pelaksana fungsi intelijen memiliki fungsi untuk kegiatan penyelidikan, pengamanan, dan penggalangan. Dalam hal kegiatan penyelidikan memiliki tugas untuk mendapatkan informasi. Naluri penyelidikan intelijen menyediakan naluri (*sense*) yang bagus bagi kebutuhan personel pengawak siber. Namun perlu dicatat bahwa kegiatan penyelidikan intelijen dilaksanakan secara tertutup dan hanya berujung kepada diperolehnya informasi intelijen sebagai bahan pengambilan keputusan pimpinan. Dihadapkan kepada kegiatan siber yang sifatnya terbuka maka ini bertentangan dengan prinsip intelijen yang dilakukan secara tertutup. Di sisi lain, kebutuhan informasi siber dibutuhkan untuk melaksanakan serangan balik terhadap sasaran (musuh) sehingga sangat berbahaya jika satuan intelijen yang tertutup itu melakukan serangan. Kapasitas pertahanan dalam jaring tertutup intelijen dilindungi dan jangan sampai terpublikasi. Karena itu pemberian kapasitas siber secara utuh kepada Pusintelad dan jajarannya akan sama denagn membuka diri kepada informasi terbuka yang

Koleksi Perpustakaan Universitas Terbuka

menyalahi prinsip intelijen. Karena itu terkait pembentukan satuan siber peran yang dapat diberikan oleh Pusintelad adalah dukungan personel, peralatan, dan pendidikan naluri intelijen dalam penyelidikan informasi. Pusintelad akan dapat memberikan dukungan kesiapan dalam pendirian satuan siber dengan kapasitas naluri intelijen dan persandian. Terlebih sejak akhir Tahun 2016, Pusintelad dengan Pusat Informasi Intelijen (PII) telah mempraktikkan metode kerja siber dalam taraf deteksi dini dan investigasi terkait sentimen isu (serangan siber psikologis) dan insiden infrastruktur siber. Kapasitas ini akan menjadi metode kerja awal yang menyediakan informasi yang dapat mendorong kerja tim lain. Tanpa dukungan informasi awal dari Pusintelad maka Satuan Siber TNI AD akan kehilangan isu dalam merespon datangnya ancaman. Jadi metode kerja siber PII Pusintelad menyediakan bekal awal bagi metode kerja satuan siber yang akan dibentuk. Gelar Pusintelad dalam kapasitas dukungan siber telah ada sampai pada tingkat Komando Distrik Militer (Kodim) dengan kapasitas intelijen dan sandi. Keberadaan satuan sandi berpotensi divalidasi menjadi Satuan Siber dan sandi

Koleksi Perpustakaan Universitas Terbuka

jika memang ada kebijakan pimpinan yang mengacu kepada bentuk pengembangan simetris Badan Siber dan Sandi Negara (BSSN) yang sebelumnya adalah peleburan Lembaga Sandi Negara dengan Direktorat Keamanan Informasi (Dirkaminfo) Kementerian Komunikasi dan Informasi (Kemkominfo) dan *Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center* (ID SIRTII).

4) Dinas Informasi dan Pengolahan Data Angkatan Darat (Disinfolahtad).

Disinfolahtad sebagai salah satu Badan Pelaksana (Balak) fungsi di lingkungan TNI AD yang melakukan kegiatan dalam pemberian dukungan teknis dalam ranah siber. Kapasitasnya sebagai dinas merupakan dukungan kegiatan secara teknis dalam pelaksanaan keamanan sistem informasi di lingkungan TNI AD. Karena itu dihadapkan pada doktrin Kartika Eka Paksi untuk melaksanakan kegiatan *ofensif* dalam bentuk serangan siber tidak mampu dilaksanakan oleh Disinfolahtad. Disinfolahtad diprediksi memberikan sumbangan kemampuan teknis informatika dalam pembentukan Satuan Siber.

Koleksi Perpustakaan Universitas Terbuka

5) Dinas Penerangan Angkatan Darat (Dispenad).

Dispenad merupakan salah satu Badan Pelaksana (Balak) fungsi di lingkungan TNI AD yang melakukan kegiatan konfirmasi opini publik agar TNI AD memiliki citra positif di masyarakat. Kapasitas Dispenad memiliki Kasubdis Media *Online* (Kasubdismedonline) yang merupakan media garapan siber. Namun karena bidang tugas pembentukan opini maka jika ikut dalam kegiatan siber harus pula melakukan kesiapan dalam menerima serangan balik siber dari lawan, sehingga sangat riskan bagi Dispenad melakukan kegiatan siber karena akan berdampak kepada citra TNI AD yang bergerak ekspansif. Petak Dispenad dan jajarannya sebagai pemberi konfirmasi berita bernada positif bagi TNI AD sebaiknya dipertahankan. Peran yang dapat diberikan Dispenad dalam pembentukan badan siber di lingkungan TNI AD adalah menyediakan personel dan pelatihan dalam kegiatan produksi berita.

b. Kewenangan Satuan Siber TNI AD.

Respon siber dari aspek teknis memerlukan kemampuan melakukan kegiatan *defensif* dan *ofensif*. Kamampuan tersebut merupakan kapasitas yang dimintakan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

oleh Doktrin TNI AD Kartika Eka Paksi (KEP). Untuk itu pembentukan satuan siber harus memperhatikan kewenangan sebagai berikut:

1) Kemampuan *defensif*.

Secara *defensif* kemampuan siber harus mampu memberikan perlindungan terhadap seluruh sumberdaya telematika yang dimiliki TNI AD. Beberapa kemampuan *defensif* tersebut antara lain adalah:

a) Kemampuan terhadap sistem informasi musuh.

(1) Melaksanakan *monitoring* kegiatan di wilayah siber.

(2) Melakukan penyelidikan dan penyidikan serta pengungkapan terhadap bukti-bukti *digital*.

b) Kemampuan terhadap sistem informasi sendiri.

(1) Kapasitas tes penetrasi (*pentest*).

Meliputi kemampuan kegiatan *monitoring*, evaluasi dan pelaporan terhadap kegiatan pembangunan atau pengembangan infrastruktur TI/SI di lingkungan TNI AD.

Koleksi Perpustakaan Universitas Terbuka

(2) Memberikan *cyber awarenes* dan instruksi khusus dalam penggunaan TI/SI di lingkungan Angkatan Darat.

(3) Identifikasi aset infrastruktur kritis dan kerentanan TI/SI yang ada di Angkatan Darat.

(4) Melakukan pendataan analisis terhadap kerentanan infrastruktur TI/SI Angkatan Darat atau serangan siber. Serta memberikan saran ataupun dokumentasi langkah-langkah penyelesaian.

(5) Membuat *helpdesk center* sebagai pusat layanan laporan atau isu masalah terhadap keamanan teknologi dan informasi. Selain itu membuat laporan media *online* yang dicatat dan dilaporkan juga diatur secara terurut dan diorganisasikan.

2) Kemampuan *ofensif.*

a) Mengembangkan kemampuan intelijen pertahanan dan serangan siber serta penegakan hukum untuk melindungi sistem infrastruktur kritis TI/SI Angkatan Darat

Koleksi Perpustakaan Universitas Terbuka

maupun kegiatan di wilayah siber sesuai dengan hukum.

b) Melakukan serangan siber.

c) Membangun kemampuan untuk respon cepat, dan melakukan pemulihan.

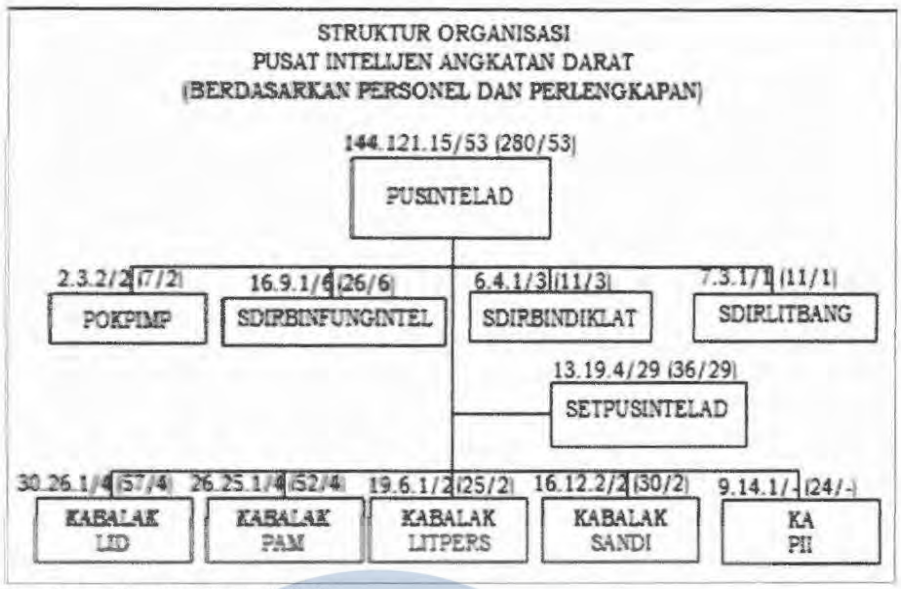
c. Peningkatan fungsi Satuan Siber TNI AD.

Pemberdayaan kemampuan siber di lingkungan TNI AD dapat dilakukan dengan meningkatkan kemampuan dan kapasitas satuan siber untuk kegiatan *defensif* siber, serta pemberian pelatihan metode kerja kepada Satuan Siber Kopassus untuk kemampuan *ofensif* siber. Kedua sumberdaya siber yang telah ada dapat menjadi sarana respon siber secara baik dengan koordinasi kerja yang dapat dilakukan melalui *Desk Siber* yang ada di Markas Besar Angkatan Darat (Mabesad).

1) Validasi organisasi Pusintelad.

Komposisi organisasi Pusintelad sesuai Peraturan Kasad (Perkasad) 78 Tahun 2014 adalah 333 orang. PII memiliki personel sejumlah 24, berkualifikasi teknologi informasi dan Balaksandi sebanyak 32 orang berkualifikasi sandi.

Koleksi Perpustakaan Universitas Terbuka



Sumber: Pusintelad, 2018

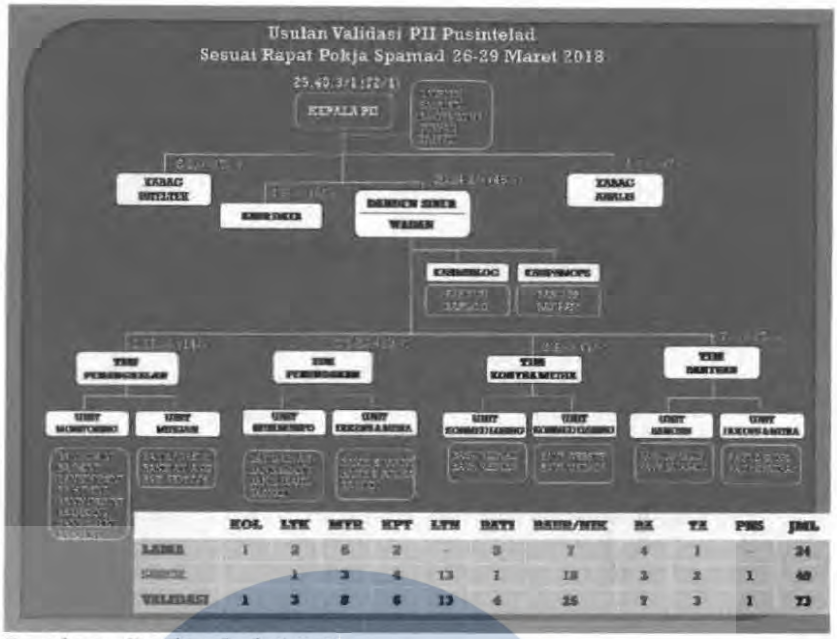
Gambar 2.4
Struktur Organisasi Pusintelad sesuai Perkasad 2014

2) Validasi kerja Pusat Informasi Intelijen (PII) Pusintelad.

PII Pusintelad telah melakukan kegiatan siber yang meliputi *monitoring* dan pelaporan serta investigasi dalam jaring. Untuk lebih mengoptimalkan perlu ditingkatkan kemampuan *monitoring*nya sehingga dapat melakukan kegiatan *defensif*. Kapasitas *monitoring* dan investigasi PII Pusintelad dapat ditingkatkan dengan penambahan personel, peralatan, dan keahlian personel. Bentuk penambahan organisasi PII Pusintelad disarankan divalidasi menjadi:

Koleksi Perpustakaan Universitas Terbuka

43794.pdf



Sumber : Pusintelad, 2018

Gambar 2.5
Struktur Organisasi PII Pusintelad sesuai Usul Validasi

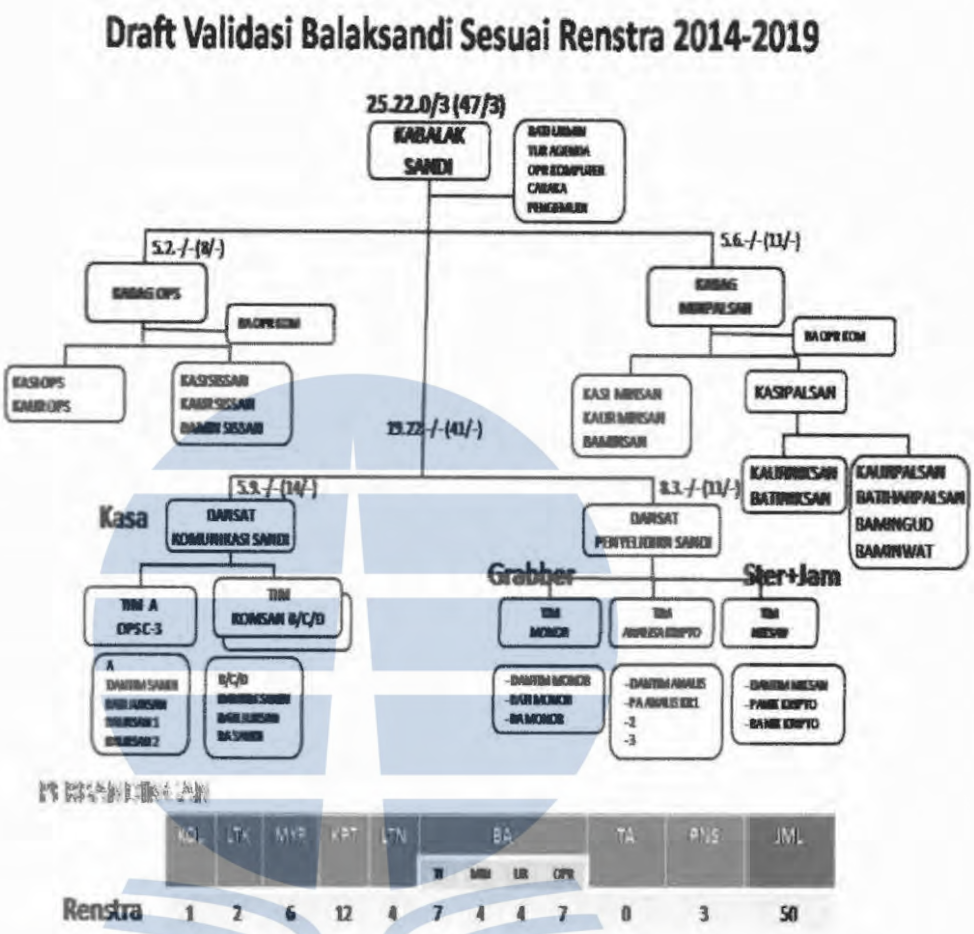
3) Validasi organisasi Badan Pelaksana Sandi (Balaksandi) Pusintelad.

Balaksandi Pusintelad merupakan unsur pelaksana Pusintelad yang bertanggung jawab menyelenggarakan kegiatan di bidang persandian Angkatan Darat. Kapasitasnya saat ini melakukan kegiatan pengamanan informasi berklasifikasi melalui komunikasi antar satuan (kamar sandi), pencarian *bug* (alat sadap), dan forensik *digital* untuk ponsel. Kemampuan ini harus ditambahkan dengan kemampuan edukasi siber (*security atau siber awareness*) dan forensik *digital*. Bentuk penambahan organisasi Balaksandi Pusintelad

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

disarankan divalidasi sesuai Perencanaan Strategis (Renstra) yang telah diajukan.



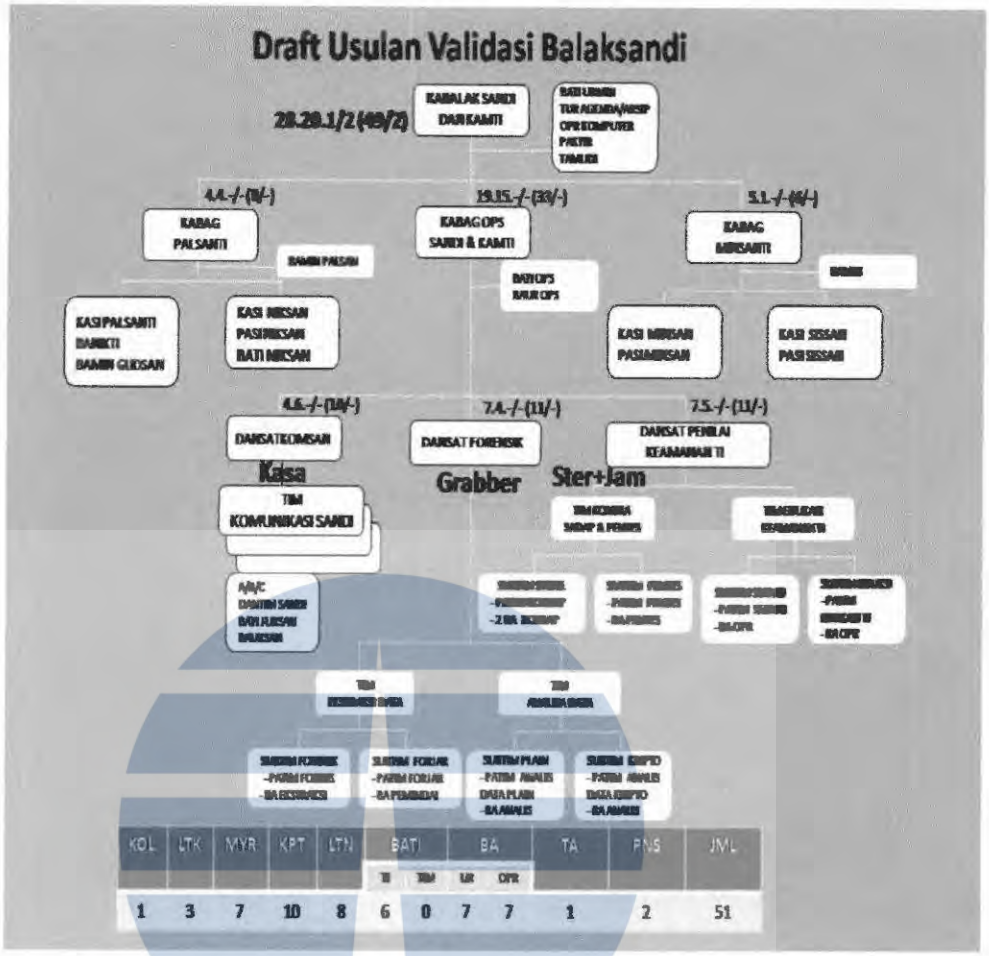
Sumber : Pusintelad, 2018

Gambar 2.6
Struktur Organisasi Balaksandi Pusintelad
sesuai Usul Perubahan Renstra 2014-2019

Optimalisasi validasi Balaksandi sesuai sinergi pembentukan fungsi siber perlu ditambah dengan kemampuan edukasi kepedulian keamanan siber dan tata laksana siber.

Koleksi Perpustakaan Universitas Terbuka

487794.pdf



Sumber : Pusintelad, 2018

Gambar 2.7
Struktur Organisasi Balaksandi Pusintelad sesuai Usul Validasi

4) Pembentukan *desk* siber Spamad.

Desk Siber Spamad akan menjadi wadah dalam melakukan koordinasi kerja antara kegiatan *monitoring* dan investigasi Pusintelad sebagai kegiatan *defensif* siber dengan kegiatan *ofensif* siber yang harus dilakukan oleh Satuan Siber Kopassus dan Unit Perang Elektronika (Pernika) di jajaran Dithubad.

Koleksi Perpustakaan Universitas Terbuka

Penambahan kapasitas sistem informasi di Pusat Informasi Intelijen (PII). Beberapa hal terkait perlunya peningkatan kapasitas aplikasi *server* Sisfo Lapor Cepat *(Humint),* serta aplikasi dan *server* Sisfo Sumber Informasi Terbuka *(Osint)* sebagai berikut:

1) Terkait aplikasi *Humint* dan *Osint* merupakan pengadaan TNI AD TA 2013, perlu dilakukan peningkatan kapasitas sistem, dengan mengingat keberadaan aplikasi versi lama dihadapkan kepada kebutuhan respon lapor cepat dan sentimen isu/konflik yang berkembang masif di media jaring (daring), sebagai berikut:

   a) Peningkatan kapasitas aplikasi *Osint*:

      (1) Pembaharuan sistem *Osint* versi yang terbaru.

      (2) Pembaharuan tampilan antarmuka yang terintregasi dengan aplikasi *chatting* aman.

      (3) Aplikasi *Osint* versi *mobile*.

      (4) Bisa melakukan penambahan situs dan akun media sosial secara mandiri.

   b) Peningkatan kapasitas aplikasi *Humint*:

      (1) Pembaharuan sistem *Humint* versi yang terbaru.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

(2) Integrasi dengan database aplikasi *chatting* aman.

(3) Aplikasi mobile versi *Humint*.

2) Dengan adanya kebutuhan peningkatan kapasitas tersebut, diperlukan penambahan perangkat keras untuk menjaga kestabilan kerja aplikasi, seperti:

a) Penambahan kapasitas server *Humint* dan *Osint*.

b) Penambahan media penyimpanan (*stroge*) *server chatting* aman sebesar 100 *terabite* (untuk prediksi pengguna aparat intelijen (Apintel) sebanyak 10.000 orang/akun).

c) Penambahan ruang *server* khusus untuk pengelolaan Sisfointel Pusintelad.

d) Penambahan *backup* daya listrik untuk mendukung operasional Sisfointel Pusintelad yang diprediksikan akan mencapai 100 KVA.

B. Penelitian Terdahulu

Penelitian terdahulu yang membahas kejahatan siber diantaranya Afitrahim M.R dalam tulisan skripsi yang berjudul Yurisdiksi berdasarkan *Convention On Cybercrime*, penulis menjabarkan masalah karena kemajuan teknologi yang sangat pesat, telah banyak pula usaha untuk melakukan pengaturan dalam dunia siber untuk mencegah atau menanggulangi terjadinya tindak dunia maya baik oleh hukum

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

internasional maupun hukum nasional. Salah satu satunya dengan lahirnya *Convention On cybercrime* yang dibuat oleh Dewan Eropa. Aspek yang menjadi perhatian khusus dalam konvensi ini adalah masalah yurisdiksi negara dalam menangani kasus tindak pidana siber karena semua negara tidak senang yurisdiksi negaranya dilampaui oleh negara lain, termasuk Indonesia. Sedangkan untuk pengaturan di negara Indonesia, penulis menggunakan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang penggunaanya terkait dengan Satuan Siber TNI AD .

Marissa Amalina Shari Harahap (2012) pada penelitian tesis berjudul Analisis Penerapan Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Dalam Tindak Pidana Siber, menjelaskan bahwa penerapan Undang – Undang No.11 Tahun 2008 ini dinilai masih banyak kelemahan dan kekurangan di dalam mengatur tindak pidana siber serta menimbulkan banyak permasalahan baru. Berkaitan dengan semakin canggihnya modus kejahatan tindak pidana siber yang semakin berkembang pesat, para pembuat Undang – Undang dan penegak hukum belum melakukan perubahan sama sekali kualitas dan kuantitas Undang – Undang ini malah cenderung Undang – Undang ini menuai banyak pro dan kontra dianggap tidak dapat menurunkan tingkat kejahatan tindak pidana siber secara signifikan sehingga memunculkan tudingan bahwa Undang – Undang ini tidak berjalan secara efektif terutama dari aspek pidananya. Undang – Undang No.11 Tahun 2008 masih membutuhkan penambahan kesempurnaan khususnya tentang *Procedural*

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Law dan hal yang masih menjadi persoalan dan perlu dicarikan solusinya adalah mengenai sifat khusus dari bidang teknologi informasi, yang penanganannya harus dilakukan oleh orang yang memahami teknologi informasi dan komunikasi serta perlunya pembaharuan Undang – Undang atau menerbitkan Peraturan Pemerintah yang mengakomodir sifat kekhususan dari bidang teknologi informasi dan komunikasi. Dalam penelitian ini aspek yang dikaji adalah bagaimana Undang-Undang No. 11 Tahun 2008 dan Undang-Undang No. 19 Tahun 2019 tentang ITE mempengaruhi kegiatan Satuan Siber TNI AD dalam kaitannya dengan penanganan kejahatan siber.

Penelitian terdahulu Donny Siswoyo (2017) dengan judul Optimalisasi Kemampuan Pengungkapan Kejahatan Cyber (Studi Kasus Di Polda DIY), membahas tentang optimalisasi pengungkapan kejahatan siber adalah merupakan penelitian hukum empiris yang dilengkapi data yang konkret. Pengungkapan kejahatan siber di krimsus Polda DIY belum terlaksana efektif karena Subdit 2 krimsus belum memiliki fasilitas sarana dan prasarana untuk mengolah data cek posisi, *Call Detail Record (CDR),* dan SMS (*Short Message Service).* Metode pelaksanaan tugas masih terhambat proses birokrasi yang diterapkan Bareskrim Polri maupun instansi terkait/samping dalam hal peminjaman sarana dan prasarana untuk mengolah data cek posisi, *Call Detail Record,* dan SMS *(Short Message Service)* cenderung memakan waktu yang lumayan lama. Aspek dalam penelitian Doni Siswoyo, dapat digunakan untuk pengembangan penelitian

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

ini bagaimana hambatan-hambatan yang dapat menyulitkan Satuan Siber TNI AD dalam mengungkap kejahatan siber.

C. Kerangka Berpikir

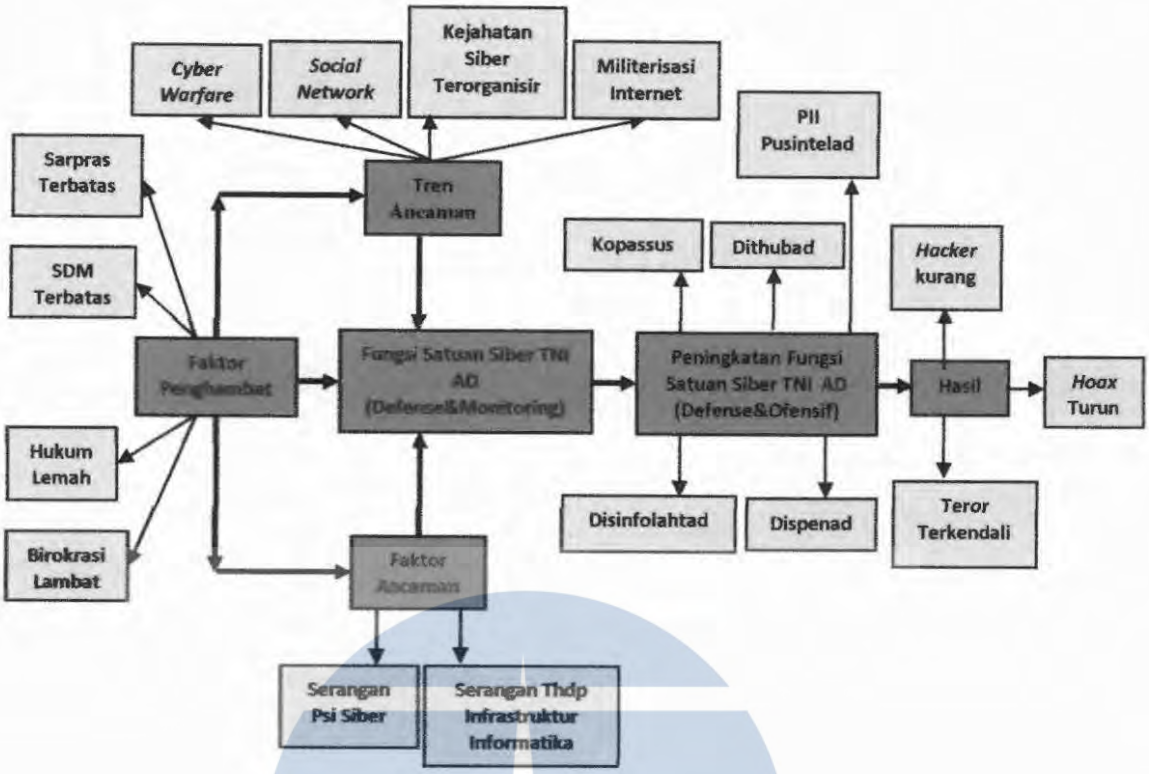
1. Konsep pemikiran

Perkembangan siber baik di dunia internasional maupun nasional telah berkembang dengan sangat pesat. Hal ini menimbulkan dampak yang positif dan negatif bagi kepentingan pertahanan dan keamanan bangsa. Dengan semakin berkembangnya *cyber war* yang dilakukan *hacker* bahkan telah menyerang tidak hanya instansi sipil melainkan juga instansi militer yang mengidentifikasikan bahwa tingkat pengamanan *cyber* atau kontra *cyber* masih sangat lemah, sehingga mempercepat pembentukan organisasi *cyber* secara berjenjang di setiap tingkatan menjadi hal utama dalam upaya menjaga kemanan data, *file* dan dokumen penting dan rahasia serta menangkal upaya serangan *cyber* lawan.

Setelah dilakukan telaah pustaka yang mendasari perumusan masalah yang diajukan dalam penelitian ini, selanjutnya dibentuk kerangka pemikiran teoritis yang akan digunakan sebagai acuan untuk pemecahan masalah. Kerangka pemikiran yang dibangun ditampilkan dalam skema kerangka penelitian sebagaimana terlihat pada Gambar 2.8.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf



Gambar 2.8
Skema Kerangka Penelitian

2. Asumsi

a. Fungsi Satuan Siber TNI AD saat ini hanya memiliki kemampuan *cyber defense* dan *monitoring* media, yang mana hal ini dapat memicu meningkatnya tren ancaman dan faktor ancaman yang dapat menyerang institusi TNI AD. Di samping itu, adanya faktor-faktor penghambat seperti keterbatasan sarana dan prasarana siber, SDM yang menguasai siber, kekuatan hukum perundang-undangan yang lemah dan lamanya jalur birokrasi penanganan siber juga menjadi penyebab terhambatnya perkembangan Satuan Siber TNI AD.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

b. Di lain sisi, dengan beragamnya faktor penghambat dalam rangka perkembangan Satuan Siber TNI AD tersebut, menyebabkan hal ini menjadi peluang dan kesempatan besar bagi para pelaku kejahatan siber untuk mengembangkan modus operandinya termasuk melakukan berbagai ancaman ke institusi Tni AD. Hal ini terjadi dikarenakan banyak pelaku kejahatan siber yang mengetahui keterbatasan yang dimiliki negara dan institusi TNI AD dalam memberantas kejahatan jenis ini.

c. Dengan berbagai faktor penghambat yang ada, faktor ancaman yang semakin lama semakin berkembang dan meningkat serta semakin bertambahnya tren ancaman yang bakal dihadapi oleh Satuan Siber TNI AD, menyebabkan peningkatan fungsi Satuan Siber TNI AD menjadi memiliki kemampuan tidak hanya *defensif* melainkan juga *ofensif* adalah merupakan suatu keharusan. Hal ini dapat segera terwujud dengan melibatkan beberapa satuan menjadi suatu tim terpadu, yaitu : Siber Kopassus, Pernika Dithubad, PII Pusintelad, Disinfolahtad dan Dispenad.

d. Dengan terwujudnya Satuan Siber TNI AD yang telah memiliki kemampuan *ofensif*, maka akan mampu mendukung kolaborasi dan sinergitas antar lembaga siber nasional dalam mempertahankan dan memelihara keamanan dunia siber nasional dan mampu menjaga kedaulatan negara

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

dari ancaman serangan siber musuh/lawan, serta secara khusus jaringan komputer, piranti lunak dan persenjataan otomatis milik TNI AD, mampu menjaga rahasia negara bidang pertahanan, sehingga pada akhirnya menghasilkan kemampuan pertahanan nasional yang dapat mengurangi *hacker*, menurunkan angka kriminalitas/kejahatan siber seperti *hoax* dan yang lebih tinggi tingkatannya mampu mengendalikan kegiatan teror kepada negara Indonesia.

D. Operasionalisasi Konsep

Menurut Sugiyono (2012:31) definisi operasional adalah penentuan konstrak atau sifat yang akan dipelajari sehingga menjadi variabel yang dapat diukur. Definisi operasional menjelaskan cara tertentu yang digunakan untuk meneliti dan mengoperasikan konstrak, sehingga memungkinkan bagi peneliti yang lain untuk melakukan replikasi pengukuran dengan cara yang sama atau mengembangkan cara pengukuran konstrak yang lebih baik.

Sedangkan menurut Nani Darmayanti (dalam Mushlihin, 2013) definisi operasional adalah rumusan tentang ruang lingkup dan ciri-ciri suatu konsep yang menjadi pokok pembahasan dan penelitian karya ilmiah Jadi, dapat disimpulkan operasional adalah definisi yang didasarkan atas sifat-sifat variabel yang diamati. Operasional mencakup hal-hal penting dalam penelitian yang memerlukan penjelasan. Operasional bersifat spesifik, rinci, tegas dan pasti yang menggambarkan karakteristik variabel-variabel penelitian dan hal-hal yang dianggap penting.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Operasional konsep pada penelitian ini bagaimana konsep tren ancaman kejahatan siber dapat mempengaruhi fungsi Satuan Siber TNI AD dari hanya bersifat *defense* dan *monitoring* yang diharapkan menjadi *defense* dan *offense*, dengan faktor penghambat yang ada baik itu secara internal maupun eskternal.

Konsep	Dimensi	Teknik Pengumpulan Data	Sumber Data
Tren Ancaman	1. *Cyber Warfare* 2. *Social Networking* 3. Kejahatan Siber Terorganisir 4. Militerisasi Internet	Studi Pustaka	Data kejahatan siber
Faktor Ancaman	1. Serangan Psi Siber 2. Serangan terhadap Infrastruktur dan Informatika	1. Studi pustaka 2. Wawancara	Data Satsiber TNI AD
Faktor Penghambat dalam peningkatan fungsi Satuan Siber TNI AD	1. Keterbatasan Sarana dan Prasarana 2. SDM Terbatas 3. Hukum yang Lemah 4. Birokrasi Lambat	Wawancara	1. Pimpinan Satsiber TNI AD 2. Prajurit Satsiber TNI AD 3. Perwira Spamad 4. Prajurit Spamad

Tabel 2.1
Operasional Konsep Penelitian

E. Hipotesis

Berdasarkan identifikasi masalah dan kerangka pemikiran di atas, peneliti mengajukan hipotesis sebagai berikut:

1. Kejahatan siber menimbulkan potensi ancaman dan mempengaruhi fungsi Satuan Siber TNI AD.

Koleksi Perpustakaan Universitas Terbuka

2. Peningkatan fungsi Satuan Siber TNI AD terhambat oleh adanya faktor-faktor seperti keterbatasan sarana dan prasarana, sumberdaya manusia, birokrasi yang lambat serta lemahnya hukum.
3. Satuan Siber TNI AD berperan dalam mendukung sinergitas lembaga siber nasional dalam rangka mengungkap kejahatan siber.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

BAB III

METODE PENELITIAN

A. Desain Penelitian

Penelitian ini berusaha untuk memaparkan apa saja bentuk dari kejahatan siber serta siapa pelakunya dan bagaimana kejahatan siber tersebut memberikan ancaman bagi institusi TNI AD. Selain itu dalam penelitian ini akan dipaparkan apa saja faktor penghambat dalam peningkatan fungsi Satuan Siber TNI AD dalam menghadapi kejahatan siber.

Pendekatan yang digunakan oleh peneliti dalam penelitian ini adalah pendekatan kualitatif. Berdasarkan pemikiran Creswell (2010) (dalam Herdiansyah, 2011:8) penelitian kualitatif adalah suatu proses penelitian ilmiah yang lebih dimaksudkan untuk memahami masalah-masalah manusia dalam konteks sosial dengan menciptakan gambaran yang disajikan secara kompleks tentang fenomena yang diangkat. Pendekatan kualitatif dipilih dengan tujuan agar diperoleh data yang spesifik, lengkap, relevan dan mendalam mengenai factor kejahatan siber dalam pengaruhnya kepada peningkatan fungsi Satuan Siber TNI AD.

Objek dalam penelitian ini adalah ancaman kejahatan siber, sedangkan subjek dalam penelitian ini adalah Satuan Siber TNI AD.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

B. Sumber Informasi dan Pemilihan *Informan*

1. Sumber informasi

Sumber data yang akan dikumpulkan dalam penelitian ini adalah data hasil penelitian dan data sekunder. Data hasil penelitian diperoleh langsung dari lapangan melalui observasi lapangan dan wawancara. Data sekunder diperoleh dari hasil kajian dokumen dan studi literatur. Pengumpulan data disesuaikan dengan ketersediaan data di lapangan, keterbatasan waktu dan efisiensi serta tingkat akurasi data yang dibutuhkan.

2. Pemilihan *informan*

Informan dalam penelitian ini ditentukan melalui teknik *purposive sampling*. Teknik ini mencakup orang-orang yang diseleksi atas dasar kriteria-kriteria tertentu yang dibuat berdasarkan tujuan riset, sedangkan orang-orang dalam populasi yang tidak sesuai dengan kriteria tersebut tidak dijadikan sampel (Kriyantono, 2006).

Menurut Spradley (dalam Moleong, 2012:4) *informan* harus memiliki beberapa kriteria yang harus dipertimbangkan, yaitu:

a. Subjek yang telah lama intensif menyatu dengan suatu kegiatan atau medan aktivitas yang menjadi sasaran atau perhatian penelitian dan ini biasanya ditandai oleh kemampuan memberikan informasi di luar kepala tentang sesuatu yang ditanyakan.

Koleksi Perpustakaan Universitas Terbuka

b. Subjek masih terikat penuh serta aktif pada lingkungan dan kegiatan yang menjadi sasaran penelitian.

c. Subjek mempunyai cukup banyak waktu dan kesempatan untuk dimintai informasi.

d. Subjek yang dalam memberikan informasi tidak cenderung diolah atau dikemas terlebih dahulu dan mereka relatif masih lugu dalam memberikan informasi (Moleong, 2000).

Informan dalam penelitian ini adalah mereka yang terkait dengan Satuan Siber TNI AD baik itu pelaku maupun supervisinya yaitu Spamad dengan jumlah 55 personel Satuan Siber TNI AD (Perwira 7 orang dan prajurit 48 orang) dan 4 personel Spamad (Perwira 3 orang dan prajurit 1 orang) selaku supervisi untuk Satuan Siber TNI AD.

C. Instrumen Penelitian

Instrumen penelitian adalah alat-alat yang akan digunakan untuk mengumpulkan data, instrumen penelitian ini dapat berupa kuesioner, formulir observasi, formulir-formulir lain yang berkaitan dengan pencatatan data dan sebagainya (Notoatmodjo, 2010). Penelitian dengan metode kualitatif, instrumennya adalah peneliti sendiri, peranan penelitilah yang menentukan keseluruhan apa yang akan dirancangnya. Dengan demikian instrumen penelitian dengan metode kualitatif adalah peneliti sendiri.

Koleksi Perpustakaan Universitas Terbuka

Penggunaan peneliti sebagai instrumen penelitian bertujuan untuk mendapatkan data empiris di lapangan, instrumen penelitian yang digunakan adalah wawancara dan pengamatan terhadap objek penelitian melalui sejumlah pendalaman dalam bentuk diskusi terfokus. Wawancara melalui sejumlah pertanyaan yang terfokus dilakukan secara logis berhubungan dengan masalah penelitian, dan tiap-tiap pertanyaan merupakan jawaban-jawaban yang mempunyai makna dalam menguji hipotesis.

D. Prosedur Pengumpulan Data

Berdasarkan penelitian kali ini data yang peneliti kumpulkan dilakukan dengan cara wawancara, studi literatur dan studi dokumentasi berkaitan dengan judul penelitian yang memiliki subjek Satuan Siber TNI AD, sedangkan untuk sampel penelitian, peneliti menggunakan teknik *purposive sampling* untuk memudahkan peneliti dalam mendapatkan informan yang sesuai dan memiliki kriteria khusus serta bisa memberikan data yang dibutuhkan sehingga sesuai dengan tujuan penelitian, dapat memecahkan permasalahan penelitian dan dapat memberikan nilai yang lebih representatif. *Informan* yang ditentukan berdasarkan kriteria melalui wawancara mendalam dan berhenti ketika tidak ada informasi baru lagi, terjadi replikasi atau pengulangan variasi informasi, mengalami titik jenuh informasi.

1. Studi literatur

Studi literatur menurut Creswell (2010:270) adalah mencari referensi konsep teori yang relevan dengan fenomena atau

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

permasalahan yang ditemukan. Referensi tersebut berisikan tentang:

a. Tren dan faktor ancaman kejahatan siber.

b. Satuan Siber TNI AD.

c. Peningkatan fungsi Satuan Siber TNI AD.

d. Faktor Penghambat.

e. Peran Satuan Siber TNI AD dalam mendukung sinergitas lembaga siber nasional.

Referensi ini dapat dicari dari buku, jurnal, artikel laporan penelitian, dan situs-situs di internet. *Output* dari studi litertur ini adalah terkoleksinya referensi yang relevan dengan perumusan masalah. Tujuannya adalah untuk memperkuat penelitian serta sebagai dasar teori dalam melakukan penelitian mengenai kejahatan siber dalam peningkatan fungsi Satuan Siber TNI AD.

2. Studi dokumentasi

Dalam Penelitian ini peneliti akan melakukan proses dokumentasi dengan mengumpulkan dokumen publik, seperti makalah, majalah atau koran. Selain itu peneliti mengumpulkan dokumen materi *audio* dan *visual*. Data ini bisa berupa foto, objek-objek seni, *videotape* dan segala jenis suara. Studi dokumentasi merupakan pelengkap dari penggunaan metode observasi dan wawancara dalam penelitian kualitatif. Dokumen merupakan catatan peristiwa yang sudah berlalu, catatan harian satuan, sejarah satuan, peraturan dan kebijakan satuan, dan materi *audio visual*

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

berbentuk foto-foto kegiatan peneliti dalam melakukan penelitian terhadap peningkatan fungsi Satuan Siber TNI AD.

3. Wawancara

Peneliti mengumpulkan data sekunder dengan melakukan wawancara maka peneliti harus dapat menentukan para narasumber yang tepat dalam memberikan informasi serta menyediakan beberapa instrumen pertanyaan untuk mengetahui apa yang melatar belakangi munculnya Satuan Siber TNI AD, sejarah, visi dan misi, proses, mobilitas, interaksi, faktor penghambat dan faktor pendukung serta segala aktivitas yang tengah dilakukan oleh Satuan Siber TNI AD.

E. Metode Analisis Data

Menurut Patton yang dikutip Moleong (2013:13) mengatakan analisis data dalam penelitian kualitatif adalah proses mengatur urutan data, mengorganisasikannya ke dalam suatu pola, kategori dari suatu uraian dasar.

Cara yang digunakan untuk menganalisis data dalam penelitian ini adalah dengan menggunakan teknik trianggulasi data, trianggulasi dilakukan dengan membandingkan dan mengecek data yang telah diperoleh melalui beberapa sumber. Cara-cara yang digunakan dalam proses trianggulasi data yaitu dengan:

1. Membandingkan data hasil pengamatan dengan data hasil wawancara.

Koleksi Perpustakaan Universitas Terbuka

143794.pdf

2. Membandingkan apa yang dikatakan *informan* di depan umum dengan apa yang dikatakannya secara pribadi.
3. Membandingkan apa yang disampaikan seorang *informan* dengan yang disampaikan oleh *informan* lain.
4. Membandingkan keadaan dan perspektif seseorang dengan berbagai pendapat dan pandangan orang lain yang berasal dari antar satuan kerja di TNI AD.
5. Membandingkan hasil wawancara dengan isi suatu dokumen yang berkaitan.

Berdasarkan pemaparan di atas, menganalisis data dalam penelitian ini menggunakan teknik trianggulasi data yang digunakan untuk mengecek kembali keabsahan agar tidak terjadi kesalahan/perbedaan dalam pengolahan data dari berbagai sumber yang ada. Peneliti membandingkan hasil wawancara yang diperoleh dari masing-masing sumber yaitu pimpinan TNI AD, Staf Umum Pengamanan Angkatan Darat (Spamad) selaku supervisi dan juga pelaku yang ada di Satuan Siber TNI AD tersebut.

Koleksi Perpustakaan Universitas Terbuka

146794.pdf

BAB IV

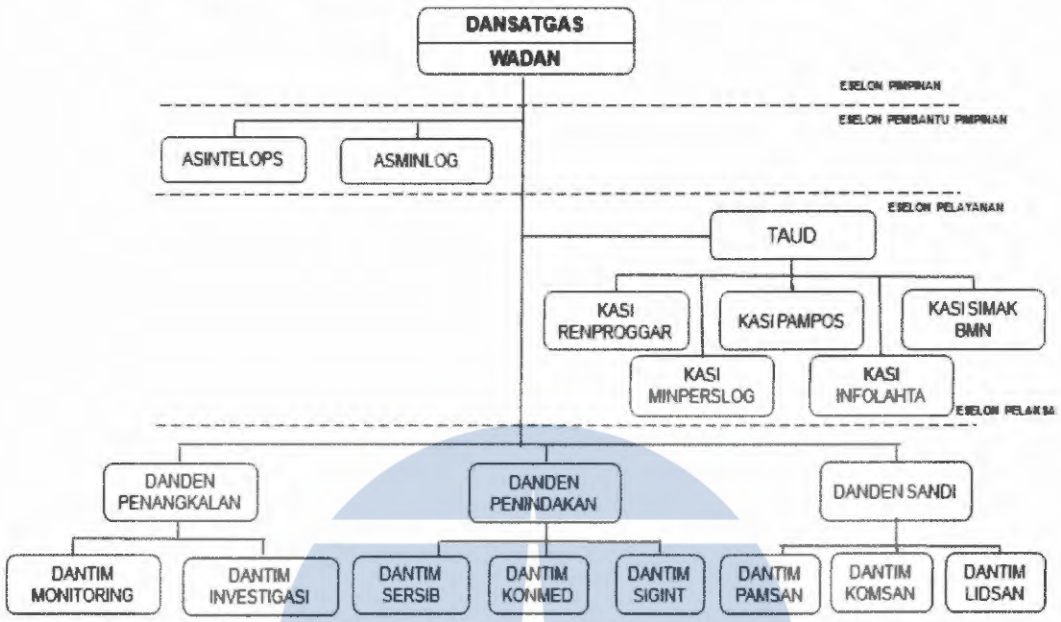
HASIL DAN PEMBAHASAN

A. Deskripsi Objek Penelitian

Satuan Siber TNI AD mulai beroperasi pada bulan Juni 2018 berdasarkan Surat Perintah Kasad Nomor Sprin/2103/VI/2018 yang berisi tentang perintah melaksanakan Satgas *Cyber Defence* Tahun 2018. Satuan Siber TNI AD berlokasi di Jalan Veteran No. 5 Jakarta Pusat, tepatnya di Gedung E lantai 7 Markas Besar TNI AD. Ruangan Satuan Siber TNI AD terbagi menjadi dua ruangan utama, yaitu ruangan pimpinan (Dansatgas Siber TNI AD) dan ruangan anggota. Untuk ruangan anggota terbagi menjadi enam bagian yang diisi oleh personel-personel sesuai dengan pembagian jabatannya, yaitu: Tim Penindakan, Tim Penangkalan, Tim Sandi, Bagian Urusan Pengamanan dan Operasional, Bagian Urusan Administrasi dan Logistik serta Staf Pimpinan. Setiap ruangan baru difasilitasi oleh perangkat kerja berupa *laptop* untuk masing-masing unit kerja dan ditunjang oleh satu *modem router* khusus untuk akses *internet*. Batasan dari lokasi Satuan Siber TNI AD berada di dalam kompleks Markas Besar TNI AD dan berada di lantai 7 yang merupakan lantai paling atas dari gedung E, sehingga dari segi kerahasian dan keamanan sudah memenuhi persyaratan. Saat ini, personel Satuan Siber TNI AD beranggotakan 55 personel yang berasal dari berbagai satuan di tanah air yang merupakan lulusan dari dua kali penataran/kursus siber yang

Koleksi Perpustakaan Universitas Terbuka

diselenggarakan oleh TNI AD bekerja sama dengan Pindad, sehingga memiliki latar belakang ilmu IT dan intelijen yang berbeda-beda.



Sumber :Satuan Siber TNI AD, 2018

Bagan 4.1
Struktur Organisasi Satuan Siber TNI AD

B. Hasil Penelitian

1. Deskripsi informan

Penelitian ini merupakan penelitian kualitatif yang bertujuan untuk mengetahui bagaimana ancaman kejahatan siber terhadap peningkatan fungsi Satuan Siber TNI AD. *Informan* berjumlah 10 orang yang berdinas di Satuan Siber TNI AD dan Staf Umum Pengamanan Angkatan Darat (Spamad), seperti yang diuraikan pada Tabel 4.1:

Koleksi Perpustakaan Universitas Terbuka

No	Informan	Usia	Jenis Kelamin	Pangkat	Jabatan
1	Informan A		Laki-Laki	Letkol	Dansat Siber TNI AD
2	Informan B	30	Laki-Laki	Kapten	Kasipam Ops Satgas Siber TNI AD
3	Informan C	27	Laki-Laki	Letnan Satu	Satgas Siber TNI AD
4	Informan D	38	Laki-Laki	Kapten	Satgas Siber TNI AD
5	Informan E	30	Laki-Laki	Sersan Satu	Satgas Siber TNI AD
6	Informan F	26	Laki-Laki	Sersan Dua	Satgas Siber TNI AD
7	Informan G	25	Laki-Laki	Letnan Dua	Dantim Komed 1.B Satgas Siber
8	Informan H	34	Laki-Laki	Kapten	Pabanda Spamad Mabesad
9	Informan I	31	Laki-Laki	Sersan Satu	Spamad Mabesad
10	Informan J	29	Laki-Laki	Sersan Satu	Spamad Mabesad

Tabel 4.1
Daftar *Informan* Penelitian Analisis Faktor Kejahatan Siber Terhadap Peningkatan Fungsi Satuan Siber TNI AD

2. Konsep mengenai tren ancaman kejahatan siber

Peneliti melakukan wawancara, melakukan observasi dan mengambil dokumentasi untuk mengetahui bagaimana pandangan *informan* mengenai tren ancaman kejahatan siber terjadi dan siapa pelakunya. Peneliti melakukan wawancara dengan *Informan* A, responden menyatakan bahwa:

"Kejahatan siber sudah terjadi. Pelakunya adalah para *hacker* yang mungkin dibayar mahal untuk mencuri rahasia negara ataupun membuat berita *hoax* untuk merusak citra TNI. Seiring dengan tumbuhnya masyarakat informasi yang dinamis dan cepat. Keterlambatan informasi berdampak kepada pembiaran ancaman dan akhirnya akan memberikan kesan pembiaran terhadap seluruh ancaman siber yang berpotensi lebih banyak di masa yang akan mendatang".

Koleksi Perpustakaan Universitas Terbuka

49794.pdf

Responden mengaku bahwa ancaman kejahatan siber sudah marak terjadi dan perlu untuk adanya pencegahan dan perlawanan. Untuk memperkuat pandangan *Informan* A maka peneliti melakukan triangulasi dengan mewawancarai *Informan* B yang bertugas sebagai Kasipamops Satgas Siber TNI AD menyatakan bahwa:

"Ancaman kejahatan siber telah terjadi. Bisa dilihat dengan banyaknya kasus terorisme menggunakan aplikasi enkripsi atau *hacking*, para pelakunya bahkan orang-orang yang tidak terduga. Karena mereka cukup bekerja dari rumah dan meretas informasi melalui komputer. Institusi TNI AD tidak luput dari kejahatan siber, contoh pada kasus terorisme yang akan melakukan penyerangan menggunakan aplikasi sandi/enkripsi untuk mengirim kode kepada rekan terorisnya"

Informan C menyatakan bahwa:

"Kejahatan siber telah terjadi. Meningkatnya modus kejahatan siber dunia diikuti dengan modusnya yang makin canggih. Contoh saja seperti pembobolan rekening nasabah di bank tertentu, para *hacker* telah mencuri uang nasabah dalam jumlah yang banyak" dan dalam tubuh TNI AD, bocornya beberapa rahasia institusi.

Informan D menyatakan bahwa:

"Sudah terjadi. Di lingkungan TNI AD saja telah terjadi bocornya rahasia negara".

Informan G yang bertugas sebagai Dantim Komed 1.B menyatakan bahwa:

"Akan terjadi. Bahkan telah terjadi ketika, satuan keamanan terbesar seperti TNI AD tidak memiliki pasukan khusus untuk menghadapi ancaman kejahatan siber, maka dengan mudah pelaku ancaman masuk ke dalam intitusi ini".

Selain itu peneliti melakukan wawancara dengan *informan* dari Spamad sebagai satuan yang *memonitoring* kegiatan Satgas Siber yakni *Informan* H dan I. *Informan* H menyatakan bahwa:

Koleksi Perpustakaan Universitas Terbuka

40794.pdf

"Kejahatan siber telah terjadi dan menyerang Institusi TNI AD. Untuk itu perlu satuan atau organisasi khusus guna menghadapi serangan tersebut sebagai antisipasi untuk menghadapi segala bentuk ancaman".

Informan I menyatakan bahwa:

"Kejahatan siber yang mengancam institusi TNI AD adalah ancaman *proxy war* yang telah terjadi dan butuh pencegahan segera".

Konsep Tren Ancaman Kejahatan Siber Terhadap Institusi TNI AD	
Konsep	Tren Ancaman Kejahatan Siber
Sebelum adanya kejahatan siber	Kejahatan yang dihadapi adalah peperangan maupun pemberontakan
Setelah adanya kejahatan siber	Kejahatan tidak lagi secara nyata, melainkan lebih berbahaya dengan menggunakan jaringan komputer yang dapat dengan mudah masuk ke dalam sistem informasi yang bersifat rahasia (Penggunaan aplikasi enkripsi, *hacking* dan teror)

Tabel 4.2
Konsep Tren Ancaman Kejahatan Siber terhadap Institusi TNI AD

3. Konsep mengenai faktor ancaman kejahatan siber

Peneliti melakukan wawancara, melakukan observasi dan mengambil dokumentasi untuk mengetahui bagaimana pandangan *informan* mengenai faktor ancaman kejahatan siber.

Peneliti melakukan wawancara dengan *Informan* A dalam kaitannya terhadap faktor ancaman kejahatan siber, responden menyatakan bahwa:

"Faktor-faktor ancamannya adanya sistem informasi yang tidak diamankan secara baik. Kepemilikan sistem informasi yang ternyata hanya memiliki pengaturan standar pabrik dan tidak dilakukan perubahan pengaturan secara maksimal sangat mengundang penyerang dalam bidang siber"

Koleksi Perpustakaan Universitas Terbuka

Responden menjelaskan bahwa ancaman kejahatan siber sudah sangat menganggu institusi TNI AD. Kejahatan yang meskipun berasal dari dunia maya tetapi sama saja seperti terjadi di alam nyata. Dalam kaitannya dengan TNI AD kejahatan siber juga mengancam secara institusi dan personal.

Untuk memperkuat pandangan *Informan* A maka peneliti melakukan triangulasi dengan melakukan wawancara staf Satsiber TNI AD dan Spamad sebagai satuan yang *memonitoring* kegiatan siber, yaitu *Informan* B, dia menyatakan bahwa:

"Faktor ancaman kejahatan siber memiliki banyak ancaman, di antaranya sabotase pihak luar terhadap sumberdaya siber TNI AD baik itu secara personel, teknologi maupun perangkat. Juga kegiatan mata-mata (*Spy*) melalui celah keamanan yang terdapat dalam sistem informasi TNI AD untuk mengakses data rahasia negara"

Contoh dari kegiatan mata-mata (*espionage*) dengan memanfaatkan teknologi pernah terjadi di Jerman yaitu dalam kampanye di Dresden pada September 2013, panel yang diduduki Kanselir Jerman Angela Merkel dan Menteri Pertahanan Thomas de Maiziere dihampiri sebuah *drone* kecil. Kemudian diketahui bahwa mesin tersebut diterbangkan oleh Pirate Party Jerman sebagai protes terhadap kebijakan pengintaian (*surveillance*) serta rencana pembelian pesawat tak berawak Euro Hawk. Majalah *New Scientist* edisi 1 Juli 2017 merilis berita berjudul Laporan "*Teror from Above*". Laporan tersebut menuturkan sejumlah gejala yang memungkinkan kelompok-kelompok teroris menggunakan *drone*. Kemudian Matrix UAV, sebuah perusahaan di Ukraina berhasil

Koleksi Perpustakaan Universitas Terbuka

memproduksi sebuah *drone* serbu dengan harga lebih murah dari *drone* predator yang digunakan Amerika Serikat. Dengan bentangan sayap selebar 1 meter, perangkat ini mampu menembakkan misil anti-tank. CEO Matrix UAV, Yury Kasyanov, menyatakan akan memproduksi *drone* seharga $100 ribu yang bisa dibeli oleh pemerintah di seluruh dunia.

Selain mewawancari *Informan* B, peneliti melakukan wawancara dengan delapan anggota Satuan Siber dan Spamad yang lain untuk memperkuat pandangan *Informan* A yaitu, *Informan* C, *Informan* D, *Informan* E, *Informan* F, *Informan* G, *Informan* H, *Informan* I, *Informan* J menyatakan bahwa:

"Kejahatan siber memiliki ancaman-ancaman seperti pencurian data, *sabotase*, maupun ancaman perang siber yang berpengaruh terhadap institusi TNI AD".

Informan C menyatakan bahwa:

"Ancaman kejahatan siber terhadap TNI AD adanya upaya penyerangan sistem informasi, *website* dan semua Alutsista yang berbasis komputer, faktornya bisa berupa kelemahan infrastuktur jaringan, penguasaan keterampilan juga serangan *hacker*".

Sebagai contoh serangan siber dengan menggunakan *drone* adalah bentuk perang siber dengan memanfaatkan penguasaan keterampilan teknologi sebagai berikut :

Pada 29 Januari 2017 sebuah serangan *drone* Amerika Serikat ke Yaman menewaskan sekitar 25 warga sipil pada operasi kontra teror AS di Yaman. Sedikitnya sembilan perempuan, enam anak kecil, termasuk putri mantan pemimpin Al-Qaida Anwar Al-Awlaqi yang berusia delapan tahun, dan 10 pria tewas dalam

Koleksi Perpustakaan Universitas Terbuka

serangan yang dilancarkan saat fajar di Desa Yakla di dalam Kabupaten Walad Rabie di Kota Kecil Qaifa, Baida. Sebanyak 10 anggota Al-Qaida juga tewas dalam serangan yang diberitakan *Xinhua*. Pemerintah tidak bersedia mengeluarkan komentar. AS telah meningkatkan operasi pesawat tanpa awak miliknya di Yaman sejak perang saudara meletus pada penghujung Tahun 2014, setelah anggota milisi Al-Houthi dengan dukungan dari mantan Presiden Yaman merebut kekuasaan.

Kasus serangan 13 *drone* yang disertai tembakan peluru kendali pada 10 Januari 2018 terjadi di instalasi militer Suriah. Serangan yang terjadi sebanyak dua kali tersebut merusak beberapa pesawat tempur dan *drone* kembali ke asalnya beberapa detik setelah melakukan serangan mematikan tersebut. Situs Tirto pada bulan Desember 2017 merilis berita yang menggambarkan sejarah pesawat tanpa awak. Dalam berita yang sama, Amerika serikat telah memanfaatkan *drone* sebagai senjata dalam perang melawan teror di Afghanistan.

Informan D menyatakan bahwa:

"Banyaknya sistem informasi yang telah digelar namun pendayagunaan teknologi atau sistem informasi tidak maksimal sehingga menjadikan kejahatan siber mudah mengancam"

Informan E menyatakan bahwa:

"Kejahatan siber sangat berbahaya bagi institusi TNI AD yang juga mengikuti perkembangan teknologi diberbagai bidang yang mencakup administrasi data rahasia dan persenjataan militer, ini adalah sebuah ancaman yang juga mempengaruhi kemanan nasional" .

Koleksi Perpustakaan Universitas Terbuka

14794.pdf

Informan F menyatakan bahwa:

"Kejahatan siber yang mengancam Institusi TNI AD harus menjadi perhatian karena dalam pengolahan data, hampir semuanya berbasis komputer. Faktor ancaman ini timbul karena akses internet yang tanpa batas, sistem keamanan jaringan yang kurang kuat, juga terbatasnya sumberdaya manusia dalam penggunaan jaringan komputer yang aman".

Informan G menyatakan bahwa:

"Kejahatan siber adalah suatu tindakan kejahatan yang memanfaatkan teknologi internet yang mengancam institusi TNI AD dalam kaitannya terhadap pembobolan data"

Informan H, *Informan* I, *Informan* J menyatakan bahwa:

"Kejahatan siber sebagai ancaman yang nyata, karena segala bentuk kejahatan yang dilakukan dapat merusak citra satuan TNI AD dimata masyarakat, sebut saja banyaknya *hoax*, yang diperparah apabila data rahasia TNI AD dapat di akses".

Bisa disimpulkan bahwa kejahatan siber merupakan bentuk kejahatan yang mengancam dunia nyata meskipun dilakukan melalui dunia maya, oleh para *hacker* yang dapat masuk ke jaringan atau sistem informasi di suatu instansi seperti TNI AD. Hal ini sangat berbahaya, karena satuan TNI AD sebagai alat pertahanan negara memiliki banyak basis data informasi rahasia juga Alutsista yang saat ini hampir seluruh penggunaanya berbasis komputer. Hal ini sesuai dengan pernyataan dari Girasa (2013) mendefinisikan kejahatan siber sebagai aksi kejahatan yang menggunakan teknologi komputer sebagai komponen utama. Untuk lebih jelas konsep faktor ancaman kejahatan siber terhadap Institusi TNI AD dapat dilihat pada Tabel 4.3:

Koleksi Perpustakaan Universitas Terbuka

Konsep Faktor Ancaman Kejahatan Siber Terhadap Institusi TNI AD	
Konsep	Faktor ancaman kejahatan siber
Sebelum adanya kejahatan siber	Kejahatan berupa kejahatan perang secara langsung yang merugikan yang merusak infrastruktur secara kasat mata
Setelah adanya kejahatan siber	Kejahatan tidak lagi secara nyata, melainkan lebih berbahaya dengan menggunakan jaringan komputer yang dapat dengan mudah masuk ke dalam sistem informasi yang bersifat rahasia menimbulkan kerusakan yang lebih besar tidak hanya berupa infrastruktur tetapi juga non-infrastruktur

Tabel 4.3
Konsep Faktor Ancaman Kejahatan Siber terhadap Institusi TNI AD

4. Konsep faktor penghambat dalam peningkatan fungsi Satuan Siber TNI AD

Satuan Siber TNI AD merupakan organisasi yang bertugas menyelenggarakan kegiatan dan operasi siber di lingkungan TNI AD dalam rangka mendukung tugas pokok TNI.

Peneliti melakukan wawancara, melakukan observasi dan mengambil dokumentasi untuk mengetahui bagaimana pandangan *informan* mengenai perkembangan organisasi Satuan Siber TNI AD. Peneliti melakukan wawancara dengan *Informan* A, responden menyatakan bahwa:

"Satuan Siber TNI AD saat ini masih berupa organisasi tugas, di mana pembentukannya adalah tuntutan zaman seiring dengan tumbuhnya masyarakat informasi yang dinamis dan cepat. Keterlambatan informasi berdampak kepada pembiaran ancaman dan akhirnya akan memberikan kesan pembiaran terhadap seluruh ancaman siber yang berpotensi lebih banyak di masa yang akan mendatang".

Koleksi Perpustakaan Universitas Terbuka

Responden mengaku bahwa Satuan Siber TNI AD belum terbentuk menjadi satuan kerja yng memiliki fungsi dan tugas yang dilindungi oleh ketentuan yang berlaku di TNI AD. Untuk memperkuat pandangan *Informan* A maka peneliti melakukan triangulasi dengan mewawancarai *Informan* B yang bertugas sebagai Kasipamops Satgas Siber TNI AD menyatakan bahwa:

"Satuan Siber TNI AD saat ini merupakan satuan tugas (Satgas) yang membantu organisasi dalam menagani isu-isu terkait dengan TNI AD yang viral di media sosial yang bermuatan sentimen negatif. Saat ini Satgas Siber TNI AD banyak terlibat dalam menangani insiden informasi yang ditujukan kepada TNI AD sehingga memberikan respon cepat dan pelaporan tindak lanjut dan hasilnya kepada pimpinan TNI AD".

Informan C menyatakan bahwa:

"Satuan Siber adalah satuan tugas yang dibentuk untuk menghadapi kejahatan siber. Satuan Siber yang ada saat ini adalah masih dalam tahap pembangunan baik infrastruktur dan kemampuan SDM, dibutuhkan percepatan untuk mengejar ketertinggalan terhadap keamanan informasi".

Informan D menyatakan bahwa:

"TNI AD belum mempunyai satuan siber, yang ada hanyalah dalam bentuk Satgas Siber yang melakukan pengamanan berita dan kegiatan di dunia maya. Pengamanan data elektronik maupun aset infrastruktur kritis belum dilakukan karena keterbatasan fungsi".

Informan G yang bertugas sebagai Dantim Komed 1.B menyatakan bahwa:

"Satuan Siber TNI AD berada langsung di bawah pimpinan Angkatan Darat yang berfungsi untuk melakukan *monitoring* dan penelusuran serta melakukan penindakan tentang kejahatan siber yang ditujukan kepada TNI AD. Dan perlu adanya peningkatan karena saat ini hanya melakukan *monitoring* dan melakukan penutupan akun dengan lapor konten karena sarana pendukung lainnya yang belum ada".

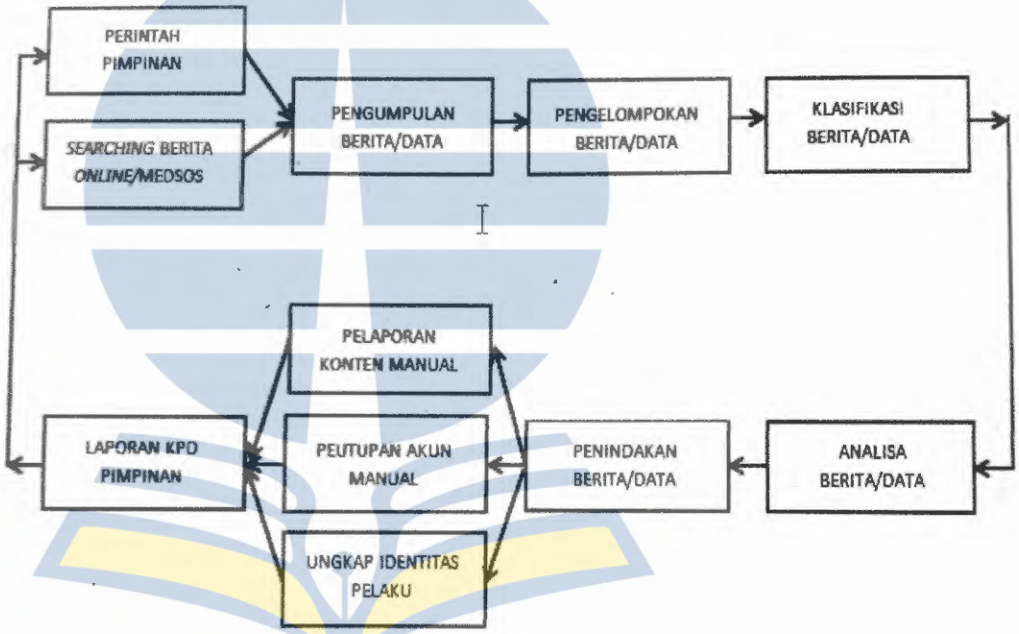
Koleksi Perpustakaan Universitas Terbuka

Selain itu peneliti melakukan wawancara dengan *informan* dari Spamad sebagai satuan yang me*monitoring* kegiatan Satgas Siber yakni *Informan* H dan I. *Informan* H menyatakan bahwa:

"Satuan Siber mengemban tugas dari institusi TNI AD terhadap ancaman kejahatan siber. Dengan berkembangnya teknologi, maka diperlukan langkah antisipasi untuk menghadapi segala bentuk ancaman".

Informan I Menyatakan bahwa:

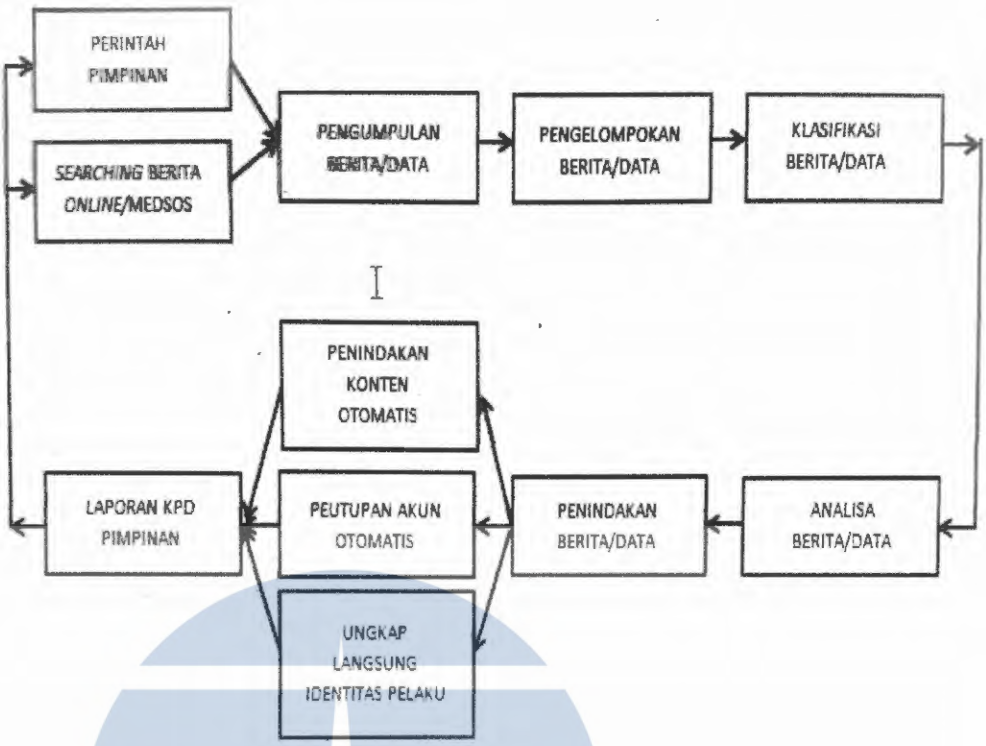
"Satuan Siber yang berada dibawah institusi TNI AD yang berfungsi sebagai satuan *offensif* dan *defensif* terhadap tindakan siber yang juga berguna untuk menghadapi ancaman *proxy war*".



Bagan 4.2
Mekanisme *Monitoring* Berita *Online*/Medsos
Dalam Fungsi *Defence* Satuan Siber TNI AD

Koleksi Perpustakaan Universitas Terbuka

48794.pdf



Bagan 4.3
Mekanisme *Monitoring* Berita *Online*/Medsos
Dalam Fungsi *Offence* Satuan Siber TNI AD

Berdasarkan bagan mekanisme di atas, perbedaan mendasar cara penanganan berita *hoax* saat ini dan setelah peningkatan fungsi (*offence*) adalah terletak pada tahap penindakannya di mana saat ini prosedur penindakan dilakukan secara *manual* yaitu dengan cara berkoordinasi dengan POLRI untuk menangkap dan menghukum pelaku kejahatan siber, membuat laporan resmi kepada penyedia aplikasi untuk menghapus konten *hoax* dan melaporkan akun palsu kepada Kemenkominfo untuk dilaksanakan pemblokiran akun tersebut, sedangkan prosedur penindakan secara *offence* dilakukan dengan cara melaksanakan serangan siber kepada akun palsu tersebut melalui kegiatan pengerusakan akun melalui virus,

Koleksi Perpustakaan Universitas Terbuka

49794.pdf

pengambil alihan akun dan penghapusan akun, sedangkan pelaku kejahatan sibernya mendapat serangan psikologi siber dengan memblokade seluruh aktivitas *online*nya serta membuka identitas yang bersangkutan kepada publik, sehingga selain *hacker* tersebut mendapatkan sanksi hukum, ia juga akan memperoleh sanksi sosial dari masyarakat.

Informasi mengenai faktor penghambat peningkatan fungsi Satuan Siber TNI AD :

Satuan Siber TNI AD yang ada saat ini masih terbatas pada fungsi pertahanan dan *monitoring* saja. Tentu terdapat faktor-faktor yang mempengaruhi alasan masih terbatasnya fungsi Satuan Siber TNI AD.

Peneliti melakukan wawancara, melakukan observasi dan mengambil dokumentasi untuk mengetahui bagaimana pandangan *informan* mengenai peran Satuan Siber TNI AD. Peneliti melakukan wawancara terbatas hanya terhadap perwira di Satuan Siber TNI AD juga Spamad. Wawancara pertama dilakukan terhadap *Informan* A, responden menyatakan bahwa:

"Pembentukan Satuan Siber sebagai satuan kerja masih dalam tahap kajian dan belum memberikan kontribusi memadai dalam merespon ancaman siber secara infrastruktur dan aplikasi. Upaya dalam lingkungan TNI AD kurang mendapatkan respon dari pimpinan yang berdampak pada keterlambatan pembentukan organisasi dan respon kegiatan. Faktor penghambat terhadap peningkatan fungsi Satuan Siber TNI AD antara lain adalah tingkat kepercayaan yang kurang dalam tataran pimpinan. Para pimpinan mempertanyakan bukti nyata adanya serangan siber secara infrastruktur kepada TNI AD. Kesadaran bahwa kejahatan siber telah mengancam belum nyata. Padahal pada April 2017 seluruh sistem informasi TNI AD dimatikan agar tidak diserang

Koleksi Perpustakaan Universitas Terbuka

Ransomware Wannacry. Seolah ini langkah tepat, tapi dalam konteks adanya serangan, bagaimana mau menang menghadapi serangan, jika personel sistem informasinya saja sudah mati sebelum adanya serangan".

Dalam pandangannya, *Informan* A juga memberikan komentar terhadap harapan peningkatan fungsi Satuan Siber TNI AD kedepannya, yakni:

"Harapan saya, Satuan Siber ke depannya adalah pelaksana fungsi militer khusus yang setara dengan keberadaan pasukan khusus yang memiliki kecakapan tinggi dalam peperangan dengan taktik non konvensional untuk itu faktor-faktor yang menjadi hambatan seperti keterbatasan alokasi dana dan SDM perlu segera diperbaiki".

Informan B menyatakan bahwa:

"Menurut saya satgas saat ini belum mampu secara maksimal dalam menghadapi kejahatan siber dikarenakan keterbatasan fungsi yang ada. Sehingga perlu menjadi Satuan Siber yang memiliki fungsi maksimal guna memberikan perlindungan dengan segala sumberdaya yang dimiliki terhadap aset di institusi TNI AD. Serta menjadi respon terdepan terhadap serangan kejahatan siber di mana selanjutnya dapat melakukan forensik *digital* dan melakukan pemulihan terhadap sistem informasi sendiri, hambatan yang terbesar adalah menurut saya adanya birokrasi yang lambat antar satuan dan kepentingan masing-masing pimpinan".

Informan C menyatakan bahwa:

"Satuan Siber saat ini perlu adanya koordinasi dan korelasi internal satuan. Yakni Satuan Siber TNI AD, Infohlatad, Dithubad, Dispenad untuk menentukan kebijakan dan langkah-langkah penanganan dalam respon cepat terhadap kejahatan siber. Sehingga kedepannya Satuan Siber TNI AD mampu menjawab dan menghadapi ancaman dari berkembangnya teknologi. Memiliki infrastruktur dan sumberdaya manusia yang cakap. Perlu juga adanya pelatihan berkelanjutan terhadap personel siber untuk menyesuaikan dengan keadaan saat ini, selain itu kurangnya koordinasi lintas sektoral dan instansi sehingga menghambat penanganan jika terjadi insiden siber. Perlunya inter operabilitas semua sektor yang bergerak dalam teknologi informasi karena merupakan tanggung jawab bersama".

Koleksi Perpustakaan Universitas Terbuka

Informan G menyatakan bahwa:

"Satuan Siber TNI AD perlu ditingkatkan fungsinya dengan dukungan segala bidang aspek agar mampu mendata serta mencari dan menghadapi sumber atau pelaku kejahatan siber. Di antaranya aspek persetujuan pimpinan yang sampai saat ini cenderung sulit memberikan ijin terbentuknya Satuan Siber TNI AD dengan fungsi khusus, karena dianggap belum ada perang secara nyata yang ditimbulkan. Satuan Spamad bertindak hanya sebagai *monitoring* saja, untuk itu diharapkan dengan adanya peningkatan fungsi maka Spamad juga dapat ikut untuk me*monitoring* dan memfasilitasi kebutuhan informasi guna menghadapi kejahatan siber. Lemahnya hukum juga menjadi faktor penghambat, tanpa adanya payung hukum yang jelas maka prajurit Satuan Siber TNI AD akan terhambat pergerakanya karena takut bahwa apa yang dilakukan melanggar aturan .

Informan H menyatakan bahawa:

"Satuan Siber yang dapat berintegrasi dengan satuan lain dan dapat menangani segala bentuk kejahatan siber, faktor penghambatnya adalah minimnya sumberdaya manusia yang memiliki kemampuan khusus dan di atas rata-rata dalam bidang siber serta keterbatasan anggaran guna membuat infrastruktur yang mumpuni".

Dari berbagai pandangan *informan* terkait pentingnya peningkatan fungsi Satuan Siber TNI AD juga faktor penghambat dapat disimpulkan bahwa kejahatan siber yang marak saat ini khususnya terhadap institusi TNI AD perlu suatu Satuan Siber yang memiliki fungsi tidak hanya *monitoring* tetapi menghadapi serta mengungkap kejahatan siber baik itu program maupun pelakunya. Diperlukan juga integrasi antar satuan intelijen dan pendukung guna membentuk Satuan Siber yang handal dan mumpuni. Untuk lebih jelasnya dapat dilihat pada Tabel 4.4:

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Konsep Faktor Penghambat Peningkatan Fungsi Satuan Siber TNI AD	
Dimensi	1. Keterbatasan sarana dan prasarana 2. SDM terbatas 3. Hukum yang lemah 4. Birokrasi lambat
Sebelum adanya Satuan Siber TNI AD	Tidak adanya satuan secara khusus untuk melakukan *monitoring* dan pertahanan terhadap kejahatan siber
Setelah adanya faktor hambatan peningkatan fungsi Satuan Siber TNI AD	Melakukan *monitoring* dan pertahanan terhadap segala aksi kejahatan siber yang ditujukkan kepada Institusi TNI AD. Hanya masih bersifat terbatas baik itu terkendala di infrastruktur maupun sumberdaya manusia. Namun diharapkan ke depannya Satuan Siber yang memiliki keahlian seperti pasukan khusus dan menjadi organisasi resmi dengan dukungan penuh dari pimpinan TNI AD dari berbagai aspek pendukung.(*ofensif* dan *defensif*)

Tabel 4.4
Konsep Pandangan Terhadap Faktor Penghambat
Peningkatan Fungsi Satuan Siber TNI AD

C. Pembahasan

1. Pengaruh kejahatan siber terhadap fungsi Satuan Siber TNI AD

Kejahatan siber merupakan salah satu bentuk baru jenis kejahatan. Kejahatan berkembang terus menerus mengikuti zaman dan teknologi, yang saat ini telah masuk ke dalam institusi-institusi keamanan negara seperti TNI AD. Pembentukan Satuan Siber TNI AD erat kepentingannya guna menghadapi ancaman serangan kejahatan siber. Menurut Haris (2010), kejahatan siber merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut:

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

a. *Unauthorized access* (dengan maksud untuk memfasilitasi kejahatan).

b. *Unauthorized alteration or destruction of data.*

c. Mengganggu atau merusak operasi komputer.

d. Mencegah atau menghambat akses komputer.

Pelaku kejahatan siber adalah perorangan maupun organisasi siber yang berasal dari masyarakat sipil maupun militer yang melakukan kejahatan siber tersebut atas dasar keinginan pribadi atau justru karena mendapatkan bayaran dari pihak lain. Pada umumnya, masyarakat sipil yang melakukan kejahatan siber didasari oleh keinginan untuk menembus sistem keamanan suatu piranti lunak komputer suatu instansi yang pada akhirnya akan menimbulkan kepuasan tersendiri bagi pelaku, selain itu adanya keinginan untuk memanipulasi data yang digunakan untuk mengambil keuntungan pribadi seperti contoh memanipulasi data kartu kredit, ATM dan lainnya, serta hal yang sedang marak terjadi adalah menyebarluaskan berita *hoax* melalui media sosial dengan menggunakan akun palsu dengan tujuan untuk mendiskreditkan individu/lawan maupun institusi tertentu, bahkan saat ini aktivitas penyimpangan melalui media sosial juga digunakan untuk kampanye hitam selama kegiatan Pemilu di Indonesia. Di sisi lain, masyarakat militer, atau lebih sering disebut prajurit militer negara lain, teroris maupun pemberontak menggunakan teknologinya untuk melakukan kejahatan siber terhadap negara yang menjadi

Koleksi Perpustakaan Universitas Terbuka

44794.pdf

sasarannya. Berbeda dengan kejahatan siber yang dilakukan oleh masyarakat sipil, kejahatan siber yang dilakukan oleh militer lebih ke arah upaya penggunaan teknologi dalam pengendalian Alutsista dan perangkat komputer sistem pertahanan negara lain hingga upaya menghancurkan suatu negara dengan peperangan yang memakan banyak korban hanya dengan menggunakan perangkat berteknologi tinggi.

Dengan meningkatnya kejahatan siber di Indonesia dan telah menyerang di berbagai segi bidang kehidupan di tanah air, maka dapat dikatakan bahwa setiap orang di negara ini berpotensi menjadi korban dari jenis kejahatan model baru ini, baik pejabat maupun bukan pejabat, baik individu maupun organisasi dapat serta merta menjadi korban dari kejahatan siber apabila tidak memiliki kesadaran akan pentingnya mengamankan dan meng-enkripsi jaringan komputer dan media sosialnya. Korban paling sederhana dari kejahatan siber adalah hilangnya privasi terhadap akun media sosial miliknya akibat dari adanya *hacker* yang menyerang dan menyabotase akun tersebut, sedangkan korban luasnya adalah timbulnya perang siber antar negara yang dilakukan oleh organisasi *hacker* atau teroris dengan memanfaatkan jaringan komputer dalam pengendalian Alutsista, sehingga dapat dikatakan akan terjadi perang nyata yang dikendalikan secara tidak kasat mata. Dengan memperhatikan besarnya tingkat bahaya yang akan ditimbulkan, maka kejahatan siber tidak dapat dikelompokkan

Koleksi Perpustakaan Universitas Terbuka

48794.pdf

berdasarkan korbannya, korban individu maupun organisasi sipil apabila terjadi dalam jumlah yang banyak dapat mengancam keberlangsungan suatu bangsa, demikian juga bila korbannya adalah prajurit atau institusi *militer yang bila terjadi dalam jumlah* besar maka akan membahayakan keamanan dan pertahanan negara. Besarnya akibat yang ditimbulkan oleh kejahatan siber sepatutnya disikapi dengan peningkatan kepedulian terhadap keamanan semua perangkat elektronik yang bekerja dengan menggunakan jaringan komputer/internet dan meng-enkripsi akun pribadi serta merubah pengaturan pabrik agar tidak mudah disabotase oleh pelaku kejahatan siber. Namun, sebagaimana yang terjadi dewasa ini, banyak orang yang kurang menyadari kejahatan model baru ini akibat keberadaannya yang tidak nyata dan tidak kasat mata membuat masyarakat cenderung ingin bukti kejadian terlebih dahulu baru mengambil langkah protektif. Apabila hal ini diterapkan dalam institusi TNI AD, bereaksi setelah terjadinya serangan siber dapat mengakibatkan bobolnya jaringan komputer sistem pertahanan negara yang mengakibatkan terbukanya rahasia negara bidang pertahanan dan sabotase atas sistem kendali senjata otomatis. Untuk itu keberadaan Satuan Siber TNI dan TNI AD sangat diperlukan untuk menangkal tren ancaman siber yang menyerang ke dalam sistem pertahanan negara kita.

Hal tersebut sesuai dengan apa yang sedang dihadapi TNI AD, kejahatan siber memiliki banyak faktor ancaman kepada

Koleksi Perpustakaan Universitas Terbuka

46794.pdf

institusi TNI AD, ancaman kejahatan siber sudah sangat menganggu institusi tersebut. Di antaranya adanya sistem informasi yang tidak diamankan secara baik sehingga mudah disabotase oleh para *hacker* tersebut. Kegiatan mata-mata sudah banyak masuk ke area intelijen institusi TNI AD melalui celah keamanan yang terdapat dalam sistem informasi TNI AD untuk mengakses data rahasia negara. Pencurian data yang mudah menjadi faktor ancaman yang juga perlu diantisipasi. Karena Institusi TNI AD memiliki banyak rahasia keamanan negara dan hampir semua perangkat Alutsista saat ini berbasiskan komputer.

Thomas Wingfield dari Marshall Center dalam forum yang dihadiri oleh 15 pakar hukum dari sekitar 12 negara di Jerman berhasil menyusun buku panduan hukum internasional bagi penerapan perang *cyber*. Wingfield mengungkapkan bahwa sebuah serangan *cyber* dapat dibalas dengan serangan militer konvensional. "Jika sudah mencapai taraf serangan bersenjata, dalam arti setara dengan invasi menggunakan *tank* atau blokade laut, setara dengan serangan terhadap warga atau serdadu sebuah negara, hukum internasional mengizinkan negara bersangkutan, bereaksi segera, sepihak dan secara militer, untuk mengakhiri ancamannya". Wingfield memberikan contoh insiden yang terjadi pada bulan Oktober 2007 di Afrika Selatan. Ketika itu, sebuah meriam penangkis serangan udara buatan perusahaan Jerman, Oerlikon lepas kendali dan menembak membabi buta ke kawasan

Koleksi Perpustakaan Universitas Terbuka

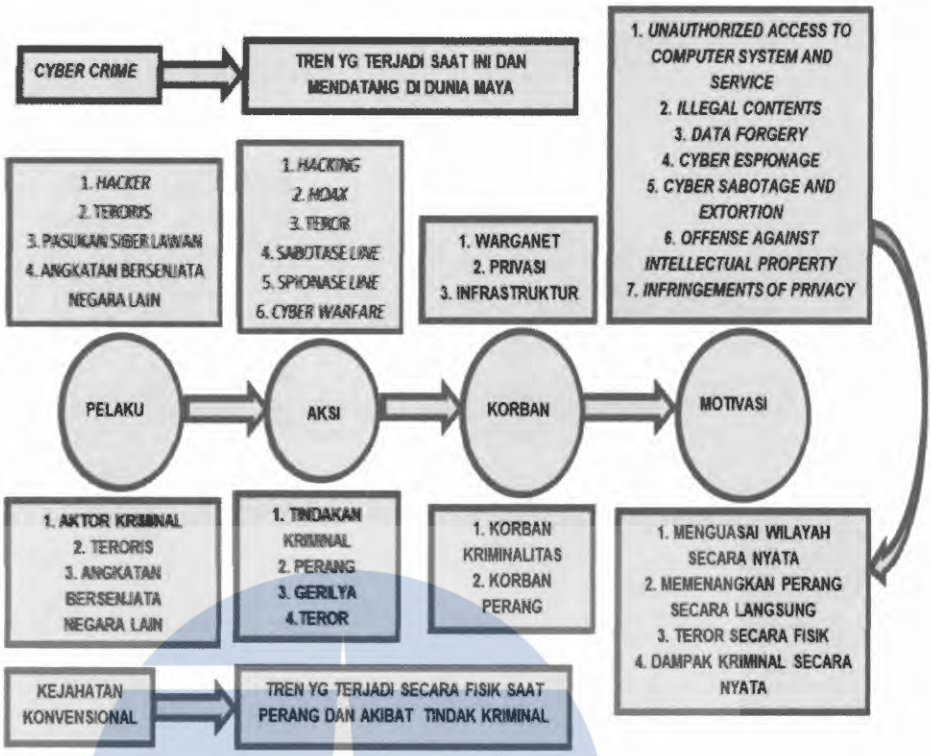
43794.pdf

sekitarnya. Akibat insiden tersebut sembilan serdadu tewas dan 14 luka parah. Penyelidikan lanjutan atas kasus tersebut diketahui bahwa penyebabnya adalah kesalahan perangkat lunak yang tidak lazim dan bukan manipulasi oleh virus *computer*, melainkan *hacker* yang mengambil alih kendali atas Alutsista.

Pada Tahun 2010, Serangan *worm "Stuxnet"* sukses menyabotase instalasi pemerkaya Uranium Natanz milik Iran. Akan tetapi perangkat pengendali elektronik yang dimanipulasi oleh *worm Stuxnet* itu, bukan hanya dipasang di Iran, melainkan juga di banyak industri di berbagai negara. Bagi pakar keamanan IT dari Finlandia, Mikko Hypponen serangan terhadap sistem pengendali elektronik menunjukkan kualitas risiko baru. "Jika *Stuxnet* dapat menginfeksi seperti itu, berarti ini revolusi besar berkaitan risiko yang mencemaskan. Sebab semua hal dikendalikan sistem semacam itu. Kita memiliki infrastruktur yang kritis. Pabrik, pembangkit listrik, pabrik kimia atau instalasi pengolah makanan, semua dikendalikan lewat komputer," tutur pakar keamanan IT Hypponen. Komputer juga mengendalikan sistem persenjataan konvensional militer. Percepatan gerakan di medan pertempuran, memaksa logika militer menerapkan lebih banyak otomatisasi.

Koleksi Perpustakaan Universitas Terbuka

48794.pdf



Bagan 4.4
Perbandingan Karakteristik Kejahatan Siber
dan Kejahatan Konvensional

Berdasarkan bagan di atas dapat diketahui perbandingan antara kejahatan siber dengan kejahatan konvensional baik ditinjau dari segi pelaku, aksi, tempat maupun motivasi. Sebagaimana uraian di atas pelaku kejahatan siber dengan kejahatan konvensional dibedakan dari lingkungan tempat mereka beraksi, pelaku kejahatan siber melakukannya melalui jaringan komputer, sedangkan pelaku kejahatan konvensional melalui kontak fisik. Didasari perbedaan tersebut, maka untuk kejahatan siber memunculkan istilah *hacker* dan pasukan siber. Aksi kejahatan siber dilaksanakan melalui jaringan komputer/*online* berupa kegiatan-kegiatan *hacking*, teror jaringan, *hoax*, sabotase jaringan, spionase jaringan dan paling puncak adalah perang siber,

Koleksi Perpustakaan Universitas Terbuka

49794.pdf

sedangkan aksi kejahatan konvensional dilaksanakan melalui kontak fisik saat terjadinya tindakan kriminal, teror, perang dan gerilya. Akibat dari ke dua jenis kejahatan ini sama-sama menimbulkan korban baik secara individu maupun organisasi/instansi, namun pada kejahatan siber memiliki kekhususan karena selain dapat menimbulkan korban secara fisik (bila terjadi alih fungsi Alutsista saat perang siber), juga menimbulkan korban warganet, privasi dan hancurnya infrastruktur jaringan. Dari segi motivasi yang mendorong terjadinya kejahatan siber dan kejahatan konvensional saling berhubungan. Pada kejahatan siber, motivasi yang timbul adalah memasuki jaringan komputer lawan untuk mencuri data, membuat konten ilegal, memalsukan data dokumen penting untuk keuntungan pribadi, kegiatan mata-mata, sabotase jaringan, meniru ilmu dan data milik orang lain secara *online*, namun dewasa ini motivasi dalam melakukan kejahatan siber pada akhirnya akan meningkat dan serupa dengan kejahatan konvensional manakala telah terjadi perang siber, hal tersebut dapat berupa motivasi untuk menguasai wilayah, melaksanakan teror, tindakan kriminal dan memenangkan perang dengan menggunakan pengambilalihan Alutsista dan sistem pertahanan suatu negara.

Untuk menghadapi faktor-faktor ancaman tersebut di lingkungan TNI AD, maka Satuan Siber TNI AD memerlukan peningkatan fungsi berupa infrastruktur komunikasi berbasis

Koleksi Perpustakaan Universitas Terbuka

internet yang terintegrasi yang disebut dengan istilah pengembangan sistem informasi *level* ke-2 yaitu melalui mekanisme penanganan informasi internet sehingga membentuk masyarakat informasi siber di lingkungan TNI AD dengan melibatkan empat satuan, yaitu Dithubad sebagai penyedia infrastruktur dan Disinfolahtad sebagai penyedia layanan sistem informasi, serta Pusintelad dan Dispenad sebagai badan pelaksana pusat yang mengelola informasi sebagai subyek utama, sedangkan apabila kemampuan Satuan Siber TNI AD telah dilengkapi dengan fungsi *ofensif,* maka akan diperkuat oleh Siber Kopassus sebagai badan pelaksana fungsi serangan siber (*ofensif*). Selain itu, terdukungnya sirkulasi informasi yang aman dan berdaya guna bagi pengambilan keputusan pimpinan TNI AD secara cepat diperlukan sistem informasi (aplikasi) yang merupakan pengadaan TNI AD dengan biaya dan perawatan yang relatif mahal. Disampaikan bahwa aplikasi sistem informasi bernama *Intelligence Media Monitoring* (IMM) yang telah dimiliki TNI AD sejak Tahun 2014 mitra PT. Eb Desk, dengan kondisi sebagai berikut:

a. Saat ini sumberdaya *Intelligence Media Monitoring* (IMM) yang dimiliki Pusintelad (bernama *Open Source Intelligent atau OSINT*), Disinfolahtad dan Pusterad merupakan tiga aplikasi yang tertanam pada *server* fisik di ketiga satuan yang masing-masing berdiri sendiri dan tidak dapat bekerja

Koleksi Perpustakaan Universitas Terbuka

bersama (kolaborasi). Sayangnya di antara ketiga *server* tersebut aplikasinya sama dengan bentuk *output* (produk) yang disesuaikan dengan kebutuhan satuan masing-masing. Kondisi ini dapat dikatakan dengan *overlaping* sumberdaya yang dapat diatasi dengan pengelolaan akses.

b. Sesuai Surat Danpusintelad Nomor B/601/VI/2018 tanggal 29 Juni 2018 telah diajukan permohonan aplikasi *Intelligence Social Media Robot* (ISR) untuk satuan intelijen, di mana dalam paket pengadaan tersebut adalah sumberdaya yang salah satunya dibangun oleh PT. Eb Desk dan mencakup tiga sumberdaya baru dan satu *update* aplikasi *OSINT*. Bagi Pusintelad yang saat ini telah memiliki tiga aplikasi dari PT. Eb Desk, yakni *OSINT*, *Video Conference* dan sarana pengirim pesan Security Message management (SMM), maka akan memiliki sebanyak enam aplikasi hasil pengadaan berikutnya.

c. Berkaitan dengan mahalnya sistem aplikasi tersebut dan kebutuhan kolaborasi kerja sistem informasi level ke-2 yang diistilahkan dengan *smart city* (di lingkungan Kemdagri), maka di kemudian hari akan dilakukan pengadaan sistem informasi bagi Satuan Siber TNI AD dengan *platform* yang sama, sehingga kolaborasi akan memberikan dukungan *big data* yang berdaya guna. Pengadaan sistem informasi dengan *platform* berbeda akan memberikan *overlaping*

Koleksi Perpustakaan Universitas Terbuka

sumberdaya dan yang lebih penting dalam pengembangan *level* ke-2 tidak akan dapat dilaksanakan.

d. Untuk perangkat Global System for Mobile Communications (GSM), 3G dan 4G *Intercept* serta perangkat *Location Base Service* memanfaatkan sumberdaya tersebut secara bersama dengan Pusintelad mengingat frekuensi kebutuhan siber yang relatif belum tinggi. Satuan Siber TNI AD juga harus sesegera mungkin memiliki perangkat *Threat Enhancement Analytical Platform* (TEA) yang berfungsi sebagai perangkat untuk mendeteksi, memberitahukan dan memblokir ancaman siber dari lawan.

e. Melaksanakan pelatihan siber secara bergantian untuk percepatan penguasaan ilmu dan teknik siber tanpa mengganggu operasional tugas Satuan Siber TNI AD, di sisi lain diikuti dengan pengadaan renovasi ruangan dan perangkat pendukung untuk *Defence/Security Operation Centre* (SOC).

Saat ini pembentukan Satuan Siber sebagai satuan kerja masih dalam tahap kajian dan belum memberikan kontribusi memadai dalam merespon ancaman siber secara infrastruktur dan aplikasi. Satuan Siber TNI AD perlu menjadi satuan siber yang memiliki kecakapan khusus baik itu dari aspek sumberdaya manusia maupun perangkatnya. Satuan siber yang ada saat ini

Koleksi Perpustakaan Universitas Terbuka

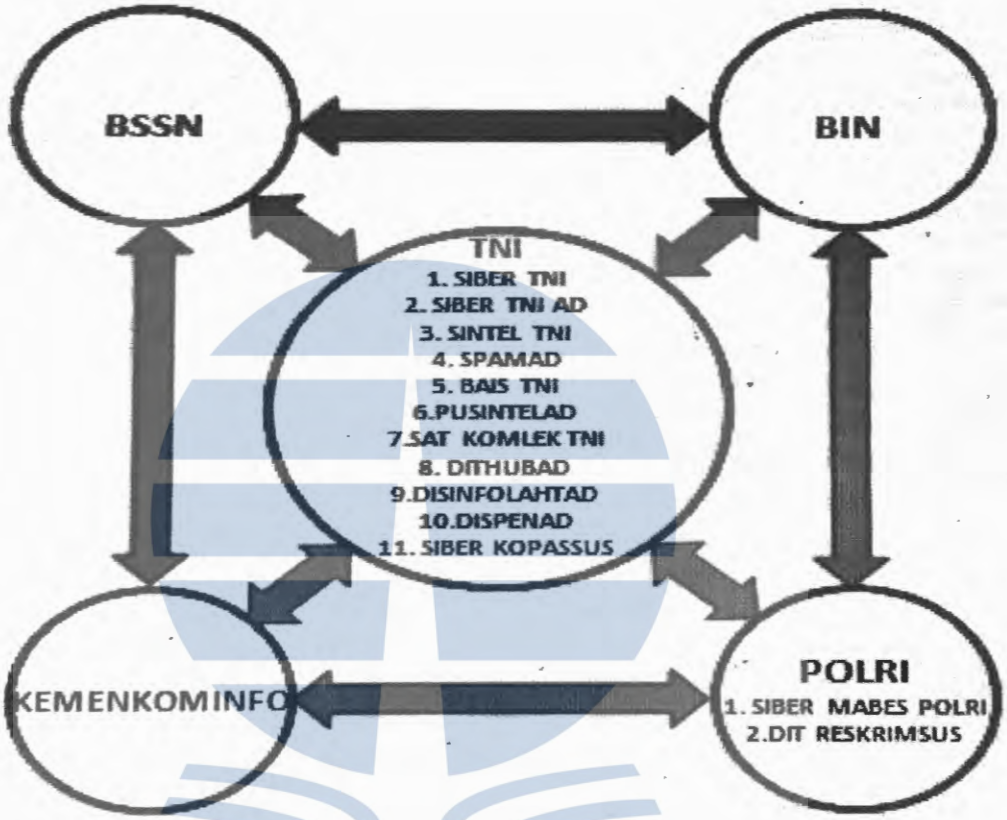
perlu adanya koordinasi dan korelasi intern satuan dengan cara validasi organisasi satuan pendukung, yaitu Satuan Siber TNI AD, Disinfohlatad, Dithubad, Dispenad, Siber Kopassus dan PII Pusintelad untuk menentukan kebijakan dan langkah-langkah penanganan dalam respon cepat terhadap kejahatan siber. Peningkatan fungsi diharapkan tidak hanya sebagai pertahanan saja melainkan mampu menghadapi dan melawan segala bentuk kejahatan siber yang menyerang TNI AD.

Hal ini sejalan dengan hasil kegiatan *Cybersecurity Multy-Stakeholder Meet-Up* yang dilaksanakan di Balai Roebiono Kertopati Badan Siber dan Sandi Nasional (BSSN) pada tanggal 24 September 2018. Kegiatan yang dibuka oleh Kepala Badan Siber dan Sandi Negara, Mayjen TNI (Purn) Dr. Joko Setiadi, M.Si ini diikuti oleh 81 orang praktisi bidang teknologi informasi (siber) instansi pemerintah, ekonomi kreatif, pengemban infrastruktur kritik nasional dan komunitas. Kegiatan ini merupakan forum *sharing* dan berbagi pengalaman dalam bidang siber, sehingga akan dilaksanakan secara periodik dengan target terdekat dalah pelaksanaan Pemilu 2019 yang berlangsung secara sukses. Selain menampung aspirasi para praktisi siber, BSSN sebagai pembina keamanan siber di Indonesia sangat mendambakan memiliki *Security Operation Centre* (SOC) yang mampu memberikan laporan insiden kritik nasional. Hal tersebut merupakan tindak lanjut arahan Presiden Joko Widodo dalam mensinergikan potensi

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

siber di Indonesia. Kolaborasi dan kerjasama menjadi kata kunci yang harus diikuti dalam merespon ancaman siber, mulai dari serangan infrastruktur sampai ancaman terhadap mentalitas generasi penerus.



Bagan 4.5
Alur Kolaborasi/Sinergitas Satuan Siber di Indonesia

Seperti penjelasan di atas, guna meningkatkan kemampuan satuan siber dalam mengatasi kejahatan siber yang semakin meningkat jumlahnya dan semakin beraneka ragam modus operandi dan tekniknya, maka perlu segera terbentuk sistem informasi *level* ke-2. Hal tersebut akan membutuhkan tingkat sinergitas dan kolaborasi seluruh satuan siber, instansi intelijen dan persandian serta lembaga penegak hukum di Indonesia. Sesuai

Koleksi Perpustakaan Universitas Terbuka

bagan di atas, seluruh alur bersifat *report and respone.* Satuan Siber dan Intelijen jajaran TNI dapat melaporkan penutupan akun dan pemblokiran konten secara *online* kepada Kemenkominfo, pengajuan sistem sandi/enkripsi tingkat lanjut kepada BSSN, permohonan pengungkapan dan pelacakan pelaku kepada BIN dan pelaporan pelaku kejahatan siber kepada POLRI. Kemenkominfo dapat meminta bantuan TNI terkait serangan siber yang dilakukan oleh pasukan siber negara lain, meminta bantuan siber dan persandian kepada BSSN dan melaporkan pelaku kepada POLRI. POLRI dapat bekerjasama dengan TNI bila serangan siber mengancam kedaulatan negara, mengajukan pemblokiran akun dan konten negatif kepada Kemenkominfo dan meminta bantuan BIN bila pelaku terindikasi sebagai agen mata-mata dari lawan/musuh. BSSN dapat bekerja sama dengan TNI terkait tren militerisasi internet, dengan BIN terkait agen mata-mata dari lawan/musuh serta Kemenkominfo terkait pemblokiran akun dan konten negatif. BIN bekerjasama dengan TNI terkait ancaman siber dari militer negara lain, dengan BSSN terkait sistem dan peralatan siber dan persandian serta dengan POLRI terkait pelaku kejahatan siber.

2. Kendala Satuan Siber TNI AD dalam mengungkap kejahatan siber

Peningkatan fungsi Satuan Siber TNI AD dihadapkan pada beberapa faktor penghambat, yang berdasarkan hasil wawancara terhadap *informan* yang berada didalam satuan tersebut yaitu

Koleksi Perpustakaan Universitas Terbuka

peningkatan fungsi dan pelaksanaanya dihadapi oleh faktor-faktor yang menjadi penghambat yaitu:

a. Keterbatasan kemampuan sumberdaya manusia di bidang Siber.

b. Keterbatasan sarana dan prasarana kepemilikan alat canggih berbasis IT dan teknologi guna menghadapi serangan kejahatan siber.

c. Masih lemahnya hukum perundang-undangan di Indonesia, termasuk peraturan dan ketentuan hukum yang mengatur Satuan Siber TNI AD.

d. Masih terbatasnya koordinasi lintas sektoral antar satuan pendukung guna menghadapi kejahatan siber.

Menghadapi cepatnya kemajuan teknologi *internet* yang seiring dengan semakin majunya teknik yang digunakan untuk melakukan kejahatan siber saat ini menimbulkan efek terhadap kegiatan pengamanan di bidang jaringan komputer. Saat ini fokus TNI AD masih berupaya pada peningkatan *level* Alutsista yang dimiliki dari *manual* menjadi otomatis. Hal ini tidak diikuti oleh pembentukan pasukan khusus siber yang memiliki kemampuan lengkap, yaitu memiliki kemampuan *defensif*/menangkal serangan siber lawan dan mampu dengan segera memperbaiki jaringan yang ditembus lawan serta melakukan perawatan jaringan dan juga memiliki kemmpuan *ofensif* siber untuk menyerang lawan dan mengungkap identitas *hacker* tersebut serta tak kalah penting

Koleksi Perpustakaan Universitas Terbuka

melakukan serangan balik kepada perangkat elektronik yang dimiliki lawan. Untuk memiliki kemampuan seperti itu dibutuhkan sumberdaya manusia yang memiliki kemampuan dan pengetahuan di tiga bidang yaitu siber, persandian dan intelijen. Tiga kemmpuan ini saling berkaitan dan saling mendukung, sehingga bila ingin membentuk sumberdaya siber yang mumpuni harus mengusai pengetahuan teknik jaringan komputer (siber) tingkat lanjut, mengikuti pendidikan prajurit intelijen untuk mengetahui langkah langkah yang harus dilakukan dalam menyelesaikan permasalahan dan menyiapkan data yang dibutuhkan pimpinan TNI AD serta mengikuti pendidikan ahli sandi untuk meningkatkan kepedulian terhadap keamanan jaringan yang dilakukan dengan meng-enkripsi tidak hanya data/*file* melainkan juga saluran/jaringan yang menjadi wadah pengiriman dan penerimaan data/*file* tersebut.

Dalam Satuan Siber TNI AD terjadi *gap* yang cukup signifikan antara kapasitas sumberdaya manusia prajurit siber yang ideal dengan yang dimiliki saat ini. Saat ini Satuan Siber TNI AD terdiri dari 55 personel di mana setiap personel yang direkrut berdasarkan atas kemampuan/pengetahuan IT yang dimiliki atas rekomendasi dari atasannya, sehingga kenyataan yang terjadi pengetahuan setiap prajurit siber antar satu orang dengan orang lainnya tidak memiliki standar kemampuan yang sama, hasilnya tentu saja berdampak pada kinerja organisasi secara umum. Di samping itu, dengan alasan mengutamakan kemampuan dan

Koleksi Perpustakaan Universitas Terbuka

pengetahuan IT lanjutan tersebut menyebabkan terabaikannya kebutuhan akan kemampuan intelijen dan persandian yang seharusnya wajib dimiliki oleh personel siber TNI AD. Akibatnya, langkah-langkah penyelesaian permasalahan dan penyajian data kepada pimpinan TNI AD menjadi berbeda-beda. Sampai dengan saat ini dari 55 orang prajurit siber yang sudah memiliki kualifikasi intelijen berjumlah 16 orang yang terdiri dari 3 orang Perwira dan 13 orang Bintara, sedangkan yang memiliki kualifikasi persandian hanya berjumlah 1 orang yaitu Dansatgas Siber.

Untuk mengatasi *gap* yang cukup signifikan terkait sumberdaya manusia di Satuan Siber TNI AD, pimpinan TNI AD telah mengambil langkah-langkah kebijakan dengan mengadakan pelatihan dan penataran siber tingkat lanjut yang terbagi menjadi tiga gelombang di mana masing-masing gelombang berjumlah 30 orang, di mana kegiatan ini bekerjasama dengan PT. Pindad dan bertempat di Pindad *Cyber Learning Center* di Gedung Axa Tower lantai 37 jl. Prof. DR. Satrio No. Kav.18 Karet Kuningan, Setiabudi, Jakarta Selatan. Gelombang I dilaksanakan pada bulan Juni 2018 dan Gelombang II dilaksanakan pada bulan Agustus 2018 dimana lamanya pelatihan memakan waktu 6 minggu, sedangkan untuk Gelombang III rencana akan dilaksanakan pada Tahun 2019 setelah dilaksanakan rekuitmen personel siber tahap ketiga.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

TNI AD menyadari dan memanfaatkan perkembangan teknologi informasi saat ini dengan sebaik-baiknya, dimulai dari mengadakan pelatihan *cyber defence* yang bekerjasama dengan Pindad dan dilanjutkan pelatihan *deep offensive hacking* untuk menciptakan prajurit yang mempunyai kemampuan *cyber defence* dalam menjawab tantangan tugas pokok dan *cyber offence* untuk mempersiapkan diri dalam menghadapi pola serta bentuk ancaman siber saat fungsi Satuan Siber TNI AD sudah ditingkatkan.

Pelatihan-pelatihan siber yang dilaksanakan bertujuan untuk menyamakan kemampuan dan pengetahuan setiap personel Satuan Siber TNI AD dan juga diarahkan untuk mampu menjawab tantangan kejahatan siber di mana tren dan modus operandinya yang semakin beraneka ragam saat ini. Pelatihan-pelatihan *cyber defence* yang telah dilaksanakan yaitu:

a. *Profiling* akun *Facebook*. Pada 19 September 2018, Satuan Siber TNI AD membentuk tim *profiling* yang beranggotakan 10 orang sebagai petugas *profiling* terhadap sasaran akun *Facebook* anggota TNI AD yang diperkirakan sejumlah 350.000 orang/akun dan jika digabungkan dengan istri prajurit dapat mencapai 600.000 akun. TNI AD bekerjasama dengan PT. Eb Desk dalam memberikan pelatihan dan peminjaman sumberdaya alat dikarenakan Satuan Siber TNI AD belum memiliki perangkat *profiling*.

Koleksi Perpustakaan Universitas Terbuka

b. Manajemen akun robot. Pada tanggal 26 September 2018 diadakan pelatihan manajemen akun robot. Akun robot merupakan pasukan dalam melakukan konter opini dalam media sosial (*Twitter* dan *Facebook*). Dalam pelatihan tersebut Satuan Siber TNI AD membentuk tim robot berjumlah 10 orang untuk membuat, memberikan status layaknya pengguna *internet* dan memanfaatkannya untuk melakukan konter opini pemberitaan negatif terhadap institusi TNI AD di media sosial.

c. *Cyber patrol*. Pada tanggal 3 Oktober 2018 dilaksanakan pelatihan tentang *cyber patrol* yang merupakan metode kerja mengumpulkan sentimen isu negatif di media daring dan sosial dengan memanfaatkan aplikasi milik PT. Eb Desk. Kegiatan *cyber patrol* ini sangat bermanfaat dalam mendukung Satuan Siber TNI AD untuk menemukan berita negatif sesuai kategori.

d. *Social network analysis* (SNA). Pada tanggal 10 Oktober 2018 dilaksanakan pelatihan *social network analysis* (SNA) yang merupakan metode analisis dalam menemukan target dalam media daring dan sosial.

Di samping pelatihan untuk meningkatkan kemampuan *cyber defence*, Satuan Siber TNI AD juga bekerjasama dengan Pindad untuk meningkatkan kemampuan dan pengetahuan *cyber offence* dengan tujuan sebagai bekal pada saat kemampuan Satuan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Siber TNI AD ditingkatkan di kemudian hari. Pelatihan-pelatihan *cyber offence* yang telah dilaksanakan yaitu pelatihan *deep offensive hacking* yang dilaksanakan pada tanggal 8-12 Oktober 2018 bertempat di Pindad *Cyber Learning Center* Di Gedung Axa Tower lantai 37 jl. Prof. DR. Satrio No. Kav.18 Karet Kuningan, Setiabudi, Jakarta selatan, dengan materi pelatihan sebagai berikut:

a. *Additional introduction to linux*. Materi ini bertujuan agar personel siber mampu dalam instalasi *Linux* dan konfigurasinya dan mampu dalam menjalankan perintah-perintah dalam sistem operasi *Linux* (*command line*).

b. *Information gathering*. Materi ini bertujuan agar personel siber mampu mengumpulkan informasi mengenai sistem yang digunakan target dan melakukan identifikasi *operating system, port and service enumeration.*

c. *Vunerability identification.* Materi ini bertujuan agar personel siber mampu mengidentifikasi kerentanan dan menganalisis masalah terhadap sistem.

d. *System hacking exploiting part I.* Materi ini bertujuan agar personel siber mampu melaksanakan *password cracking, type of brute force attack* dan *over view of hash, encryption and decoding* serta mampu *dumping process, web shell, local versus remote exploit* dan *privilege escalation.*

e. *System hacking exploiting part II.* Materi ini bertujuan agar personel siber mampu menggunakan *tools metasploit*,

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

identifikasi *local file inclusion, unrestricted files upload* dan *directory traversal*.

f. *System hacking exploiting part III.* Materi ini bertujuan agar personel siber mampu melakukan *exploit vulnerable app*, mampu *common (web) bug hunting methodology, the important thing of recon in (web) bug hunting* dan melakukan *data enumeration from recon step*.

Namun masih terdapat hambatan dalam pelatihan *deep offensive hacking* yaitu personel siber tidak dilatihkan proses meretas akun sosial media yang dapat mendukung tugas pokok Satuan Siber TNI AD, melainkan hanya mempelajari tentang kerentanan sistem dan infrastruktur teknologi informasi saja. Hal ini disebabkan karena pihak Pindad menghindari terjadinya pelanggaran hukum akibat belum adanya payung hukum yang jelas untuk melaksanakan serangan siber.

Faktor lain yang menjadi penghambat dalam pelaksanaan tugas Satuan Siber TNI AD adalah keterbatasan sarana dan prasarana kepemilikan alat canggih berbasis IT dan teknologi guna menghadapi serangan kejahatan siber. Idealnya, Satuan Siber TNI AD memiliki ruangan kerja dengan konsep *Security Operation Centre* (SOC) sehingga semua perangkat elektroniknya terkoneksi dalam satu jaringan dengan tingkat pengamanan tinggi dan berlapis serta memiliki akses ke seluruh satuan siber di Indonesia baik sipil maupun militer guna terbentuk sistem informasi *level* ke-2. Di

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

samping itu, perangkat kerja dengan spesifikasi tingkat tinggi juga diperlukan untuk memfasilitasi upaya melakukan serangan siber dan di sisi lain memiliki tingkat keamanan perangkat dan jaringan yang tidak mudah ditembus oleh lawan.

Berdasarkan hasil kegiatan *Cybersecurity Multy-Stakeholder Meet-Up* yang dilaksanakan BSSN, terdapat beberapa hal yang layak untuk segera dimiliki dalam infrastruktur Satuan Siber TNI AD yaitu:

a. *Security Operation Centre* (SOC) merupakan sistem pengamanan jaringan komputer yang mampu memonitor aktivitas dan memberikan laporan jika terjadi insiden intrusi (usaha orang luar masuk ke dalam infrastruktur/jaringan komputer atau sistem informasi/Sisfo).

b. *Vulnerability assessment* merupakan usaha yang dilakukan untuk menemukan celah keamanan pada sisi sistem informasi, aplikasi yang dibangun dan metode kerja yang diawaki personel. Setiap hari lahir program jahat di komputer (*malware*) sebanyak sejuta, dan pada 2017 Indonesia merupakan negara ke dua yang mendapat serangan *malware,* setelah Cina. Kegiatan ini juga sangat berguna untuk menangkal tindakan sabotase *digital*.

c. Metode kerja *fraud* (penipuan) *security* merupakan kegiatan forensik dalam transaksi *digital*. Sebagai bagian dari kegiatan forensik *digital* yang secara khusus membuktikan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

terjadinya kejahatan siber dengan melihat aspek perilaku. Pelaku tindak kejahatan *fraud* dapat dideteksi dan ditangkal dari aspek perilaku serta pembuktian tindak pidana kejahatan terorganisasi *digital* bukan pidana umum penipuan.

d. Metode standar keamanan informasi Satuan TNI AD, seperti penerapan penyandian terhadap informasi berklasifikasi rahasia dan layanan dalam bentuk layanan informasi yang dapat diakses dalam lingkungan organisasi TNI AD.

Selain peralatan yang canggih, Satuan Siber TNI AD juga idealnya harus selalu memperoleh *up date* ilmu pengetahuan dan bimbingan teknik tentang siber dari tenaga ahli baik secara rutin maupun berkala agar personel siber dapat mengetahui perkembangan kejahatan siber yang terbaru dan mampu untuk mengatasinya. Bimbingan teknik dapat berupa pendidikan, kursus maupun pelatihan yang dilaksanakan dengan menjalin kerjasama dengan Pindad dan mitra TNI AD lain yang turut memberikan bantuan pengadaan peralatan siber dengan tujuan pengetahuan dan perkembangan peralatan siber tersebut mendapat *up grade* kemampuan secara terus menerus.

Dibandingkan dengan kondisi ideal terkait sarana dan prasarana yang dimiliki Satuan Siber TNI AD terdapat *gap* yang sangat besar dan merupakan kelemahan utama dalam pelaksanaan

Koleksi Perpustakaan Universitas Terbuka

48794.pdf

tugas pokoknya. Saat ini kondisi ruang kerja Satuan Siber TNI AD sangat jauh dari kondisi ideal dikarenakan ruangan siber belum terkoneksi dengan jaringan komputer antar staf dan masih berdiri sendiri (tidak terkoneksi dengan satuan siber lainnya). Hal ini menyebabkan jalur komunikasi dan koordinasi antar badan pelaksana di dalam TNI AD saja sudah membutuhkan waktu yang lama apalagi bila berkomunikasi dengan instansi sipil dan pemerintah. Hal ini semakin diperparah dengan kondisi perangkat kerja dan piranti lunaknya. Saat ini, Satuan Siber TNI AD hanya didukung oleh satu *router* untuk mendukung jaringan *internet*, sedangkan perangkat kerasnya menggunakan *laptop* yang sebagian besar adalah milik pribadi setiap personel siber. Dampak yang ditimbulkan dari adanya kondisi demikian adalah satuan siber sangat rentan untuk disabotase ataupun diserang oleh *hacker* yang memiliki wawasan luas dan teknologi perangkat yang tinggi. Hal ini pada akhirnya akan mengancam bocornya rahasia negara bidang pertahanan. Oleh karena itu, dengan segala keterbatasannya Satuan Siber TNI AD hanya memiliki kemampuan *monitoring* aktivitas media sosial yang bersentimen negatif terhadap TNI AD dan belum mampu melaakukan serangan siber, *tracking digital* terhadap *hacker* dan lainnya. Bahkan untuk tahap membongkar identitas pelaku, Satuan Siber TNI AD masih meminta bantuan kepada Pusat Informasi Intelijen (PII) Pusintelad dalam rangka penggunaan peralatan pelacak keberadaan atau posisi pelaku serta

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

pertolongan tenaga ahli dalam mengoperasionalkan peralatan tersebut, sehingga dalam hal ini Satuan Siber TNI AD baru dapat mengambil langkah setelah PII Pusintelad selesai melaksanakan tugasnya. Selanjutnya setelah pelaku terdeteksi, langkah yang dilakukan oleh Satuan Siber TNI AD adalah langkah nyata berupa pelaporan konten kepada pihak pemilik aplikasi, sedangkan langkah penanganan secara siber masih nihil.

Faktor lain yang menjadi penghambat dalam pelaksanaan tugas Satuan Siber TNI AD adalah masih lemahnya hukum perundang-undangan di Indonesia, termasuk peraturan dan ketentuan hukum yang mengatur Satuan siber TNI AD dalam melaksanakan tugas pokoknya terutama serangan siber dan mekanisme penindakan pelaku kejahatan siber terhadap institusi militer, sehingga menyebabkan personel siber menjadi tidak leluasa dalam melaksanakan tugasnya.

Seperti pernyataan dari Sovia Hasanah, S.H. dari artikel dengan judul Landasan Hukum Penanganan *Cybercrime* di Indonesia yang terbit pada tanggal 12 Oktober 2018 dijelaskan bahwa:

"Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana sepanjang dengan menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas. Akan tetapi, dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana yang telah diubah oleh Undang-Undang Nomor 19

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik."

Ada begitu banyak definisi *cyber crimes*, baik menurut para ahli maupun berdasarkan peraturan perundang-undangan. Definisi-definisi tersebut dapat dijadikan dasar pengaturan hukum pidana siber materil. Misalnya, Sussan Brenner (2011) membagi *cyber crimes* menjadi tiga kategori:

"Crimes in which the computer is the target of the criminal activity. Crimes in which the computer is a tool used to commit the crime. Crimes in which the use of the computer is an incidental aspect of the commission of the crime."

Sedangkan, Nicholson (2010) menggunakan terminologi *computer crimes* dan mengkategorikan *computer crimes* (*cyber crimes*) menjadi objek maupun subjek tindak pidana serta instrumen tindak pidana.

"First, a computer may be the 'object' of a crime: the offender targets the computer itself. This encompasses theft of computer processor time and computerized services. Second, a computer may be the 'subject' of a crime: a computer is the physical site of the crime, or the source of, or reason for, unique forms of asset loss. This includes the use of 'viruses', 'worms', 'Trojan horses', 'logic bombs', and 'sniffers.' Third, a computer may be an 'instrument' used to commit traditional crimes in a more complex manner. For example, a computer might be used to collect credit card information to make fraudulent purchases."

Menurut instrumen Perserikatan Bangsa Bangsa (PBB) dalam *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* yang diselenggarakan di Vienna, 10-17 April 2000, kategori *cyber crime* dapat dilihat secara sempit maupun secara luas, yaitu:

Koleksi Perpustakaan Universitas Terbuka

"Cyber crime in a narrow sense ("computer crime"): any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them."

"Cyber crime in a broader sense ("computer-related crime"): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network."

Convention on Cyber Crime (Budapest, 23.XI.2001) tidak memberikan definisi *cyber crimes*, tetapi memberikan ketentuan-ketentuan yang dapat diklasifikasikan menjadi:

a. *Offences against the confidentiality, integrity and availability of computer data and systems.*

b. *Computer-related offences.*

c. *Content-related offences.*

d. *Offences related to infringements of copyright and related rights.*

e. *Ancillary liability and sanctions corporate liability.*

Sementara dalam *Black's Law Dictionary 9th Edition*, definisi *computer crime* adalah sebagai berikut:

"A crime involving the use of a computer, such as sabotaging or stealing electronically stored data. - Also termed cyber crime."

Berdasarkan Instrumen PBB di atas, maka pengaturan tindak pidana siber di Indonesia juga dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas. Demikian juga tindak pidana dalam Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana (UU 3/2011) maupun tindak pidana perbankan serta tindak pidana pencucian uang dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU).

UU ITE (tahun 2008) merupakan undang-undang pertama di bidang teknologi informasi dan transaksi elektronik sebagai produk legislasi yang sangat dibutuhkan dan telah menjadi pionir yang meletakkan dasar pengaturan di bidang pemanfaatan teknologi informasi dan transaksi elektronik. Akan tetapi, dalam kenyataannya, implementasi dari UU ITE mengalami beberapa persoalan.

Pertama, terhadap UU ITE telah diajukan beberapa kali uji materiil di Mahkamah Konstitusi (MK) dengan Putusan MK Nomor 50/PUU-VI/2008, Nomor 2/PUU-VII/2009, Nomor 5/PUU-VIII/2010, dan Nomor 20/PUU-XIV/2016. Sesuai dengan peraturan maka harus dilakukan penyesuaian terkait dengan Putusan MK terhadap pasal-pasal di dalamnya. Berdasarkan Putusan MK Nomor 50/PUU-VI/2008 dan Nomor 2/PUU-VII/2009, tindak pidana penghinaan dan pencemaran nama baik dalam bidang informasi elektronik dan transaksi elektronik bukan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

semata-mata sebagai tindak pidana umum, melainkan sebagai delik aduan. Penegasan mengenai delik aduan dimaksudkan agar selaras dengan asas kepastian hukum dan rasa keadilan masyarakat. Berdasarkan Putusan MK Nomor 5/PUU-VIII/2010, MK berpendapat bahwa kegiatan dan kewenangan penyadapan merupakan hal yang sangat sensitif karena di satu sisi merupakan pembatasan hak asasi manusia, tetapi di sisi lain memiliki aspek kepentingan hukum. Oleh karena itu, pengaturan (*regulation*) mengenai legalitas penyadapan harus dibentuk dan diformulasikan secara tepat sesuai dengan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Di samping itu, Mahkamah Konstitusi (MK) berpendapat bahwa karena penyadapan merupakan pelanggaran atas hak asasi manusia sebagaimana ditegaskan dalam Pasal 28J ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, sangat wajar dan sudah sepatutnya jika negara ingin menyimpangi hak privasi warga negara tersebut, negara haruslah menyimpanginya dalam bentuk undang-undang dan bukan dalam bentuk peraturan pemerintah. Selain itu, berdasarkan Putusan MK Nomor 20/PUU-XIV/2016, MK berpendapat bahwa untuk mencegah terjadinya perbedaan penafsiran terhadap Pasal 5 ayat (1) dan ayat (2) UU ITE, Mahkamah menegaskan bahwa setiap intersepsi harus dilakukan secara sah, terlebih lagi dalam rangka penegakan hukum. Oleh karena itu, Mahkamah dalam amar putusannya menambahkan kata

Koleksi Perpustakaan Universitas Terbuka

48794.pdf

atau frasa "khususnya" terhadap frasa "informasi elektronik dan/atau dokumen elektronik". Agar tidak terjadi penafsiran bahwa putusan tersebut akan mempersempit makna atau arti yang terdapat di dalam Pasal 5 ayat (1) dan ayat (2) UU ITE, untuk memberikan kepastian hukum keberadaan informasi elektronik dan/atau dokumen elektronik sebagai alat bukti perlu dipertegas kembali dalam Penjelasan Pasal 5 UU ITE.

Kedua, ketentuan mengenai penggeledahan, penyitaan, penangkapan, dan penahanan yang diatur dalam UU ITE menimbulkan permasalahan bagi penyidik karena tindak pidana di bidang teknologi informasi dan transaksi elektronik begitu cepat dan pelaku dapat dengan mudah mengaburkan perbuatan atau alat bukti kejahatan.

Ketiga, karakteristik virtualitas ruang siber memungkinkan konten ilegal seperti informasi dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau pengancaman, penyebaran berita bohong dan menyesatkan sehingga mengakibatkan kerugian konsumen dalam transaksi elektronik, serta perbuatan menyebarkan kebencian atau permusuhan berdasarkan suku, agama, ras, dan golongan, dan pengiriman ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi dapat diakses, didistribusikan, ditransmisikan, disalin, disimpan untuk didiseminasi kembali dari

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

mana saja dan kapan saja. Dalam rangka melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi elektronik dan transaksi elektronik, diperlukan penegasan peran Pemerintah dalam mencegah penyebarluasan konten ilegal dengan melakukan tindakan pemutusan akses terhadap informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar hukum agar tidak dapat diakses dari yurisdiksi Indonesia serta dibutuhkan kewenangan bagi penyidik untuk meminta informasi yang terdapat dalam penyelenggara sistem elektronik untuk kepentingan penegakan hukum tindak pidana di bidang teknologi informasi dan transaksi elektronik.

Keempat, penggunaan setiap informasi melalui media atau sistem elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Untuk itu, dibutuhkan jaminan pemenuhan perlindungan diri pribadi dengan mewajibkan setiap penyelenggara sistem elektronik untuk menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.

Berdasarkan keempat pertimbangan inilah pembentuk Undang-Undang (Pemerintah dan DPR) melakukan perubahan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

terhadap UU ITE. Materi muatan perubahan tidak lepas dari latar belakang atau pertimbangan tersebut.

Dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU 19/2016") sama halnya seperti *Convention on Cyber Crimes*, UU ITE juga tidak memberikan definisi mengenai *cyber crimes*, tetapi membaginya menjadi beberapa pengelompokkan yang mengacu pada *Convention on Cybercrimes* (Sitompul, 2012):

a. Tindak pidana yang berhubungan dengan aktivitas illegal, yaitu:

   Distribusi atau penyebaran, transmisi, dapat diaksesnya konten ilegal, yang terdiri atas:

   1) Kesusilaan (Pasal 27 ayat (1) UU ITE).
   2) Perjudian (Pasal 27 ayat (2) UU ITE).
   3) Penghinaan dan/atau pencemaran nama baik (Pasal 27 ayat (3) UU ITE).
   4) Pemerasan dan/atau pengancaman (Pasal 27 ayat (4) UU ITE).
   5) Berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat (1) UU ITE).
   6) Menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat (2) UU ITE).

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

7) Mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE).

8) Dengan cara apapun melakukan akses illegal (Pasal 30 UU ITE).

9) Intersepsi atau penyadapan ilegal terhadap informasi atau dokumen elektronik dan sistem elektronik (Pasal 31 UU 19/2016).

b. Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:

1) Gangguan terhadap informasi atau dokumen elektronik (*Data Interference* - Pasal 32 UU ITE).

2) Gangguan terhadap sistem elektronik (*System Interference* –Pasal 33 UU ITE).

3) Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE).

4) Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE).

5) Tindak pidana tambahan (*accessoir* Pasal 36 UU ITE).

6) Perberatan-perberatan terhadap ancaman pidana (Pasal 52 UU ITE).

Selain mengatur tindak pidana siber materil, UU ITE mengatur tindak pidana siber formil, khususnya dalam bidang

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

penyidikan. Pasal 42 UU ITE mengatur bahwa penyidikan terhadap tindak pidana dalam UU ITE dilakukan berdasarkan ketentuan dalam Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) dan ketentuan dalam UU ITE. Artinya, ketentuan penyidikan dalam KUHAP tetap berlaku sepanjang tidak diatur lain dalam UU ITE. Kekhususan UU ITE dalam penyidikan antara lain:

a. Penyidik yang menangani tindak pidana siber ialah dari instansi Kepolisian Negara RI atau Pejabat Pegawai Negeri Sipil (PPNS) Kementerian Komunikasi dan Informatika.
b. Penyidikan dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data.
c. Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan sesuai dengan ketentuan hukum acara pidana.
d. Dalam melakukan penggeledahan dan/atau penyitaan sistem elektronik, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.
e. Ketentuan penyidikan dalam UU ITE dan perubahannya berlaku pula terhadap penyidikan tindak pidana siber dalam arti luas. Sebagai contoh, dalam tindak pidana perpajakan, sebelum dilakukan penggeledahan atau penyitaan terhadap server bank, penyidik harus memperhatikan kelancaran

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

layanan publik, dan menjaga terpeliharanya kepentingan pelayanan umum sebagaimana diatur dalam UU ITE dan perubahannya. Apabila dengan mematikan *server* Bank akan mengganggu pelayanan publik, tindakan tersebut tidak boleh dilakukan.

Prosedur untuk menuntut secara pidana terhadap perbuatan tindak pidana siber, secara sederhana dapat dijelaskan sebagai berikut:

a. Korban yang merasa haknya dilanggar atau melalui kuasa hukum, datang langsung membuat laporan kejadian kepada penyidik POLRI pada unit/bagian *cyber crime* atau kepada penyidik PPNS pada Sub Direktorat Penyidikan dan Penindakan, Kementerian Komunikasi dan Informatika. Selanjutnya, penyidik akan melakukan penyelidikan yang dapat dilanjutkan dengan proses penyidikan atas kasus bersangkutan Hukum Acara Pidana dan ketentuan dalam UU ITE.

b. Setelah proses penyidikan selesai, maka berkas perkara oleh penyidik akan dilimpahkan kepada penuntut umum untuk dilakukan penuntutan di muka pengadilan. Apabila yang melakukan penyidikan adalah PPNS, maka hasil penyidikannya disampaikan kepada penuntut umum melalui penyidik POLRI. Selain UU ITE, peraturan yang menjadi landasan dalam penanganan kasus *cyber crime* di Indonesia

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

ialah peraturan pelaksana UU ITE dan juga peraturan teknis dalam penyidikan di masing-masing instansi penyidik.

Sesuai dengan pembahasan di atas, Revolusi Industri 4.0 telah memberikan pengaruh yang sangat signifikan dalam bidang pertahanan dan keamanan, dimana banyak negara negara lain yang berlomba-lomba untuk menciptakan suatu sistem piranti lunak yang menjadi basis untuk pengendali persenjataan dan sistem pertahanan negaranya. Hal ini harus segera diantisipasi dengan cara membentuk suatu satuan siber yang mampu melindungi negara Indonesia dari serangan siber. Peningkatan fungsi Satuan Siber TNI AD adalah salah satu upaya nyata yang selaras untuk menjawab tantangan dan ancaman tersebut. Di samping itu, Revolusi Industri 4.0 juga memberikan pengaruh yang tidak kecil terhadap bidang keamanan siber di Indonesia. Pemerintah telah membentuk Satuan Siber Nasional (BSSN) sebagai koordinator satuan siber lain se-Indonesia yang diharapkan dapat menciptakan suatu kesatuan sistem keamanan siber yang terintegrasi dan efektif serta efisien dalam menghadapi gangguan siber dari lawan. Peningkatan fungsi Satuan Siber TNI AD dapat memberikan manfaat dalam terciptanya suatu koordinasi yang lebih baik antar satuan siber di Indonesia. Pada Akhirnya, adanya Revolusi Industri 4.0 yang menghilangkan batasan dunia siber dan dunia nyata semakin membuka celah timbulnya upaya-upaya tindak kejahatan baru yang telah berusaha diantisipasi oleh pemerintah dengan

Koleksi Perpustakaan Universitas Terbuka

48794.pdf

melakukan revisi UU ITE untuk mewadahi kerancuan yang ditimbulkan dalam tindak kejahatan siber.

Dengan regulasi yang ada tersebut tidak ada pasal yang menjelaskan apabila kejahatan siber melibatkan prajurit atau institusi militer, tidak adanya peraturan teknis yang mengatur dan menjembatani antara Undang-Undang ITE dengan peraturan/hukum militer. Selain itu tidak ada penjelasan kapan kejahatan siber yang menyerang negara dapat dikatakan mengancam kedaulatan negara, sehingga pasukan siber TNI dapat turun tangan. Regulasi yang ada masih mengkotak-kotakan antara pelaku dan korban sipil atau militer, sehingga tidak dapat menjelaskan apabila pelaku sipil menyerang piranti lunak militer dan mengambil alih sistem Alutsista dan pertahanan negara, maka akan dilakukan penanganan secara militer atau secara sipil, demikian juga berlaku sebaliknya.

Mengingat keinginan Presiden Joko Widodo untuk mensinergikan seluruh satuan siber di Indonesia untuk memperoleh data yang cepat dan mudah maka dibutuhkan aturan atau regulasi teknis yang ikut mengatur mekanisme pelaksanaan kerjasama tersebut, dimana regulasi tersebut dapat menjembatani peraturan di Kemkominfo, POLRI dan TNI, sehingga terbentuk regulasi yang memiliki prosedur jelas bagi setiap personel siber baik sipil maupun militer dalam mengambil langkah penyelesaian masalah termasuk salah satunya adalah langkah hukum.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Faktor lain yang menjadi penghambat dalam pelaksanaan tugas Satuan Siber TNI AD adalah masih terbatasnya koordinasi lintas sektoral antar satuan pendukung guna menghadapi kejahatan siber. Secara ideal pola birokrasi penanganan masalah kejahatan siber harus dikalukan secara terintegrasi, namun tetap menjaga privasi/data rahasia masing-masing instansi. Dengan adanya suatu jaringan yang terintegrasi tersebut maka akan memotong jalur birokrasi yang terlalu panjang dan membutuhkan waktu yang cukup lama. Sebagai contoh, saat ini untuk memblokir akun palsu atau membongkar identitas pelaku/*hacker*, TNI AD membutuhkan waktu lebih dari 1 minggu sehingga menyebabkan berita *hoax* menjadi viral sebelum masalah diselesaikan. Setelah Satuan Siber TNI AD berhasil mengungkap identitas pelaku dan mengetahui bahwa akun yang digunakan adalah palsu, maka personel siber segera membuat pelaporan kepada pihak pemilik aplikasi untuk menutup akun palsu tersebut, pada kenyataannya penutupan akun oleh pihak pengembang aplikasi berbeda-beda, sehingga waktu yang lama tersebut menyebabkan berita sudah menjadi viral. Di sisi lain, setelah identitas pelaku terungkap langkah yang dilakukan adalah personel siber membuat laporan kepada Kemenkominfo untuk dilaksanakan pemblokiran aktivitas media sosial milik pelaku, sedangkan untuk tindakan pidananya dilaporkan kepada POLRI juga membutuhkan waktu yang sangat lama untuk ditindak lanjuti.

Koleksi Perpustakaan Universitas Terbuka

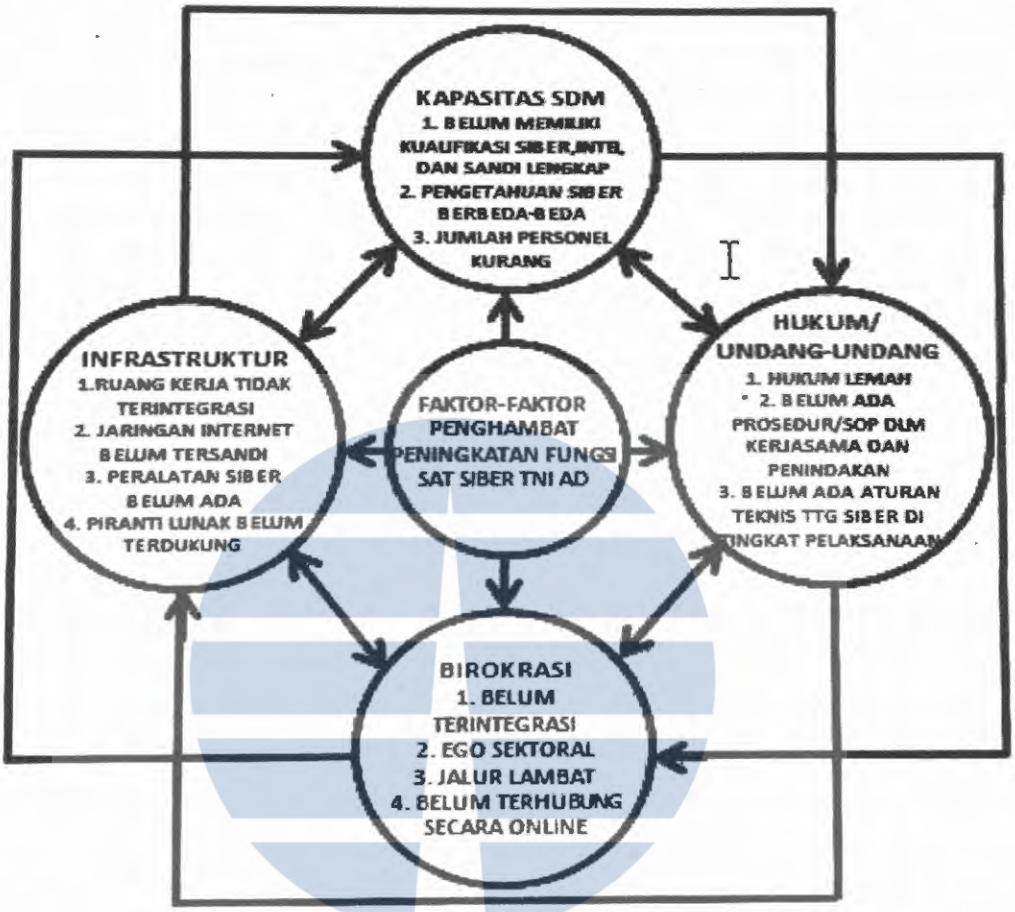
43794.pdf

Berdasarkan pada panjangnya jalur birokrasi di atas, maka idealnya terbentuk satu jaring besar koordinasi antara BSSN, Kemenkominfo, Mabes TNI dan Mabes POLRI serta BIN, kemudian jaring utama tersebut diteruskan ke bagian satuan kecil masing-masing. Untuk satuan siber di masyarakat sipil menginduk kepada Kemenkominfo, satuan siber jajaran POLRI menginduk kepada Mabes POLRI dan satuan jajaran TNI (termasuk Satuan Siber TNI AD) menginduk kepada Satuan Siber Mabes TNI, di mana pada akhirnya semua satuan siber tersebut akan terhubung dalam suatu jaringan terintegrasi dalam jaringan siber BSSN selaku koordinator satuan siber nasional. Dengan demikian akan terbentuk jaringan *online* yang akan *memonitor* kejahatan di dunia maya dan apabila ditemukan adanya pelaku yang melakukan aktivitas kejahatan siber maka akan dengan segera dapat diambil tindakan tentunya setelah adanya laporan dari pihak/instansi yang menjadi korban. Dengan adanya sistem yang terintegrasi secara *online* ini maka akan mengurangi manajemen resiko dan keraguan personel siber dalam melaksanakan tugasnya, dikarenakan sudah ada prosedur dan mekanisme kerja serta yang tidak kalah pentingnya sudah ada payung hukum yang melindungi baik secara hukum sipil maupun hukum militer. Di sisi lain adanya sistem yang terintegrasi ini akan sangat membantu pemerintah dalam menentukan kejahatan siber mana yang dinilai membahayakan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

kedaulatan negara dan kejahatan siber mana yang mengganggu privasi pribadi individu ataupun suatu organisasi.



Bagan 4.6
Korelasi Faktor-Faktor Penghambat
Peningkatan Fungsi Satuan Siber TNI AD

3. Peran Satuan Siber TNI AD dalam mendukung sinergitas lembaga siber nasional untuk mengungkap kejahatan siber

Satuan Siber TNI AD yang ada saat ini masih merupakan organisasi satuan tugas yang bertugas menyelenggarakan kegiatan dan operasi siber di lingkungan TNI AD dalam rangka mendukung tugas pokok TNI. Satuan Siber TNI AD belum terbentuk menjadi satuan kerja yang memiliki fungsi dan tugas yang dilindungi oleh

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

ketentuan yang berlaku di TNI AD. Saat ini yang dapat dilakukan oleh Satuan Siber TNI AD adalah sebagai *monitoring* dan pertahanan menghadapi serangan kejahatan siber serta memberikan respon cepat dan melaporkannya kepada pimpinan TNI AD dalam rangka mengamankan institusi TNI AD dari ancaman kejahatan siber. Faktor-faktor ancaman tersebut adalah berupa serangan psikologi siber dan serangan terhadap infrastruktur dan sistem informatika yang dimiliki TNI AD.

Berdasarkan artikel yang ditulis oleh Klaus Schwab, *Founder* dan *Executive Chairman World Economic Forum*, menyatakan bahwa saat ini kita berada pada transisi revolusi teknologi yang secara fundamental akan mengubah cara hidup, bekerja, dan berhubungan satu sama lain. Dalam skala, ruang lingkup, dan kompleksitasnya, transformasi ini akan berbeda serta tidak seperti yang pernah dialami oleh umat manusia sebelumnya. Walaupun belum diketahui bagaimana transformasi ini akan terjadi, namun satu hal yang jelas adalah respon terhadap transformasi ini harus terintegrasi dan komprehensif, melibatkan seluruh pemangku kepentingan dan pemerintahan global, dari sektor publik dan swasta, hingga komunitas akademisi dan sipil.

Revolusi Industri Pertama (1784) menggunakan tenaga air dan uap untuk mekanisasi produksi. Revolusi Industri Kedua (1870) menggunakan tenaga listrik untuk membuat produksi massal. Revolusi Industri Ketiga (1969) menggunakan elektronika

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

dan teknologi informasi untuk otomatisasi produksi. Kemudian, Revolusi Industri Keempat dibangun di atas Revolusi Industri Ketiga, suatu revolusi *digital* yang telah berlangsung sejak pertengahan abad ke-20. Revolusi Industri Keempat ini ditandai oleh perpaduan teknologi yang mengaburkan batas-batas fisik, *digital*, dan biologi.

Dengan kemampuan pemrosesan, kapasitas penyimpanan, dan akses pengetahuan yang belum pernah ada sebelumnya, kemungkinan dari beberapa miliar orang yang terhubung oleh perangkat bergerak menjadi tidak terbatas. Dan kemungkinan tersebut akan semakin bertambah seiring munculnya terobosan baru dalam kecerdasan buatan, robotika, *Internet of Things*, kendaraan otonom, pencetakan 3D, nanoteknologi, bioteknologi, ilmu material, penyimpanan energi, dan komputasi kuantum.

Seiring dengan penyatuan dunia fisik, *digital*, dan biologis, maka teknologi dan *platform* baru akan semakin memungkinkan warga untuk terlibat dengan pemerintah, menyuarakan pendapat, mengkoordinasikan upayanya, dan bahkan menghindari pengawasan otoritas publik. Secara bersamaan, pemerintah akan memperoleh kemampuan teknologi baru untuk meningkatkan kendali atas populasi, berdasarkan sistem pengawasan menyeluruh dan kemampuan untuk mengendalikan infrastruktur *digital*. Secara keseluruhan, pemerintah akan semakin menghadapi tekanan untuk mengubah pendekatan saat ini dalam keterlibatan dan pembuatan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

kebijakan publik. Hal ini karena peran sentralnya untuk melakukan kebijakan berkurang disebabkan oleh permasalahan kompetisi dan teknologi baru yang memungkinkan untuk redistribusi dan desentralisasi kekuasaan.

Revolusi Industri 4.0 juga akan sangat berakibat pada keamanan nasional dan internasional, serta mempengaruhi baik probabilitas maupun sifat konflik. Sejarah peperangan dan keamanan internasional merupakan sejarah inovasi teknologi, dan hal ini tidak terkecuali. Konflik modern yang melibatkan negara-negara menjadi semakin samar, menggabungkan teknik perang tradisional dengan unsur yang sebelumnya dikaitkan sebagai aktor non-negara. Membedakan antara perang dengan damai, kombatan dengan non-kombatan, dan bahkan kekerasan dengan tanpa kekerasan menjadi semakin rancu.

Seiring terjadinya proses ini dan kemudahan dalam penggunaan teknologi baru seperti senjata otonom atau biologis, maka individu dan kelompok kecil akan bergabung sehingga menyebabkan kerusakan fatal. Kerawanan baru ini akan menyebabkan ketakutan baru. Tetapi pada saat yang sama, kemajuan teknologi akan menciptakan potensi untuk mengurangi skala atau dampak kekerasan, melalui pengembangan cara-cara baru untuk perlindungan atau lebih presisi dalam penargetan.

Saat ini Panglima TNI juga tengah fokus untuk mengembangkan sumberdaya manusia (SDM) yang sesuai dengan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

tantangan era revolusi Industri 4.0. Salah satu caranya adalah lewat pendidikan dan kursus *reguler* bagi kesatuan TNI untuk mengikuti dan menguasai perkembangan bidang teknologi yang menjadi pilar Industri 4.0.

Presiden Joko Widodo juga telah mencanangkan strategi *Making* Indonesia 4.0 yang telah menjadi pedoman bagi seluruh kementerian dan lembaga negara. TNI yang merupakan alat negara tentunya sangat berkepentingan untuk mengantisipasi secara cepat dan tepat tentang perkembangan global terkait dengan Industri 4.0.

Apalagi seluruh alutsista TNI kini serba canggih yang dioperasikan dan dikontrol secara *digital*. TNI bersiap menghadapi perkembangan tatanan dunia baru yang diwarnai dengan era revolusi Industri 4.0. Dalam era tersebut tentunya kekuatan militer menjadi salah satu unsur penting karena perkembangan teknologi telah mengubah seluruh tatanan strategi militer. Hal ini merupakan tantangan yang harus dihadapi oleh seluruh personel TNI maupun para Taruna-Taruni Akademi Militer.

Menurut konsultan dunia terkemuka Deloitte, bahwa Industri 4.0 mampu meningkatkan tingkat kesiapan operasional militer. Kemajuan dalam teknologi Industri 4.0 sangat membantu organisasi pertahanan negara meningkatkan kesiapan dan keefektifan mereka.

Bermacam alutsista dan infrastruktur militer penunjang kini telah menerapkan dan didukung dengan teknologi *Internet of*

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Things (IoT) dan teknologi *Big Data*. Teknologi pilar Industri 4.0 itu sangat membantu perencanaan tugas militer, operasi militer maupun untuk efektivitas anggaran militer suatu negara.

Dalam laporan terbaru, Deloitte menyatakan bahwa pasukan pertahanan AS mampu meningkatkan kesiapan mereka berkat teknologi Industri 4.0. Upaya keras pimpinan TNI untuk membangun dan mendirikan lembaga pendidikan berkelas dunia harus didukung penuh.

Baik pendidikan dan latihan terkait bidang kemiliteran, maupun untuk pendidikan umum, yakni Sekolah Menengah Atas (SMA) unggulan yang dikelola oleh keluarga besar TNI. Seperti SMA Taruna Nusantara, SMA Taruna Nala, dan SMA Pradhita Dirgantara. Semuanya memiliki misi besar untuk mencetak SDM unggul khususnya bidang Hankam yang mampu mewujudkan metode pengamanan yang paling tepat untuk Indonesia. Sehingga pada akhirnya, dapat terbentuk masyarakat 5.0 yang mampu menghadapi perkembangan teknologi dan menjawab tantangan dari revolusi industri 4.0 di mana pada prinsipnya sebesar apapun perkembangan suatu teknologi, manusia tetap harus menjadi pusat dari kegiatannya. Menciptakan SDM yang unggul adalah cara terbaik guna mewujudkan masyarakat 5.0 tersebut.

Hal itu searah dengan visi Presiden Joko Widodo yang dikemukakan saat memberikan pembekalan kepada perwira remaja TNI/Polri, di Mabes TNI. Tak hentinya-hentinya Panglima TNI

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

menyatakan bahwa Indonesia kini termasuk dalam wilayah Indo Pasifik yang sangat dinamis, sehingga memiliki peluang dan tantangan untuk menghadapi perubahan geopolitik yang terjadi tiba-tiba.

Oleh karena itu, Indonesia perlu menjalin kerja sama dengan negara maju untuk menjawab tantangan revolusi Industri 4.0 beserta dampak sosialnya. Panglima TNI menyatakan alutsista Indonesia harus segera mengikuti perkembangan pesat teknologi *digital*.

Alat utama sistem persenjataan (alutsista) TNI harus segera dikembangkan menjadi berbasis teknologi *digital*. Keniscayaan pembaruan alutsista itu perlu dilakukan mengingat jenis teknologi yang menjadi pilar Industri 4.0 semakin bergerak cepat dan sulit dikuasai.

Tak pelak lagi sekarang setiap orang dan setiap pasukan TNI terhubung dengan internet satu sama yang lain. Keterbukaan informasi semakin lebar sehingga kita harus mengimbangi dengan perkembangan revolusi tersebut. Alutsista TNI juga harus secepatnya dikembangkan agar berbasis pada penggunaan teknologi *big data* dan *artificial intelligence*.

Masuknya revolusi industri 4.0 harus diimbangi dengan kemampuan teknologi yang memadai. Karena itu, Panglima TNI Marsekal Hadi Tjahjanto menargetkan alat utama sistem persenjataan (alutsista) TNI ada yang berbasis *digital*. Ia

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

mengatakan akibat revolusi industri 4.0 itu semua akan mengalami perubahan. Termasuk doktrin, dulu kita adalah nyata, tetapi sekarang musuh kita menggunakan *`articial intelligence`*, maupun *`big data`*.

"Jadi semua alusista digunakan untuk *`big data`*. Perang semakin terbuka dan tidak kenal batas sehingga doktrin pun harus laksanakan penyesuaian," ujarnya

Sebagaimana dilansir Antara, Strategi dari Kementerian Pertahanan dan TNI. Kebijakan perencanaan pertahanan tahun 2019 diwujudkan melalui arah kebijakan penguatan pertahanan, yaitu penyelenggaraan Operasi Militer Selain Perang (OMSP) dalam rangka pengamanan Pemilu, pengadaan Alutsista TNI dalam rangka pemenuhan MEF, pemeliharaan dan perawatan Alutsista TNI. Selanjutnya pembangunan sarana dan prasarana satuan alutsista TNI dan satuan baru, peningkatan sarana dan prasarana perbatasan dan penguatan industri pertahanan.

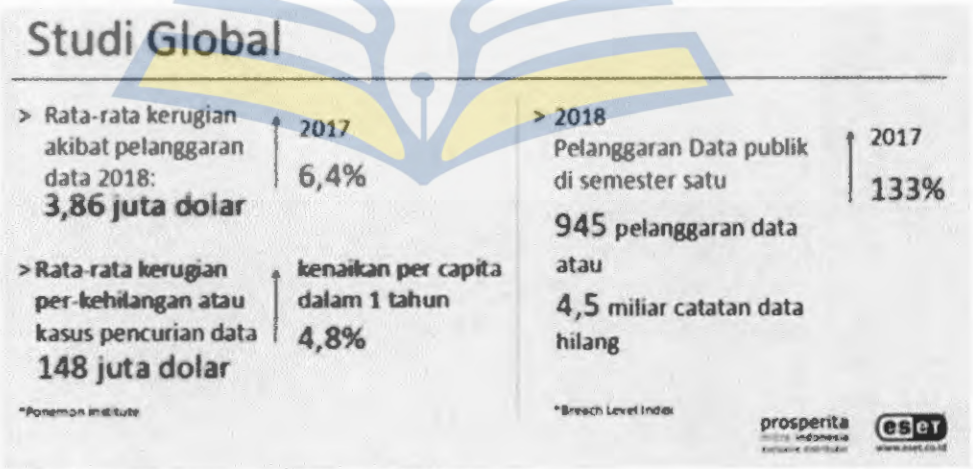
Sasaran yang ingin dicapai melalui alokasi anggaran fungsi pertahanan pada Tahun 2019 tersebut di antaranya: pengadaan 125 paket kendaraan taktis, suku cadang, kendaraan tempur, dan suku cadang kendaraan taktis; pengadaan/penggantian 3 unit kendaraan tempur; pengadaan/penggantian 688 pucuk senjata dan munisi; pembangunan 18 unit KRI, KAL, dan Alpung; dan modernisasi 1 paket *Command Center* Komando Pertahanan Udara Nasional (Kohanudnas).

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Menurut kajian *Global Power*, Indonesia menempati peringkat ke-19 dari 55 negara yang disurvei dalam urutan kekuatan pertahananan negara. Kapabilitas itu dibuat berdasarkan strategi pertahanan negara yang merefleksikan kemampuan, kekuatan, dan gelar kekuatan pertahanan dan sumberdaya nasional. Dalam rangka melaksanakan strategi pertahanan negara, kapabilitas pertahanan negara dikembangkan untuk mencapai standar penangkalan, yakni kapabilitas pertahanan negara yang mampu menangkal dan mengatasi ancaman terhadap kedaulatan negara, keutuhan wilayah NKRI dan keselamatan segenap warga bangsa.

Pelaku revolusi Industri 4.0 mengalami ancaman dunia maya yang sama seperti organisasi lain. Di mana bisnis dari semua ukuran menjadi sasaran kejahatan siber yang terus meningkat dari tahun ke tahun.



Sumber : Ponemon Institute, 2018

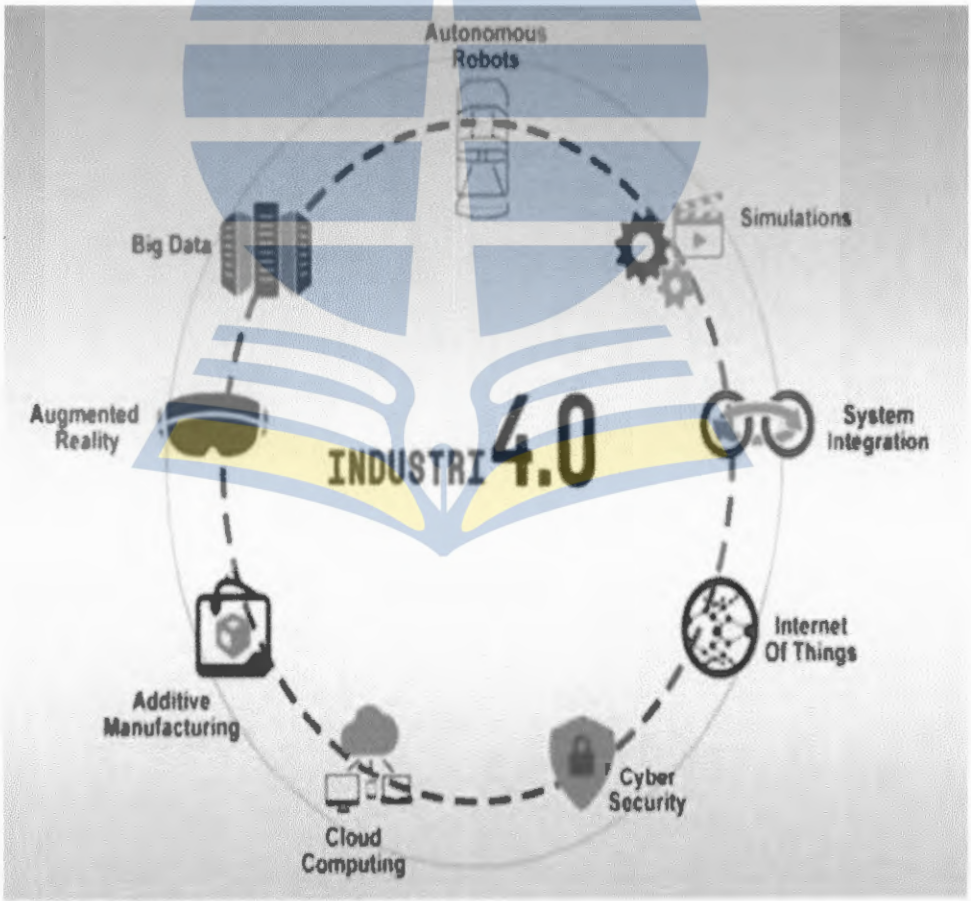
Gambar 4.1
Kerugian Akibat Pelanggaran Data Secara Global

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Ponemon Institute dalam studinya pada 2018 menyatakan, rata-rata kerugian akibat pelanggaran data secara global pada tahun ini mencapai 3,86 juta dolar (Rp56 miliar) atau meningkat 6,4 persen dari tahun sebelumnya.

Menurut *Breach Level Index*, basis data global dari pelanggaran data publik mengungkapkan 945 pelanggaran data menyebabkan 4,5 miliar catatan data dikompromikan di seluruh dunia pada paruh pertama 2018. Dibandingkan dengan periode yang sama pada 2017, jumlah data yang hilang, dicuri atau dikompromikan meningkat 133 persen.



Sumber : www.iNews.id, 2018

Gambar 4.2
Ancaman Siber dalam Revolusi Industri 4.0

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Setelah diwacanakan sejak beberapa tahun yang lalu, akhirnya Presiden Joko Widodo, mengesahkan sebuah badan siber nasional yang bernama Badan Siber dan Sandi Negara (BSSN). Menurut pemerintah, badan ini didirikan untuk memperkuat pertahanan siber Indonesia mencegah serangan-serangan siber yang dilakukan oleh pihak luar.

Di dalam kehidupan siber saat ini, Indonesia sebagai negara kepulauan terbesar di dunia, tidak mungkin pertahanan hanya dilakukan dengan cara konvensional, sehingga pertahanan melalui siber sangat dibutuhkan untuk menjaga kedaulatan RI.

BSSN dalam kesehariannya akan bertugas mendeteksi dan mencegah kejahatan siber dengan menjaga keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber di Indonesia. Oleh karena itu, dalam upaya mewujudkan sinergitas kelembagaan siber nasional, BSSN berperan sebagai koordinator seluruh badan siber di Indonesia.

Sejatinya lembaga baru ini merupakan sebuah badan hasil transformasi Lembaga Sandi Negara (LSN) yang sudah ada sebelumnya. Dengan pertimbangan bahwa bidang keamanan siber merupakan salah satu bidang penting yang perlu didorong dan diperkuat sebagai upaya mewujudkan keamanan nasional di era digital ini, maka Badan Siber dan Sandi Negara perlu dibentuk guna menjamin terselenggaranya kebijakan dan program

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

pemerintah di bidang keamanan siber. Selain itu, perhatian pemerintah pada aspek keamanan siber juga untuk mendorong pertumbuhan ekonomi nasional.

Lembaga siber yang dibentuk pemerintah dapat menjadi sebuah *cyber-intelligence hub* yakni sebagai media penghubung antara agen-agen siber yang sudah ada di Indonesia sebelumnya. Hubungan ini nantinya bisa menjadi media berbagi informasi tentang serangan, ancaman dan kejahatan melalui siber, serta sebagai media untuk melakukan konsolidasi strategi untuk penanggulangannya. Di tengah maraknya serangan siber seperti *Ransomware Wannacry, Hoax, Spamming*, pembentukan BSSN ini dinilai tepat waktu dan penting.

Berkaca dari negara tetangga, Singapura menurut *Global Cybersecurity Index* menjadi salah satu negara dengan index paling tinggi dalam hal komitmen penerapan keamanan siber saat ini. Singapura sebenarnya sejak lama sudah mempersiapkan inisiasi keamanan sibernya dengan meluncurkan *Cyber Security Master Plan* pada Tahun 2005. Sedangkan pembentukan *The Cyber Security Agency of Singapore (CSA)* direalisasikan pada Tahun 2015 lalu. Sejak Tahun 2016, Singapura sudah menjalankan strategi yang komprehensif tentang keamanan siber ini.

Negeri jiran Malaysia, berdasarkan *Global Cybersecurity Index (GCI)* berada pada peringkat 2 di Asia perihal *Cybersecurity*. Di Malaysia, entitas pemerintah memiliki tanggung jawab atas

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

keamanan informasi negara, selain itu juga pemerintah gencar menawarkan pelatihan profesional melalui perguruan tinggi Malaysia. Situs seperti *Cyberguru* contohnya didedikasikan untuk pelatihan keamanan siber untuk profesional.

Keamanan siber merupakan sebuah ekosistem di mana aturan hukum, organisasi, *skill*, kerja sama dan implementasi teknis harus berjalan secara harmonis untuk mencapai efektivitas yang tinggi. Selain itu juga, keamanan siber tidak hanya menjadi fokus pemerintah tetapi membutuhkan komitmen dari sektor swasta dan pengguna. Sehingga penting untuk membangun budaya keamanan siber bagi masyarakat Indonesia ketika menggunakan jaringan dan teknologi *digital*.

Menurut *Global Competitiveness Index* (GCI), tingginya efektivitas di dalam ekosistem keamanan siber sangat dipengaruhi oleh beberapa faktor, yang diistilahkan 5 pilar yakni :

a. Peraturan (*Legal*).

Pilar ini mengukur keberadaan peraturan pemerintah dan kerangka kerja yang dibuat pemerintah untuk menjawab permasalahan keamanan siber dan kejahatan siber. Pilar ini berkaitan dengan peraturan yang mengatur tentang lembaga pelindungan dan tindakan-tindakan yang berkaitan dengan aksi ilegal tehadap akses data, sistem, penyadapan melalui jaringan *internet*. Saat ini, sudah ada UU ITE yang mengatur tentang kegiatan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

transaksi elektronik dan Peraturan Presiden (Perpres) Nomor 133 Tahun 2017 tentang Badan Siber dan Sandi Negara, sedangkan kerangka kerja *(Framework)* memuat tentang peraturan dan prosedur untuk memastikan pengelolaan teknologi informasi berjalan secara berkelanjutan *(sustainable)*.

b. Pilar teknis (*Technical*).

Aspek ini berhubungan dengan keberadaan tim yang bertujuan untuk menjalankan fungsi teknis pada lingkungan siber. Di dalam BSSN nantinya mesti dibentuk tim handal untuk *Computer Emergency Response Team (CERT)* yang akan mendukung keamanan sektor vital, contohnya menjaga keamanan siber pemerintahan dan keuangan dari ancaman, serangan pihak luar. Pembangunan dan pengembangan laboraturium untuk tim CERT menjadi bagian penting di dalam pilar teknis ini.

Sebenarnya sudah ada tim yang dimiliki oleh Kementerian Kominfo yakni *id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center)*. Id-SIRTII/CC yang sudah ada ini dapat menguatkan BSSN yang baru saja dibentuk .

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

c. Pilar organisasi (*Organizational*).

Pemerintah dalam hal ini BSSN penting untuk menyusun strategi keamanan siber secara nasional dan mengkoordinasikan antar lembaga keamanan siber yang ada di Indonesia. *National Cyber Security Strategy (NCSS)* biasanya memuat tentang rencana strategis 5 tahun dalam menjalankan misi keamanan siber nasional. Selain itu, pembentukan Badan Siber Nasional ini dapat menjadi badan yang mampu mengkoordinasikan kerja tim pertahanan siber yang ada di Kementerian Pertahanan, *cyber intelligence* di Badan Intelijen Negara (BIN), dan *unit cyber crime* di kepolisian.

d. Pilar kapasitas (*Capacity Building*).

Ekosistem siber yang sangat dinamis tentu menuntut penyesuaian teknologi bagi lembaga keamanan siber nantinya. Pembangunan pusat riset dan pengembangan bidang keamanan siber, pendidikan, pelatihan dan sertifikasi profesional mutlak diperlukan dalam penyesuaian teknologi ke depan.

e. Pilar kerjasama (*Cooperation*).

Untuk meningkatkan *sharing* informasi, Badan siber seperti BSSN tentu harus membangun kerja sama baik dengan pihak swasta maupun badan siber negara lain. Kerja sama ini juga bisa berbentuk kerja sama teknis dan

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

keamanan siber untuk memperkuat ketahanan siber, menguji sistem respons yang dimiliki dan meningkatkan *sharing* informasi siber di kawasan.

Pada tanggal 8 November 2018, Badan Siber dan Sandi Negara (BSSN) dan Tentara Nasional Indonesia (TNI) melaksanakan kegiatan Penandatanganan *Memorandum of Understanding (MoU)* yang dilaksanakan di Ruang Hening, Gedung Soedirman, Mabes TNI Cilangkap, Jakarta. Penandatanganan ini dilakukan oleh Kepala BSSN Djoko Setiadi dan Panglima TNI Hadi Tjahjanto. MoU ini merupakan landasan berbagai kerja sama penguatan sistem teknologi informasi di lingkungan TNI melalui implementasi teknologi keamanan siber dan persandian.

Di awal sambutan Kepala BSSN menyampaikan pada saat ini perkembangan teknologi yang begitu pesat dengan pemanfaatannya dalam berbagai aspek kehidupan. Di mana ancaman non militer memiliki potensi yang dampaknya terhadap keamanan pertahanan negara sangat besar. Salah satu bentuk ancaman munculnya *hybrid warfare* yaitu strategi perang yang menggabungkan antara perang konvensional dengan perang informasi dan perang siber. Serangan siber yang dilakukan oleh penyerang memiliki tujuan yang pada umumnya menargetkan informasi sebagai aset yang strategis dan berharga. Oleh sebab itu dibutuhkan jaminan keamanan informasi terhadap kerahasiaan,

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

keutuhan, ketersediaan, keotentikan, dan nir penyangkalan dari informasi yang dikelola.

BSSN sebagai Lembaga pemerintah yang memiliki tugas dan wewenang dalam bidang siber dan persandian siap memberikan dukungan pengamanan teknologi di ruang siber pada lingkungan pemerintah, infrastruktur informasi kritikal nasional, dan ekonomi *digital*, termasuk pada bidang pertahanan dan keamanan. Bidang pertahanan dan keamanan merupakan salah satu bidang strategis yang tentunya dapat menjadi target serangan, baik serangan yang dilakukan oleh individu, komunitas, bahkan negara. Penyerang yang disponsori oleh negara merupakan penyerang yang paling membahayakan karena memiliki sumberdaya yang tidak terbatas yang disediakan oleh negara. TNI sebagai institusi yang memilik aset strategis terkait keamanan dan pertahanan negara, harus senantiasa memperhatikan keamananan siber dalam kerangka menjaga kedaulatan nasional. Maka dari itu perlu ditunjang dengan pertahanan siber yang kuat.

Pemerintah telah meresmikan *roadmap* menuju era baru industri 4.0 yang disebut dengan *Making* Indonesia 4.0. Hal ini memerlukan ketahanan siber yang dapat dijalankan dengan adanya 3 unsur yakni jaringan, konten, dan aplikasi. Apabila salah satunya tidak ada, maka siber tidak berjalan. Untuk menjalankan *roadmap* tersebut, seluruh pihak diharapkan memiliki komitmen dan dapat berpartisipasi aktif untuk bersama-sama mengejar kesiapan dalam

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

memasuki era baru tersebut, termasuk di dalamnya instansi pemerintah dan di dalamnya ada unsur TNI. Maka dari itu TNI perlu untuk bekerjasama dengan BSSN dalam penguatan keamanan siber dan persandian. Dengan persandian yang kuat, maka akan menjadi langkah awal menuju pertahanan dan keamanan siber nasional yang kuat.

Kementerian Pertahanan mempersiapkan puluhan ahli *internet* dan teknologi informasi atau *information technology (IT)* untuk membantu Badan Siber Nasional. Mereka dididik di berbagai institusi di dalam dan luar negeri. Para ahli IT akan mendukung lembaga siber yang sudah aktif di Kementerian Pertahanan. Menurut Ryamizard, ada *Cyber Defense* yang menangani pertahanan negara dari ancaman siber dari luar.

Ryamizard memastikan fungsi Badan Siber Nasional tak akan tumpang-tindih dengan institusi siber yang sudah ada. Saat ini, Kementerian Pertahanan memiliki *Cyber Defence*, Badan Intelijen Negara mempunyai *Cyber Intelligence*, dan Kepolisian RI memiliki *Cyber Security*. Lembaga-lembaga *cyber* itu akan tetap berfungsi seperti biasanya.

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mencatat lebih dari 143 juta pengguna aktif di *internet* pada 2017. Berdasarkan data tersebut, mereka yang menghabiskan waktu di media sosial hampir mencapai 70%. Jika 1% saja yang mereka unggah adalah materi negatif (ujaran kebencian, radikalisme,

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

pornografi, *hoax*, fitnah, dan adu domba), ada sekitar satu juta konten negatif di media sosial setiap hari yang bisa saja viral ke seantero jagat maya. Dilihat dari perspektif pertahanan negara, tentu hal ini menjadi ancaman serius. Perang siber adalah ancaman paling nyata yang bisa saja memorak-porandakan keutuhan dan kedaulatan NKRI akibat tidak terkendalinya konten-konten negatif di *internet*.

Dalam konteks Indonesia, memaknai perang siber bisa diartikan secara utuh ataupun tidak. Pemaknaan utuh artinya memang Indonesia mengartikulasikannya sebagai perang dalam pengertian sebenarnya. Namun, sebaliknya, perang tidak didefinisikan sebagai bertemunya dua pasukan atau lebih di medan laga. Perang senyap yang tidak kelihatan siapa musuh dan lawan, ini menjadi sesuatu yang sulit untuk dihadapi dan ancaman sebenarnya.

Tidak bisa dipungkiri, salah satu perilaku pengguna *internet* adalah berlomba-lomba unjuk diri, kelompok, ideologi, pemikiran, dan masih banyak lagi. Konstelasi ini kemudian menimbulkan "peperangan" untuk memengaruhi dunia *virtual*.

Atmosfer kegaduhan di media sosial terjadi karena masing-masing kelompok saling melempar isu bernuansa politik, ekonomi, ideologi, atau agama yang bisa dibilang tendensius dan provokatif. Kondisi ini melahirkan prasangka terhadap seseorang atau lembaga

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

berdasarkan persepsi (*stereotip*) karena dibangun berdasarkan sesuatu yang belum tentu sesuai kenyataan di dunia nyata.

Jika dibiarkan, ini berpotensi menimbulkan aksi di dunia nyata yang berujung pada bentrok, perang, maupun persaingan antar kelompok masyarakat. Ini yang menjadi inti perang siber, dimulai dari dunia maya dan bisa saja berakhir di dunia nyata. Jangan sampai kita menyesal karena terlambat menyadari ancaman yang sesungguhnya ada di depan mata.

Peningkatan Kemampuan Satuan Siber TNI AD merupakan upaya dalam mendukung tercapainya strategi keamanan siber nasional. Adapun strategi tersebut, yaitu :

a. Membentuk arsitektur siber kontemporer yang terdiri dari pemerintah, industri / swasta, akademisi dan komunitas / masyarakat. Pemerintah berperan dalam menjaga lingkungan siber nasional, melindungi *e-commerce* nasional, melindungi infrastruktur informasi kritis nasional, mengendalikan penetrasi Ipoleksosbudhankam, dan melindungi warga negara (*privacy*). Pihak swasta/industri turut berperan dalam penyedia kemampuan dasar siber yaitu: peralatan (*device*), piranti lunak (*software*) dan jaringan (satelit dan serat optik). Akademisi berperan sebagai penyedia kualitas SDM yang memiliki disiplin ilmu seperti ilmu komputer, sistem informasi, teknologi informasi, peperangan asimetris, rekayasa komputer atau

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

media siber. Sedangkan peran komunitas/masyarakat khusus siber sebagai komunitas otodidak siber, komunitas *hacker* khususnya *white and grey hacker*, komunitas Medsos, komunitas siber masyarakat yang dibina pemerintah atau swasta dan komunitas industri siber.

b. Menciptakan manajemen keamanan dan kontijensi berupa mekanisme pencegahan serangan siber, mekanisme penanganan keamanan siber dan mekanisme penanggulangan serangan siber.

c. Membentuk kolaborasi keamanan siber dengan cara bekerjasama dalam lingkup internasional, regional dan bilateral sesuai kebijakan politik luar negeri Indonesia dalam rangka peningkatan kapasitas dan kualitas kemampuan siber, tukar menukar informasi, membentuk regulasi dan penegakan hukum.

d. Meningkatkan penegakan hukum melalui penguatan kapabilitas penegak hukum, penegakan koordinasi antar penegak hukum, penegakan regulasi penegak hukum di ruang siber dan membuat regulasi transnasional.

e. Mengutamakan inovasi dan kreativitas melalui percepatan inovasi untuk mendukung kebijakan pemerintah dalam bidang *e-commerce* dan peningkatan kemampuan SDM di bidang siber untuk melindungi kebijakan ruang pemerintah di ruang siber.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

harus dapat berperan aktif sebagai salah satu satuan siber nasional yang bertugas untuk mengamankan pertahanan siber nasional bersama-sama dengan Satuan Siber TNI dan Kemhan, serta memiliki peranan dalam melakukan serangan siber terhadap ancaman kejahatan siber teroris ataupun pasukan siber negara lain. Sehingga dalam lingkup kepentingan di bidang siber nasional, Satuan Siber TNI AD dapat berperan aktif dalam mewujudkan *cyber defence* yang handal dan memberikan *input* di bidang pertahanan siber kepada BSSN selaku koordinator badan siber nasional. Sinergitas yang terbentuk antara BSSN dengan lembaga siber nasional lainnya juga harus didasari oleh pola kerjasama yang profesional dan berlandaskan hukum, sehingga tercipta suatu tingkat kepercayaan terhadap masing-masing badan siber tersebut. Dengan demikian transfer data kejahatan siber yang terjadi dan ditemukan oleh setiap badan siber dapat dengan segera terangkum di BSSN dan digunakan menjadi data strategis oleh negara. Penyedia data kejahatan siber di bidang *cyber defence* dilaksanakan oleh Satuan Siber TNI dan Kemhan, penyedia data *cyber crime* dilaksanakan oleh Satuan Siber Mabes POLRI, penyedia data kejahatan siber di bidang *cyber intelligent* dilaksanakan oleh Satuan Siber BIN dan penyedia data kejahatan siber di bidang informasi dan media sosial dilaksanakan oleh Satuan Siber Kemenkominfo, semua data tersebut tentunya bersifat by request untuk menghormati privasi dari masing-masing badan siber tersebut. Namun, hal yang terpenting dalam sinergitas ini adalah kecepatan dan kevalidan data yang dihimpun serta kepercayaan dan kesolidan antar lembaga/badan siber itu sendiri. Dengan demikian

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

pada akhirnya akan tercipta sinergitas yang sangat kuat antar lembaga/badan siber nasional dalam mewujudkan kemampuan siber nasional yang mumpuni dan dapat diandalkan dalam menghadapi perkembangan kejahatan siber baik secara lokal, nasional, regional dan global.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

BAB V

KESIMPULAN DAN SARAN

A. Kesimpulan

Kesimpulan umum penelitian menggambarkan bahwa faktor ancaman kejahatan siber memiliki banyak sekali pengaruhnya terhadap Institusi TNI AD. Satuan Siber TNI AD yang ada pada saat ini perlu ditingkatkan fungsinya dengan kemampuan ofensif untuk menunjang kolaborasi dengan satuan siber nasional. Simpulan khusus pada penelitian ini adalah sebagai berikut:

Satu, tren kejahatan siber merupakan bentuk kejahatan yang mengancam dunia nyata meskipun dilakukan melalui dunia maya, oleh para *hacker* yang dapat masuk ke jaringan atau sistem informasi di suatu instansi seperti TNI AD. Hal ini sangat berbahaya, karena satuan TNI AD sebagai alat pertahanan negara memiliki banyak basis data/informasi rahasia dan Alutsista yang saat ini hampir seluruh penggunaanya berbasis komputer. Oleh karena itu, ancaman kejahatan siber mempengaruhi peningkatan fungsi Satuan Siber TNI AD untuk mencegah terjadinya sabotase, pencurian data rahasia militer dengan menggunakan sistem enkripsi, *hacking*, teror *digital*, serangan psikologi siber dan serangan terhadap infrastruktur dan sistem informatika TNI AD.

Dua, dalam upaya peningkatan fungsi Satuan Siber TNI AD masih terdapat beberapa faktor penghambat, yaitu: 1. Keterbatasan kemampuan sumberdaya manusia di bidang Siber. 2. Keterbatasan sarana dan prasarana

Koleksi Perpustakaan Universitas Terbuka

kepemilikan alat canggih berbasis IT dan teknologi guna menghadapi serangan kejahatan siber. 3. Masih lemahnya hukum perundang-undangan di Indonesia, termasuk peraturan dan ketentuan hukum yang mengatur Satuan siber TNI AD. 4. Masih terbatasnya koordinasi lintas sektoral antar satuan pendukung guna menghadapi kejahatan siber.

Tiga, peran Satuan Siber TNI AD dalam mendukung sinergitas lembaga siber nasional untuk mengungkap kejahatan siber saat ini hanya sebagai satuan yang bertugas untuk *monitoring* dan pelaporan konten/berita *hoax* dalam rangka menangkal serangan psikologi siber lawan ke institusi TNI AD. Untuk itu perlu peningkatan fungsi agar peran tersebut berubah tidak hanya pertahanan, akan tetapi juga dapat berperan sebagai : 1. Satuan *Cyber Attack* TNI AD yang dapat menyerang dan mampu menghadapi serta mengungkap kejahatan siber baik itu program maupun pelakunya sehingga *hacker* memiliki ketakutan tersendiri untuk masuk dan meretas institusi TNI AD sebagai alat pertahanan Negara. 2. Kontributor, di mana Satuan Siber TNI AD yang merupakan bagian dari Satuan Siber Nasional dapat memberikan kontribusi positif bagi bidang pertahanan dan keamanan dalam menjawab tantangan Revolusi Industri 4.0 melalui pencegahan serangan siber, penanganan keamanan siber dan penanggulangan serangan siber terhadap sistem pertahanan nasional. 3. Inisiator, di mana Satuan Siber TNI AD menjadi inisiator bagi satuan intelijen dan pendukung guna membentuk satuan siber yang handal dan mumpuni, sehingga diperoleh kondisi yang diharapkan yaitu berkurangnya aktivitas *hacking*, menurunnya pemberitaan *hoax* dan terkontrolnya teror

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

digital yang tidak hanya menyerang individu melainkan juga institusi TNI AD. 4. Fasilitator, di mana Satuan Siber TNI AD berperan dalam memfasilitasi satuan siber jajaran di bawahnya (Siber Kopassus, Dithubad, PII Pusintelad, Disinfolahtad dan Dispenad) dalam berkoordinasi dengan Satuan *Cyber Defence* TNI dan Kemhan, Satuan *Cyber Crime* POLRI, Satuan *Cyber Intelligence* BIN dan Satuan Siber BSSN serta Kemkominfo.

B. Saran

Berdasarkan pembahasan dan kesimpulan yang telah diuraikan sebelumnya, peneliti mengajukan beberapa saran di antaranya :

1. Untuk internal TNI AD guna menghadapi kejahatan siber
   a. Meningkatkan kemampuan sumberdaya manusia bagi personel Satuan Siber TNI AD dengan cara:
      1) Melakukan percepatan pembekalan ilmu intelijen, persandian dan siber yang selalu *up date* melalui kursus dasar persandian dan intelijen yang diadakan di BSSN, Kemhan dan Mabes TNI.
      2) Melakukan perekrutan personel tahap ketiga sejumlah 30 orang, namun dengan mengutamakan pada personel yang sudah memiliki minimal dua klasifikasi dari tiga klasifikasi mutlak yang dibutuhkan, yaitu: siber, intelijen dan persandian.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

b. Meningkatkan sarana dan prasarana siber dengan pengadaan infastruktur siber yang modern serta ditunjang oleh aplikasi/*software* terbaru secara bertahap sesuai dengan Rencana Strategis Angkatan Darat, tidak hanya peralatan untuk pelaksanaan tugas *monitoring* dan *defensif* melainkan peralatan yang menunjang kemampuan *ofensif* dan *tracking digital* dengan daya jangkau yang luas.

Beberapa hal yang layak untuk segera dimiliki dalam infrastruktur Satuan Siber TNI AD yaitu:

1) *Security Operation Centre* (SOC). Merupakan sistem pengamanan jaringan komputer yang mampu *memonitor* aktivitas dan memberikan laporan jika terjadi insiden intrusi (usaha orang luar masuk ke dalam infrastruktur/jaringan komputer atau sistem informasi/sisfo).

2) *Vulnerability assessment*. Merupakan usaha yang dilakukan untuk menemukan celah keamanan pada sisi sistem informasi, aplikasi yang dibangun dan metode kerja yang diawaki personel. Kegiatan ini juga sangat berguna untuk menangkal tindakan sabotase *digital*.

3) Metode kerja *fraud* (penipuan) *security*. Merupakan kegiatan forensik dalam transaksi *digital*. Sebagai bagian dari kegiatan forensik *digital* yang secara

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

khusus membuktikan terjadinya kejahatan siber dengan melihat aspek perilaku. Pelaku tindak kejahatan *fraud* dapat dideteksi dan ditangkal dari aspek perilaku serta pembuktian tindak pidana kejahatan terorganisasi *digital* bukan pidana umum penipuan.

4) Metode standar keamanan informasi Satuan TNI AD, seperti penerapan penyandian terhadap informasi berklasifikasi rahasia dan layanan dalam bentuk layanan informasi yang dapat diakses dalam lingkungan organisasi TNI AD.

Satuan Siber TNI AD juga idealnya harus selalu memperoleh *up date* peralatan dan bimbingan teknik tentang siber dari tenaga ahli mitra TNI AD baik secara rutin maupun berkala agar personel siber mendapat *up grade* kemampuan secara terus menerus.

c. Meningkatkan dan mempercepat jalur birokrasi dengan cara:

1) Koordinasi dan korelasi internal satuan TNI AD melalui validasi organisasi satuan pendukung, yaitu: Satuan Siber TNI AD, Disinfohlatad, Dithubad, Dispenad, Siber Kopassus dan PII Pusintelad untuk menentukan kebijakan dan langkah-langkah

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

penanganan dalam respon cepat terhadap kejahatan siber.

2) Satuan Siber TNI AD memiliki satu jaringan *online* dengan Dithubad selaku penyedia infrastruktur, Disinfolahtad selaku penyedia sistem jaringan, PII Pusintelad selaku penyedia pelacak/*tracking digital* dan penyedia data, Dispenad selaku pemberi respon cepat klarifikasi resmi TNI AD dan Siber Kopassus selaku badan pelaksana pusat untuk melakukan serangan siber apabila fungsi Satuan Siber TNI AD telah ditingkatkan.

3) Membentuk jaringan *online* dan sistem pelaporan berjenjang secara hirarkis antara Satuan Siber TNI AD dengan Spamad selaku supervisi pengamanan TNI AD, Sintel TNI selaku supervisi pengamanan TNI, Bais TNI selaku badan pelaksana pusat bidang intelijen dan pengamanan TNI dan Satkomlek TNI selaku penyedia jaringan persandian dan infrastruktur TNI.

4) Membentuk satu jaring besar koordinasi antara Kemkominfo, Kemhan, BIN, BSSN, Mabes TNI dan Mabes POLRI, kemudian jaring utama tersebut diteruskan ke bagian satuan kecil masing-masing. Untuk satuan siber di masyarakat sipil menginduk

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

kepada Kemkominfo, satuan siber jajaran POLRI menginduk kepada Mabes POLRI dan satuan jajaran TNI (termasuk Satuan Siber TNI AD) menginduk kepada Satuan Siber Mabes TNI. Dengan demikian akan terbentuk jaringan *online* yang akan memonitor kejahatan di dunia maya dan apabila ditemukan adanya pelaku yang melakukan aktivitas kejahatan siber maka akan dengan segera dapat diambil tindakan tentunya setelah adannya laporan dari pihak/instansi yang menjadi korban. Dengan adanya sistem yang terintegrasi secara *online* ini maka akan mengurangi manajemen resiko dan keraguan personel siber dalam melaksanakan tugasnya, dikarenakan sudah ada prosedur dan mekanisme kerja serta yang tidak kalah pentingnya sudah ada payung hukum yang melindungi baik secara hukum sipil maupun hukum militer. Di sisi lain adanya sistem yang terintegrasi ini akan sangat membantu pemerintah dalam menentukan kejahatan siber mana yang dinilai membahayakan kedaulatan negara dan kejhatan siber mana yang mengganggu privasi pribadi individu ataupun suatu organisasi.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

2. Untuk lingkup nasional guna menghadapi kejahatan siber

   a. Melakukan pendekatan antar *stakeholder* di bidang siber nasional dengan cara:

      1) Membangun pusat pengendalian operasi siber nasional.

      2) Membangun *National Information Exchange Network.*

      3) Peningkatan *partnership* pihak swasta.

      4) Membangun forum informal di masyarakat.

      5) Pemberdayaan komunitas keamanan siber.

      6) Mendorong *public key infrastructure* dengan *Certification Authority* (CA).

   b. Dalam menghadapi Revolusi Industri 4.0 perlu diterapkannya kebijakan strategi keamanan siber nasional, yaitu:

      1) Membentuk arsitektur siber kontemporer yang terdiri atas pemerintah, industri/swasta, akademisi dan komunitas/masyarakat.

      2) Menciptakan manajemen keamanan dan kontijensi berupa mekanisme pencegahan serangan siber, mekasnisme penanganan keamanan siber dan mekanisme penanggulangan serangan siber.

      3) Membentuk kolaborasi keamanan siber dengan cara bekerjasama dalam lingkup internasional, regional

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

dan bilateral sesuai kebijakan politik luar negeri Indonesia dalam rangka peningkatan kapasitas dan kualitas kemampuan siber, tukar menukar informasi, membentuk regulasi dan penegakan hukum.

4) Meningkatkan penegakan hukum melalui penguatan kapabilitas penegak hukum, penegakan koordinasi antar penegak hukum, penegakan regulasi penegak hukum di ruang siber dan membuat regulasi transnasional.

5) Mengutamakan inovasi dan kreativitas melalui percepatan inovasi untuk mendukung kebijakan pemerintah dalam bidang *e-commerce* dan peningkatan kemampuan SDM di bidang siber untuk melindungi kebijakan ruang pemerintah di ruang siber.

c. Membuat peraturan/ketentuan hukum yang mengatur pelaksanaan mekanisme kerja Satuan Siber TNI AD yang merupakan turunan dari Undang-Undang No.11 Tahun 2008 tentang informasi dan transaksi elektronik dalam tindak pidana siber, antara lain:

1) Aturan atau regulasi teknis yang mengatur mekanisme pelaksanaan kerjasama antara Satuan Siber Kemkominfo, Kemhan, BIN, BSSN, POLRI dan TNI, sehingga terbentuk regulasi yang memiliki

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

prosedur jelas bagi setiap personel siber baik sipil maupun militer dalam mengambil langkah penyelesaian masalah.

2) Aturan atau regulasi tentang penanganan dan penindakan kejahatan siber bila pelakunya dari masyarakat sipil atau instansi sipil dan bagaimana penyelesaiannya apabila pelakunya militer ataupun instansi militer.

3) Aturan dan regulasi yang merupakan turunan dari UU ITE yang mengatur bidang pertahanan dan keamanan karena militer memiliki pola birokrasi yang khusus.

4) Aturan dan regulasi yang mengatur mekanisme kerjasama siber lintas negara dan penanganan serta penindakan kejahatan siber lintas negara.

Koleksi Perpustakaan Universitas Terbuka

DAFTAR PUSTAKA

Alfatih, R. 2017. Siber dalam Revolusi Industri Ke-4, Hambatan atau Tantangan. Jakarta: www.rinoalfatih.wordpress.com.

Arief, B. N. 2006. Tindak Pidana Mayantra: Perkembangan Kajian *Cyber Crime* di Indonesia. Jakarta: Raja Grafindo Persada.

Badan Siber dan Sandi Negara. 2018. BSSN Perkuat Keamanan Siber TNI. Jakarta: www.bssn.go.id.

Badio, Sabjan. 2018. Apakah yang Dimaksud Masyarakat 5.0 atau *New Society* Menurut Pemerintah Jepang?. Jakarta: www. Abasrin.com.

Badio, Sabjan. 2018. Contoh Penerapan Nilai Baru Masyarakat 5.0 dalam Berbagai Bidang Menurut Pemerintah Jepang. Jakarta: www. Abasrin.com.

Chinn, D. 2018. Indonesia Rentan Kena Serangan Siber. Jakarta: CNN Indonesia.

Hakim, Riyan. 2017. Sinergitas Kelembagaan Publik dalam Mendukung Tercapainya Visi Organisasi. Jakarta: www.tugaskuliah.com

Harahap, M. Y. 2006. Pembahasan Permasalahan dan Penerapan Hukum (edisi Kedua). Jakarta: Sinar Grafika.

Hasanah, S. 2018. Landasan Hukum Penanganan *Cybercrime* di Indonesia. Jakarta: www.hukumonline.com.

Hutabarat, D. 2018. Agama Sebagai Pertahanan Siber. Jakarta: www.kominfo.go.id.

Irianto, Jusuf. 2011. Manajemen Sumber Daya Manusia Sektor Publik di Indonesia: Pengantar Pengembangan Model MSDM Sektor Publik. Jakarta: www.journal.unair.ac.id.

Kristo, F.Y. 2016. Bedah UU ITE: 7 Poin Utama Revisi UU ITE. Jakarta: www.detik.com.

Kurnia N. M, E. 2014. Kebijakan Strategi Keamanan *Cyber* Nasional. Jakarta: www.academia.edu.

Mastel. 2016. *Revisi UU ITE Dorong* Netizen agar Lebih Bijak. Jakarta: www.mastel.id.

Mayasari, Deasy. 2019. Mengenal *Society* 5.0, Transformasi Kehidupan yang Dikembangkan Jepang. Jakarta: www.timesindonesia.co.id.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Paskalis, Y. 2017. Kementerian Pertahanan Siapkan 50 Ahli IT untuk Awak Badan *Cyber* Nasional. Jakarta: www.nasional.tempo.com.

Raharjo, A. 2002. *Cyber Crime* Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi. Bandung: PT. Citra Aditya Utama.

Randi, Y. 2000. Proteksi terhadap Kriminalitas dalam Bidang Komputer. Bandung: PT. Citra Aditya Utama.

Ridwan, S. 2018. Revolusi Industri 4.0, Panglima TNI Targetkan Alutsista Berbasis *Digital*. Jakarta: www.reliji.com.

Rodrigues, A. 2018. *Cybersecurity* untuk Revolusi Industri 4.0. Jakarta: www.indotelko.com.

Sasongko, B. J. 2018. TNI dan Tantangan Revolusi Industri 4.0. Jakarta: www.beritasatu.com.

Sitompul, Josua. 2012. *Cyberspace, Cybercrimes, Cyberlaw*: Tinjauan Aspek Hukum Pidana. Jakarta: Tatanusa.

Slaughter Steven. 1999. *Cosmopolitan Governance: Building Global Democracy*. Jakarta: www.springer.com.

Subagyo, A. 2015. Sinergi dalam Menghadapi Ancaman *Cyberwarfare*. Bandung: www.researchgate.net.

Surat Perintah Kasad Nomor Sprin/2103/VI/2018 yang berisi tentang perintah melaksanakan Satgas *Cyber Defence* Tahun 2018.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Wahid, A. 2005. Kejahatan Mayantara (*Cyber Crime*). Malang: Fakultas Hukum Unisma.

Wanda, P. 2018. Menegakkan Kedaulatan Siber di Nusantara. Jakarta: www.student.cnnindonesia.com.

Wibowo, S. 2018. BSSN dan Peta Keamanan Siber Indonesia. Jakarta: www.detik.com

Ziadah, O. 2016. Latar Belakang Perubahan Undang-Undang ITE. Jakarta: www.marlekum.com.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

PANDUAN WAWANCARA
(Informan Kunci: Perwira Satuan Siber TNI AD)

Cara menjawab :

1. Mohon Bapak dapat mengisi identitas pada bagian A dengan lengkap.
2. Mohon Bapak isi pertanyaan dari bagian B sampai dengan E sesuai dengan apa yang Bapak ketahui.

A. Karakteristik Informan

1. Nama :
2. Umur :
3. Jenis Kelamin :
4. Pangkat/Satuan :

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   .....
2. Kapan menurut Bapak ancaman *kejahatan siber akan mengancam* institusi TNI AD?
   .....
3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   .....
4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana institusi TNI AD?
   .....
5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   .....
6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD?
   .....

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   .....
2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   .....
3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

.....

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?

.....

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?

.....

D. Informasi untuk menggali pentingnya peningkatan fungsi Satuan Siber TNI AD

1. Apakah menurut pandangan Bapak, Satuan Siber yang sudah dibentuk cukup untuk menghadapi kejahatan siber?

.....

2. Kapan menurut pandangan Bapak Satuan Siber perlu adanya peningkatan fungsi?

.....

3. Menurut pandagan Bapak, siapa yang dapat melakukan peningkatan funsi Satuan Siber?

.....

4. Pada bagian mana Satuan siber perlu peningkatan fungsi?

.....

5. Mengapa Satuan Siber perlu peningkatan fungsi?Berikan pandangan Bapak.

.....

6. Bagaimana menurut pandangan Bapak cara untuk peningkatan fungsi Satuan Siber TNI AD?

.....

E. Informasi untuk menggali pandangan mengenai faktor penghambat peningkatan fungsi Satuan Siber TNI AD

1. Apa saja menurut pandangan Bapak yang menjadi faktor penghambat peningkatan fungsi Satuan Siber TNI AD ?

.....

2. Berikan pandangan Bapak, siapa saja yang dapat menghambat dalam peningkatan fungsi satuan siber TNI AD?

.....

3. Pada bagian faktor penghambat mana yang dapat diperbaiki untuk disegerakan dalam peningkatan fungsi Satuan Siber TNI AD?

.....

4. Mengapa menurut pandnagan Bapak, faktor penghambat perlu segera diperbaiki?

.....

5. Bagaimana menurut pandangan Bapak cara untuk mengatasi faktor penghambat agar segera terjadi peningkatan fungsi Satuan Siber TNI AD?

.....

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

PANDUAN WAWANCARA
(Informan Kunci: Perwira Spamad)

Cara menjawab :

1. Mohon Bapak dapat mengisi identitas pada bagian A dengan lengkap.
2. Mohon Bapak isi pertanyaan dari bagian B sampai dengan E sesuai dengan apa yang Bapak ketahui.

A. Karakteristik Informan

1. Nama :
2. Umur :
3. Jenis Kelamin :
4. Pangkat/Satuan :

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   .....
2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   .....
3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   .....
4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana institusi TNI AD?
   .....
5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   .....
6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD?
   .....

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   .....
2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   .....
3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

.....

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?

.....

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?

.....

D. Informasi untuk menggali pentingnya peningkatan fungsi Satuan Siber TNI AD

1. Apakah menurut pandangan Bapak, Satuan Siber yang sudah dibentuk cukup untuk menghadapi kejahatan siber?

.....

2. Kapan menurut pandangan Bapak Satuan Siber perlu adanya peningkatan fungsi?

.....

3. Menurut pandagan Bapak, siapa yang dapat melakukan peningkatan funsi Satuan Siber?

.....

4. Pada bagian mana Satuan siber perlu peningkatan fungsi?

.....

5. Mengapa Satuan Siber perlu peningkatan fungsi?Berikan pandangan Bapak.

.....

6. Bagaimana menurut pandangan Bapak cara untuk peningkatan fungsi Satuan Siber TNI AD?

.....

E. Informasi untuk menggali pandangan mengenai faktor penghambat peningkatan fungsi Satuan Siber TNI AD

1. Apa saja menurut pandangan Bapak yang menjadi faktor penghambat peningkatan fungsi Satuan Siber TNI AD ?

.....

2. Berikan pandangan Bapak, siapa saja yang dapat menghambat dalam peningkatan fungsi satuan siber TNI AD?

.....

3. Pada bagian faktor penghambat mana yang dapat diperbaiki untuk disegerakan dalam peningkatan fungsi Satuan Siber TNI AD?

.....

4. Mengapa menurut pandnagan Bapak, faktor penghambat perlu segera diperbaiki?

.....

5. Bagaimana menurut pandangan Bapak cara untuk mengatasi faktor penghambat agar segera terjadi peningkatan fungsi Satuan Siber TNI AD?

.....

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

PANDUAN WAWANCARA
(Informan Kunci: Prajurit Satuan Siber TNI AD)

Cara menjawab :

1. Mohon Bapak dapat mengisi identitas pada bagian A dengan lengkap
2. Mohon Bapak isi pertanyaan dari bagian B dan C sesuai dengan apa yang Bapak ketahui.

A. Karakteristik Informan

1. Nama :
2. Umur :
3. Jenis Kelamin :
4. Pangkat/Satuan :

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   .....
2. Kapan *menurut Bapak ancaman kejahatan siber akan mengancam* institusi TNI AD?
   .....
3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   .....
4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana institusi TNI AD?
   .....
5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   .....
6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD ?
   .....

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   .....

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?

.....

3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?

.....

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?

.....

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?

.....

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

PANDUAN WAWANCARA
(Informan Kunci: Prajurit Spamad)

Cara menjawab :

1. Mohon Bapak dapat mengisi identitas pada bagian A dengan lengkap
2. Mohon Bapak isi pertanyaan dari bagian B dan C sesuai dengan apa yang Bapak ketahui.

A. Karakteristik Informan

1. Nama :
2. Umur :
3. Jenis Kelamin :
4. Pangkat/Satuan :

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   .....
2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   .....
3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   .....
4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana institusi TNI AD?
   .....
5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   .....
6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD ?
   .....

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   .....

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?

.....

3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?

.....

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?

.....

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?

.....

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

TRANSKRIP WAWANCARA
(Informan Kunci: Komandan Satuan Siber TNI AD/Informan A)

A. Karakteristik Informan

1.	Nama	:	Subur Wahono
2.	Umur	:	42 Tahun
3.	Jenis Kelamin	:	Laki-Laki
4.	Pangkat/Satuan	:	Letkol Chb/Siber TNI AD

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui *mengenai tren ancaman kejahatan siber*?
   Adalah kejahatan yang memanfaatkan media jaringan internet global (internet).

2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   Setiap saat, bahkan sudah dimulai sejak lama namun kita banyak yang tidak mengetahui dan menyadari kejahatan ini.

3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   Semua pihak yang menguasai IT, baik itu perorangan atau organisasi **maupun pihak sipil atau militer**.

4. **Bagaimana pandangan Bapak** mengenai kejahatan Siber dan pada **bagian mana menyerang institusi** TNI AD?
   Kejahatan siber sama dengan kejahatan dalam alam nyata. Dalam kaitannya dengan TNI AD, potensi kejahatan siber juga mengancam secara institusi dan personal.

5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   Adanya sistem informasi yang tidak diamankan secara baik. Kepemilikan Sisfo yang ternyata hanya memiliki pengaturan standar pabrik dan tidak dilakukan perubahan pengaturan secara maksimal sangat mengundang penyerang dalam bidang siber.

6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD?
   Melalui penyebaran berita *hoax* di Medsos, melalui penggunaan grup Medsos yang terenkripsi oleh teroris, melalui penyadapan, sabotase dan perusakan jaringan komputer.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   Satuan Siber TNI AD belum ada. Kebijakan pembentukan masih dalam tahap kajian. Saat ini baru berupa Satuan Tugas Siber TNI AD.

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   Secepatnya, peningkatan fungsi satuan siber wajib dilakukan. Selain menangkal datangnya ancaman dari serangan *hacker* terhadap sisfo TNI AD, kemampun personel perlu ditingkatkan dan dikelola agar handal.

3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?
   Prajurit yang memiliki dasar intelijen, persandian dan pengetahuan IT dan siber.

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?
   Harapannya Satuan Siber adalah pelaksana fungsi militer khusus yang setara dengan keberadaan Pasukan Khusus yang memiliki kecakapan tinggi dalam peperangan dengan taktik non konvensional.

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?
   Pembentukan Satuan Siber dalam tahap kajian dan belum memberikan kontribusi memadai dalam merespon ancaman siber secara infrastruktur dan aplikasi.

D. Informasi untuk menggali pentingnya peningkatan fungsi Satuan Siber TNI AD

1. Apakah menurut pandangan Bapak, Satuan Siber yang sudah dibentuk cukup untuk menghadapi kejahatan siber?
   Belum cukup karena baru berfungsi sebagai alat pertahanan dan *monitoring* media saja.

2. Kapan menurut pandangan Bapak Satuan Siber perlu adanya peningkatan fungsi?
   Segera mungkin, karena kejahatan siber sudah marak menyerang institusi TNI AD.

3. Menurut pandangan Bapak, siapa yang dapat melakukan peningkatan funsi Satuan Siber?
   Berdasarkan keputusan dan kebijakan pemerintah dan unsur pimpinan TNI dan TNI AD.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

4. Pada bagian mana Satuan siber perlu peningkatan fungsi?
   Pada bagian penindakan ditingkatkan kemampuannya bukan hanya *monitoring* berita saja melainkan dapat melakukan tindakan ofensif seperti pendeteksian jaringan yang ditembus lawan dan melakukan serangan balasan.

5. Mengapa Satuan Siber perlu peningkatan fungsi?Berikan pandangan Bapak.
   Peningkatan fungsi satuan siber wajib dilakukan. Selain menangkal datangnya ancaman dari serangan *hacker* terhadap sisfo TNI AD, kemampun personel perlu ditingkatkan dan dikelola agar handal.

6. Bagaimana menurut pandangan Bapak cara untuk peningkatan fungsi Satuan Siber TNI AD?
   Melalui peningkatan kemampuan SDM, sarana dan prasarana serta peralatan canggih yang memiliki kemampuan untuk melakuakan serangan siber.

E. Informasi untuk menggali pandangan mengenai faktor penghambat peningkatan fungsi Satuan Siber TNI AD

1. Apa saja menurut pandangan Bapak yang menjadi faktor penghambat peningkatan fungsi Satuan Siber TNI AD ?
   Faktor penghambat terhadap peningkatan fungsi Satuan Siber TNI AD antara lain adalah kepercayaan yang kurang dalam tataran pimpinan. Para pimpinan mempertanyakan bukti nyata adanya serangan siber secara infrastruktur kepada TNI AD. Kesadaran bahwa siber telah mengancam belum nyata. Padahal pada April 2017 Seluruh Sisfo TNI AD dimatikan agar tidak diserang Ransomware Wnnacry. Seolah langkah ini tepat, tapi dalam konteks adanya serangan, bagaimana mau menang menghadapi serangan, orang sisfonya saja sudah mati sebelum datangnya serangan.

2. Berikan pandangan Bapak, siapa saja yang dapat menghambat dalam peningkatan fungsi satuan siber TNI AD?
   Setiap prajurit dari level pimpinan sampai dengan pelaksana yang belum menyadari besarnya ancaman perang siber, sehingga merasa peningkatan fungsi Satuan Siber TNI AD bukan hal vital dan harus diprioritaskan.

3. Pada bagian faktor penghambat mana yang dapat diperbaiki untuk disegerakan dalam peningkatan fungsi Satuan Siber TNI AD?
   Pada peningkatan kualitas SDM dan pengadaan sarana dan prasarana yang canggih.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

4. Mengapa menurut pandangan Bapak, faktor penghambat perlu segera diperbaiki?
   Agar dapat mengamankan serangan siber yang masuk ke institusi TNI AD, sekaligus mendukung upaya pemerintah membentuk suatu satuan siber nasional yang teritegrasi.

5. Bagaimana menurut pandangan Bapak cara untuk mengatasi faktor penghambat agar segera terjadi peningkatan fungsi Satuan Siber TNI AD?
   Peningkatan kualitas SDM memalui pendidikan dan kursus intelijen, sandi dan siber, pengadaan sarana dan prasarana yang canggih dan modern, memperjelas status hukum sdampai level pelaksanaan teknis di lapangan serta memotong jalur birokrasi yang terlalu panjang dan memakan waktu lama melalui pembentukan satuan siber nasional yang terintegrasi.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

TRANSKRIP WAWANCARA
(Informan Kunci: Perwira Seksi Pengamanan dan Operasi Satuan Siber TNI AD/Informan B)

A. Karakteristik Informan

1.	Nama	:	Kiki Rezki Ramadhan
2.	Umur	:	30 Tahun
3.	Jenis Kelamin	:	Laki-Laki
4.	Pangkat/Satuan	:	Kapten Kav/Siber TNI AD

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   Adalah kejahatan yang bertentangan dengan hukum yang dilakukan *melalui pemanfaatan kemajuan IT sebagai media perantaranya dengan* berrmacam-macam pola seperti serangan terhadap infrastruktur siber melalui program virus/*malware* dan *ransomware* dan serangan psikologi siber melalui berita *hoax*, propaganda dan lainnya.

2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   Setiap saat, bahkan sudah banyak yang masuk ke institusi TNI AD terutama penyebaran berita *hoax* namun kita banyak yang tidak mengetahui dan menyadari kejahatan ini.

3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   Semua pihak yang menguasai IT, baik itu perorangan atau organisasi maupun pihak sipil atau militer.

4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana menyerang institusi TNI AD?
   Kejahatan siber dapat menyerang infrastruktur sisfo TNI AD,
   sehingga lawan dapat mengakses data-data yang bersifat rahasia milik TNI AD.

5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   Adanya sistem informasi yang tidak diamankan secara baik. Kepemilikan Sisfo yang ternyata hanya memiliki pengaturan standar pabrik dan tidak dilakukan perubahan pengaturan secara maksimal sangat mengundang penyerang dalam bidang siber.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD?
   Melalui penyebaran berita *hoax* di Medsos, melalui penggunaan grup Medsos yang terenkripsi oleh teroris, melalui penyadapan, sabotase dan perusakan jaringan komputer.

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   Satuan Siber TNI AD saat ini berupa satuan tugas yang membantu organisasi dalam menangani isu-isu terkait dengan TNI AD yang viral di media *online* yang bermuatan sentimen negatif.

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   Secepatnya, peningkatan fungsi satuan siber wajib dilakukan. Selain menangkal datangnya ancaman dari serangan *hacker* terhadap sisfo TNI AD, kemampun personel perlu ditingkatkan dan dikelola agar handal.

3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?
   Prajurit yang memiliki dasar intelijen, persandian dan pengetahuan IT dan siber.

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?
   Harapannya Satuan Siber adalah pelaksana fungsi militer khusus yang setara dengan keberadaan Pasukan Khusus yang memiliki kecakapan tinggi dalam peperangan dengan taktik non konvensional.

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?
   Belum mampu secara maksimal dalam menghadapi kejahatan siber dikarenakan teknologi terkait IT/siber senantiasa *update* setiap saat, sehingga proses belajar dan berlatih melalui metode kerja siber harus senantiasa di *update* juga.

D. Informasi untuk menggali pentingnya peningkatan fungsi Satuan Siber TNI AD

1. Apakah menurut pandangan Bapak, Satuan Siber yang sudah dibentuk cukup untuk menghadapi kejahatan siber?
   Belum cukup karena baru berfungsi sebagai alat pertahanan dan *monitoring* media saja.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

2. Kapan menurut pandangan Bapak Satuan Siber perlu adanya peningkatan fungsi?
   Segera mungkin, karena kejahatan siber sudah marak menyerang institusi TNI AD.

3. Menurut pandangan Bapak, siapa yang dapat melakukan peningkatan funsi Satuan Siber?
   Pemerintah dan unsur pimpinan TNI dan TNI AD.

4. Pada bagian mana Satuan siber perlu peningkatan fungsi?
   Pada bagian unit penindakan dan penanggulangan ditingkatkan kemampuannya bukan hanya *monitoring* berita saja melainkan dapat melakukan tindakan ofensif seperti pendeteksian jaringan yang ditembus lawan dan melakukan serangan balasan.

5. Mengapa Satuan Siber perlu peningkatan fungsi?Berikan pandangan Bapak.
   Peningkatan fungsi satuan siber wajib dilakukan. Selain menangkal datangnya ancaman dari serangan *hacker* terhadap sisfo TNI AD, kemampun personel perlu ditingkatkan dan dikelola agar handal.

6. Bagaimana menurut pandangan Bapak cara untuk peningkatan fungsi Satuan Siber TNI AD?
   Melalui peningkatan kemampuan SDM, sarana dan prasarana serta peralatan canggih yang memiliki kemampuan untuk melakukan serangan siber.

E. Informasi untuk menggali pandangan mengenai faktor penghambat peningkatan fungsi Satuan Siber TNI AD

1. Apa saja menurut pandangan Bapak yang menjadi faktor penghambat peningkatan fungsi Satuan Siber TNI AD ?
   Faktor penghambat terhadap peningkatan fungsi Satuan Siber TNI AD antara lain adalah kesadaran yang kurang akan tingkat bahaya dari kejahatan siber, kualitas SDM, infrastruktur, birokrasi dan kekuatan hukum yang belum jelas.

2. Berikan pandangan Bapak, siapa saja yang dapat menghambat dalam peningkatan fungsi satuan siber TNI AD?
   Setiap pimpinan sampai dengan prajurit pelaksana yang belum menyadari besarnya ancaman perang siber.

3. Pada bagian faktor penghambat mana yang dapat diperbaiki untuk disegerakan dalam peningkatan fungsi Satuan Siber TNI AD?
   Pada peningkatan kualitas SDM dan pengadaan sarana dan prasarana yang canggih.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

4. Mengapa menurut pandangan Bapak, faktor penghambat perlu segera diperbaiki?
   Agar dapat mengamankan serangan siber yang masuk ke institusi TNI AD, sekaligus mendukung upaya pemerintah membentuk suatu satuan siber nasional yang teritegrasi.

5. Bagaimana menurut pandangan Bapak cara untuk mengatasi faktor penghambat agar segera terjadi peningkatan fungsi Satuan Siber TNI AD?
   Peningkatan kesadaran akan pentingnya keamanan siber di semua level prajurit TNI AD,peningkatan kualitas SDM memalui pendidikan dan kursus intelijen, sandi dan siber, pengadaan sarana dan prasarana yang canggih dan modern, memiliki kekuatan hukum yang jelas dan birokrasi yang ringkas antar organisasi siber.

Koleksi Perpustakaan Universitas Terbuka

TRANSKRIP WAWANCARA
(Informan Kunci: Perwira Satuan Siber TNI AD/Informan C)

A. Karakteristik Informan

1.	Nama	:	Ady Basuki Kusumo
2.	Umur	:	27 Tahun
3.	Jenis Kelamin	:	Laki-Laki
4.	Pangkat/Satuan	:	Letnan Satu Inf/Siber TNI AD

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   Merupakan aktivitas kejahatan dengan menggunakan jaringan dan teknologi internet dengan sasaran para pengguna internet dan media sosial, seperti : Phising, yaitu pengelabuan URL/Web untuk mendapatkan credential dan spamming, yaitu pengiriman pesan/informasi palsu.

2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   Setiap saat, bahkan sudah banyak yang masuk ke institusi TNI AD terutama penyebaran berita *hoax* namun kita banyak yang tidak mengetahui dan menyadari kejahatan ini.

3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   Semua pihak yang menguasai IT, baik pihak sipil atau militer.

4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana menyerang institusi TNI AD?
   Kejahatan siber dapat menyerang infrastruktur sisfo TNI AD, sehingga lawan dapat mengakses data-data yang bersifat rahasia milik TNI AD.

5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   Adanya faktor kelalaian *user*/pengguna, faktor infrastruktur jaringan, faktor *software/platform*, faktor penguasaan keterampilan yang kurang baik/*skill lack*, faktor eksternal (serangan *hacker* di luar instansi).

6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD?
   Melalui penyerangan terhadap sisfo TNI AD, *website* dan semua Alutsista berbasis komputer milik TNI AD.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   Merupakan satuan tugas yang dibentuk untuk menghadapi/respon terhadap meningkatnya kejahatan siber.

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   Secepatnya, peningkatan fungsi satuan siber wajib dilakukan. Selain menangkal datangnya ancaman dari serangan *hacker* terhadap sisfo TNI AD, kemampun personel perlu ditingkatkan dan dikelola agar handal.

3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?
   Prajurit yang memiliki dasar intelijen, persandian dan pengetahuan IT dan siber.

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?
   Satuan Siber adalah pelaksana fungsi militer khusus yang bertanggungjawab langsung kepada Kasad.

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?
   Belum mampu karena masih dalam tahap pembangunan baik infrastruktur dan kemampuan SDM. Dibutuhkan percepatan untuk mengejar ketertinggalan terhadap keamanan informasi, baik di bidang infrastruktur maupun SDM.

D. Informasi untuk menggali pentingnya peningkatan fungsi Satuan Siber TNI AD

1. Apakah menurut pandangan Bapak, Satuan Siber yang sudah dibentuk cukup untuk menghadapi kejahatan siber?
   Belum cukup karena baru berfungsi sebagai alat pertahanan dan *monitoring* media saja serta belum adanya koordinasi lintas sektoral yang terintegrasi antar TNI, BSSN, Kemenkominfo, POLRI, dan Kemhan.

2. Kapan menurut pandangan Bapak Satuan Siber perlu adanya peningkatan fungsi?
   Segera mungkin, karena kejahatan siber sudah marak menyerang institusi TNI AD.

3. Menurut pandangan Bapak, siapa yang dapat melakukan peningkatan funsi Satuan Siber?
   Pemerintah dan unsur pimpinan TNI dan TNI AD.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

4. Pada bagian mana Satuan siber perlu peningkatan fungsi?
   Pada bagian unit penindakan dan penanggulangan ditingkatkan kemampuannya bukan hanya *monitoring* berita saja melainkan dapat melakukan tindakan ofensif.

5. Mengapa Satuan Siber perlu peningkatan fungsi?Berikan pandangan Bapak.
   Peningkatan fungsi satuan siber wajib dilakukan, karena belum mampu menghadapi kejahatan siber dengan kompleksitas tinggi. Upaya yang dilakukan baru sampai tahap monitoring dan pelaporan saja.

6. Bagaimana menurut pandangan Bapak *cara untuk peningkatan fungsi* Satuan Siber TNI AD?
   Melalui peningkatan kemampuan SDM, sarana dan prasarana serta peralatan canggih yang memiliki kemampuan untuk melakukan serangan siber serta koordinasi lintas sektoral antar satuan siber nasional.

E. Informasi untuk menggali pandangan mengenai faktor penghambat peningkatan fungsi Satuan Siber TNI AD

1. Apa saja menurut pandangan Bapak yang menjadi faktor penghambat peningkatan fungsi Satuan Siber TNI AD ?
   Faktor penghambat terhadap peningkatan fungsi Satuan Siber TNI AD antara lain adalah kualitas SDM, infrastruktur, birokrasi yang belum terintegrasi dan kekuatan hukum yang belum jelas.

2. Berikan pandangan Bapak, siapa saja yang dapat menghambat dalam peningkatan fungsi satuan siber TNI AD?
   Prajurit TNI AD yang belum menyadari besarnya ancaman perang siber.

3. Pada bagian faktor penghambat mana yang dapat diperbaiki untuk disegerakan dalam peningkatan fungsi Satuan Siber TNI AD?
   Pada peningkatan kualitas SDM dan pengadaan sarana dan prasarana yang canggih serta kerjasama lintas sektoral antar satuan siber nasional.

4. Mengapa menurut pandangan Bapak, faktor penghambat perlu segera diperbaiki?
   Agar dapat mengamankan serangan siber yang masuk ke institusi TNI AD, sekaligus mendukung upaya pemerintah membentuk suatu satuan siber nasional yang teritegrasi.

5. Bagaimana menurut pandangan Bapak cara untuk mengatasi faktor penghambat agar segera terjadi peningkatan fungsi Satuan Siber TNI AD?

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

Mengadakan/membentuk kelompok kerja untuk melakukan *assesment* internal dan eksternal guna memaksimalkan Satuan Siber TNI AD serta perlu dikaji lebih dalam dan detail terkait tugas satuan Siber TNI AD, sehingga menghindari duplikasi tugas yang telah dilakukan oleh satuan lain.

Koleksi Perpustakaan Universitas Terbuka

TRANSKRIP WAWANCARA
(Informan Kunci: Perwira Satuan Siber TNI AD/Informan D)

A. Karakteristik Informan

1.	Nama	:	Andi Nugroho
2.	Umur	:	38 Tahun
3.	Jenis Kelamin	:	Laki-Laki
4.	Pangkat/Satuan	:	Kapten Caj/Siber TNI AD

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   Merupakan kejahatan yang menggunakan komputer melalui jaringan yang terkoneksi satu sama lain.

2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   Setiap saat, bahkan sudah banyak yang masuk ke institusi TNI AD terutama penyebaran berita *hoax* namun kita banyak yang tidak mengetahui dan menyadari kejahatan ini.

3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   Semua pihak yang menguasai IT, baik pihak sipil atau militer.

4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana menyerang institusi TNI AD?
   Kejahatan siber menyerang institusi TNI AD terkait pengamanan data internal/data elektronik dan pengamanan berita dan kegiatan personel di dunia maya. Kegiatan perang operasi gabungan TNI AD yang menggunakan IT sebagai sarana dan prasarana utama dan pendukung dalam perang merupakan aset kritis infrastruktur yang harus diamankan dari kejahatan siber.

5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   Adanya faktor SDM tentang kejahatan siber yang masih rendah, faktor infrastruktur yang terbatas dan penggunaannya belum maksimal, faktor kebijakan dan aturan hukum yang belum ada terkait Satuan Siber TNI AD serta masih besarnya ego sektoral masing-masing satuan siber nasional.

6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD?

Koleksi Perpustakaan Universitas Terbuka

Melalui penyerangan terhadap sisfo TNI AD, *website* dan semua Alutsista berbasis komputer milik TNI AD.

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   Merupakan satuan tugas yang bertugas untuk melakukan pengamanan berita dan kegiatan di dunia maya.

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   Secepatnya, peningkatan fungsi satuan siber wajib dilakukan. Selain menangkal datangnya ancaman dari serangan *hacker* terhadap sisfo TNI AD, kemampun personel perlu ditingkatkan dan dikelola agar handal.

3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?
   Prajurit yang memiliki dasar intelijen, persandian dan pengetahuan IT dan siber.

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?
   Satuan Siber adalah pelaksana fungsi militer khusus yang bertanggungjawab langsung kepada Kasad.

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?
   Belum mampu karena masih dalam tahap pembangunan baik infrastruktur dan kemampuan SDM.

D. Informasi untuk menggali pentingnya peningkatan fungsi Satuan Siber TNI AD

1. Apakah menurut pandangan Bapak, Satuan Siber yang sudah dibentuk cukup untuk menghadapi kejahatan siber?
   Belum cukup karena baru berfungsi sebagai alat pertahanan dan *monitoring* media saja serta belum adanya koordinasi lintas sektoral yang terintegrasi.

2. Kapan menurut pandangan Bapak Satuan Siber perlu adanya peningkatan fungsi?
   Segera mungkin, karena kejahatan siber sudah marak menyerang institusi TNI AD.

3. Menurut pandangan Bapak, siapa yang dapat melakukan peningkatan funsi Satuan Siber?
   Pemerintah dan unsur pimpinan TNI dan TNI AD.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

4. Pada bagian mana Satuan siber perlu peningkatan fungsi?
   Pada bagian unit penindakan dan penanggulangan ditingkatkan kemampuannya bukan hanya *monitoring* berita saja melainkan dapat melakukan tindakan ofensif.

5. Mengapa Satuan Siber perlu peningkatan fungsi?Berikan pandangan Bapak.
   Peningkatan fungsi satuan siber wajib dilakukan, karena belum mampu menghadapi kejahatan siber dengan kompleksitas tinggi. Upaya yang dilakukan baru sampai tahap monitoring dan pelaporan saja.

6. Bagaimana menurut pandangan Bapak cara untuk peningkatan fungsi Satuan Siber TNI AD?
   Melalui peningkatan kemampuan SDM, sarana dan prasarana serta peralatan canggih yang memiliki kemampuan untuk melakukan serangan siber serta koordinasi lintas sektoral antar satuan siber nasional.

E. Informasi untuk menggali pandangan mengenai faktor penghambat peningkatan fungsi Satuan Siber TNI AD

1. Apa saja menurut pandangan Bapak yang menjadi faktor penghambat peningkatan fungsi Satuan Siber TNI AD ?
   Keterbatasan dukungan alat dan teknologi, belum memiliki kebijakan penggunaan teknologi informasi dan sistem informasi secara menyeluruh di lingkungan Angkatan Darat dan masih besarnya ego sektoral satuan lain.

2. Berikan pandangan Bapak, siapa saja yang dapat menghambat dalam peningkatan fungsi satuan siber TNI AD?
   Prajurit TNI AD yang belum menyadari besarnya ancaman perang siber.

3. Pada bagian faktor penghambat mana yang dapat diperbaiki untuk disegerakan dalam peningkatan fungsi Satuan Siber TNI AD?
   Pada peningkatan kualitas SDM dan pengadaan sarana dan prasarana yang canggih serta kerjasama lintas sektoral antar satuan siber nasional.

4. Mengapa menurut pandangan Bapak, faktor penghambat perlu segera diperbaiki?
   Agar dapat mengamankan aset infrastruktur kritis teknologi dan sistem informasi yang ada di lingkungan Angkatan Darat, sehingga TNI AD dapat mencapai level yang lebih baik dalam penggunaan teknologi dan sistem informasi.

Koleksi Perpustakaan Universitas Terbuka

5. Bagaimana menurut pandangan Bapak cara untuk mengatasi faktor penghambat agar segera terjadi peningkatan fungsi Satuan Siber TNI AD?
   Berkolaborasi bersama dengan satuan lain dengan pembagian tugas dan anggaran sesuai dengan porsi dan tugasnya.

Koleksi Perpustakaan Universitas Terbuka

TRANSKRIP WAWANCARA
(Informan Kunci: Prajurit Satuan Siber TNI AD/Informan E)

A. Karakteristik Informan

1.	Nama	:	Zuliananta
2.	Umur	:	30 Tahun
3.	Jenis Kelamin	:	Laki-Laki
4.	Pangkat/Satuan	:	Sersan Satu/Siber TNI AD

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   Merupakan dampak negatif yang timbul dari perkembangan teknologi dan aplikasi internet yang dapat berupa penyebaran virus dan *hacking*.

2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   Setiap saat, bahkan sudah banyak yang masuk ke institusi TNI AD terutama penyebaran berita *hoax* namun kita banyak yang tidak mengetahui dan menyadari kejahatan ini.

3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   Semua pihak yang menguasai IT, baik pihak sipil atau militer.

4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana menyerang institusi TNI AD?
   Kejahatan siber dapat menyerang infrastruktur sisfo TNI AD, sehingga lawan dapat mengakses data-data yang bersifat rahasia milik TNI AD.

5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   SDM yang dimiliki TNI AD untuk bidang siber masih rendah, infrastruktur siber milik TNI AD belum memadai dan sistem keamanan jaringan yang belum ada.

6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD ?
   Kejahatan siber sangat membahayakan institusi TNI yang juga mengikuti perkembangan teknologi di berbagai bidang yang mencakup administrasi data yang rahasia dan Alutsista.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   Satuan siber TNI AD masih dalam tahap satuan tugas dan dibutuhkan untuk mengamankan institusi TNI AD dari kejahatan siber dan perang siber.

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   Segera mungkin, karena kejahatan siber sudah marak menyerang institusi TNI AD.

3. Siapa saja menurut Bapak *yang perlu tergabung pada Satuan Siber* TNI AD?
   Prajurit yang memiliki dasar intelijen, persandian dan pengetahuan IT dan siber.

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?
   Satuan pelaksana fungsi khusus yang berkedudukan dan bertanggungjawab langsung di bawah Kasad.

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?
   Untuk saat ini Satuan Siber TNI AD belum maksimal karena masih terkendala masalah infrastruktur dan SDM yang kurang memadai, sehingga saat ini untuk penindakan dilakukan dengan cara melaporkan konten dan melakukan pendekatan secara persuasif terhadap pemilik akun di Medsos.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

TRANSKRIP WAWANCARA
(Informan Kunci: Prajurit Satuan Siber TNI AD/Informan F)

A. Karakteristik Informan

1.	Nama	:	Teguh Putra Muslimin
2.	Umur	:	26 Tahun
3.	Jenis Kelamin	:	Laki-Laki
4.	Pangkat/Satuan	:	Sersan Dua/Siber TNI AD

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   Merupakan suatu tindak kejahatan yang dilakukan orang, kelompok maupun organisasi dengan menggunakan perangkat komputer yang terhubung dengan jaringan internet di dunia maya yang berupa kejahatan yang menyangkut data atau informasi komputer, kejahatan yang menyangkut program atau software komputer, pemakaian fasilitas komputer tanpa wewenang untuk kepentingan yang tidak sesuai dengan tujuan pengelolaan, tindakan yang mengganggu operasi komputer dan tindakan merusak peralatan komputer.

2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   Setiap saat, bahkan sudah banyak yang masuk ke institusi TNI AD terutama penyebaran berita *hoax* namun kita banyak yang tidak mengetahui dan menyadari kejahatan ini.

3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   Semua pihak yang menguasai IT, baik pihak sipil atau militer.

4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana menyerang institusi TNI AD?
   Kejahatan siber dapat menyerang infrastruktur sisfo TNI AD, sehingga lawan dapat mengakses data-data yang bersifat rahasia milik TNI AD.

5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   SDM yang dimiliki TNI AD untuk bidang siber masih rendah, infrastruktur siber milik TNI AD belum memadai, sistem keamanan jaringan yang belum ada, sabotase dari pihak luar dan upaya pihak luar lainnya dalam hal mencuri data/informasi pertahanan negara.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD ?
   Kejahatan siber sangat membahayakan institusi TNI yang juga mengikuti perkembangan teknologi di berbagai bidang yang mencakup administrasi data yang rahasia dan Alutsista.

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   Satuan siber TNI AD adalah satuan yang bertugas mengamankan alat, sarana dan prasarana serta informasi rahasia yang dimiliki TNI AD dari serangan siber.

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   Segera mungkin, karena kejahatan siber sudah marak menyerang institusi TNI AD.

3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?
   Prajurit yang memiliki dasar intelijen, persandian dan pengetahuan IT dan siber.

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?
   Satuan pelaksana fungsi khusus yang berkedudukan dan bertanggungjawab langsung di bawah Kasad.

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?
   Untuk saat ini Satuan Siber TNI AD belum maksimal dalam menghadapi kejahatan siber, masih dalam tahap monitoring dan melakukan pelaporan ke komando atas.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

TRANSKRIP WAWANCARA
(Informan Kunci: Perwira Satuan Siber TNI AD/Informan G)

A. Karakteristik Informan

1.	Nama	:	Isnan Kurniawan
2.	Umur	:	25 Tahun
3.	Jenis Kelamin	:	Laki-Laki
4.	Pangkat/Satuan	:	Letnan Dua Chb/Siber TNI AD

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   Merupakan tindak kejahatan yang mulai berkembang saat ini dengan memanfaatkan sebuah teknologi komputer sebagai alat kejahatan primer dan timbul sejak adanya internet.

2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   Setiap saat, bahkan sudah banyak yang masuk ke institusi TNI AD terutama penyebaran berita *hoax* namun kita banyak yang tidak mengetahui dan menyadari kejahatan ini.

3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   Semua pihak yang menguasai IT, baik pihak sipil atau militer.

4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana menyerang institusi TNI AD?
   Kejahatan siber menyerang institusi TNI AD terkait pengolahan data yang telah menggunakan sistem operasi komputer dan jaringan internet. Data-data tersebut harus diamankan agar tidak bocor ke tangan pihak yang tidak bertanggungjawab.

5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   Adanya sistem keamanan jaringan yang kurang kuat, kelalaian operator/pengguna komputer, kurang sadarnya pengguna internet tentang kejahatan siber dan akses internet yang tanpa batas.

6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD?
   Melalui penyerangan terhadap sisfo TNI AD, *website* dan semua Alutsista berbasis komputer milik TNI AD.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   Merupakan satuan yang berada langsung di Angkatan Darat yang bertugas untuk melakukan *monitoring* dan penelusuran serta melakukan penindakan tentang kejahatan siber yang ditujukan kepada TNI AD.

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   Secepatnya, peningkatan fungsi satuan siber wajib dilakukan. Selain menangkal datangnya ancaman dari serangan *hacker* terhadap sisfo TNI AD, kemampun personel perlu ditingkatkan dan dikelola agar handal.

3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?
   Prajurit yang memiliki dasar intelijen, persandian dan pengetahuan IT dan siber.

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?
   Satuan Siber adalah pelaksana fungsi militer khusus yang bertanggungjawab langsung kepada Kasad.

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?
   Belum mampu karena hanya dapat melakukan *monitoring* dan penutupan akun dengan cara melaporkan konten.

D. Informasi untuk menggali pentingnya peningkatan fungsi Satuan Siber TNI AD

1. Apakah menurut pandangan Bapak, Satuan Siber yang sudah dibentuk cukup untuk menghadapi kejahatan siber?
   Belum cukup karena baru berfungsi sebagai alat pertahanan dan *monitoring* media saja serta belum adanya koordinasi lintas sektoral yang terintegrasi.

2. Kapan menurut pandangan Bapak Satuan Siber perlu adanya peningkatan fungsi?
   Segera mungkin, karena kejahatan siber sudah marak menyerang institusi TNI AD.

3. Menurut pandangan Bapak, siapa yang dapat melakukan peningkatan funsi Satuan Siber?
   Pemerintah dan unsur pimpinan TNI dan TNI AD.

Koleksi Perpustakaan Universitas Terbuka

43794.pdf

4. Pada bagian mana Satuan siber perlu peningkatan fungsi?
   Pada bagian unit penindakan dan penanggulangan ditingkatkan kemampuannya bukan hanya *monitoring* berita saja melainkan dapat melakukan tindakan ofensif.

5. Mengapa Satuan Siber perlu peningkatan fungsi?Berikan pandangan Bapak.
   Peningkatan fungsi satuan siber wajib dilakukan, agar dapat menangkal dan mengeksekusi tindak kejahatan yang ditujukan kepada TNI AD, sehingga aset data/informasi terjamin keamanannya.

6. Bagaimana menurut pandangan Bapak cara untuk peningkatan fungsi Satuan Siber TNI AD?
   Melalui peningkatan kemampuan SDM, sarana dan prasarana serta peralatan canggih yang memiliki kemampuan untuk melakukan serangan siber serta koordinasi lintas sektoral antar satuan siber nasional.

E. Informasi untuk menggali pandangan mengenai faktor penghambat peningkatan fungsi Satuan Siber TNI AD

1. Apa saja menurut pandangan Bapak yang menjadi faktor penghambat peningkatan fungsi Satuan Siber TNI AD ?
   Keterbatasan dukungan alat dan teknologi, belum adanya aturan hukum yang jelas, SDM yang terbatas dan masih besarnya ego sektoral satuan lain.

2. Berikan pandangan Bapak, siapa saja yang dapat menghambat dalam peningkatan fungsi satuan siber TNI AD?
   Prajurit TNI AD yang belum menyadari besarnya ancaman perang siber.

3. Pada bagian faktor penghambat mana yang dapat diperbaiki untuk disegerakan dalam peningkatan fungsi Satuan Siber TNI AD?
   Pada peningkatan kualitas SDM dan pengadaan sarana dan prasarana yang canggih serta kerjasama lintas sektoral antar satuan siber nasional.

4. Mengapa menurut pandangan Bapak, faktor penghambat perlu segera diperbaiki?
   Agar dapat mengamankan aset infrastruktur kritis teknologi dan sistem informasi yang ada di lingkungan Angkatan Darat, sehingga TNI AD dapat mencapai level yang lebih baik dalam penggunaan teknologi dan sistem informasi.

5. Bagaimana menurut pandangan Bapak cara untuk mengatasi faktor penghambat agar segera terjadi peningkatan fungsi Satuan Siber TNI AD?

Koleksi Perpustakaan Universitas Terbuka

Sarana/prasarana harus diperbaiki/ditingkatkan, peralatan dilengkapi, akses internet ditingkatkan,serta diadakan pelatihan-pelatihan siber bagi personel Satuan Siber TNI AD.

Koleksi Perpustakaan Universitas Terbuka

TRANSKRIP WAWANCARA
(Informan Kunci: Perwira Spamad/Informan H)

A. Karakteristik Informan

1.	Nama	:	Aswin Sepriansyah
2.	Umur	:	34 Tahun
3.	Jenis Kelamin	:	Laki-Laki
4.	Pangkat/Satuan	:	Mayor Inf/Spamad

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   Adalah kejahatan yang dilakukan dari dunia maya dengan menggunakan internet sebagai media.

2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   Setiap saat, bahkan saat ini sudah semakin meningkat.

3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   Semua oknum tak bertanggungjawab baik organisasi atau poronganan yang menguasai IT.

4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana menyerang institusi TNI AD?
   Kejahatan siber sebagai kejahatan yang nyata, karena dapat memperburuk citra TNI AD dan dapat membobol rahasia pertahanan melalui jaringan internet, yang diserang adalah sistem pertahanan dan piranti lunak milik TNI AD.

5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   Sistem keamanan jaringan komputer yang belum baik dan Sumber Daya yang dimiliki TNI AD masih mudah diserang oleh siber lawan serta tingkat kesadaran akan pentingnya keamanan siber masih sangat kurang.

6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD?
   Melalui penyadapan, sabotase dan perusakan jaringan komputer, melalui penyebaran berita *hoax* di Medsos dan melalui jaringan *online* terorisme.

Koleksi Perpustakaan Universitas Terbuka

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   Satuan Siber TNI AD bertugas untuk mengamankan institusi TNI AD dari kejahatan siber.

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   Secepatnya, peningkatan fungsi satuan siber perlu dilakukan untuk mencegah kejahatan siber masuk ke institusi TNI AD.

3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?
   Semua prajurit TNI AD yang telah memiliki dasar intelijen, persandian dan ilmu siber yang handal.

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?
   Satuan Siber TNI AD sebaiknya berada di Mabesad dan langsung bertanggung jawab kepada Kasad.

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?
   Masih terbatas pada kemampuan monitoring media saja, sehingga masih kurang dalam menghadapi maraknya kejahatan siber.

D. Informasi untuk menggali pentingnya peningkatan fungsi Satuan Siber TNI AD

1. Apakah menurut pandangan Bapak, Satuan Siber yang sudah dibentuk cukup untuk menghadapi kejahatan siber?
   Belum cukup masih harus ditingkatkan sampai memiliki kemampuan yang lengkap (*defence* dan *offence*).

2. Kapan menurut pandangan Bapak Satuan Siber perlu adanya peningkatan fungsi?
   Segera mungkin, karena kejahatan siber sudah marak menyerang institusi TNI AD.

3. Menurut pandangan Bapak, siapa yang dapat melakukan peningkatan funsi Satuan Siber?
   Pemerintah dan pimpinan TNI dan TNI AD.

4. Pada bagian mana Satuan siber perlu peningkatan fungsi?
   Pada bagian penindakan dan penanggulangan harus ditingkatkan kemampuannya agar dapat melakukan tindakan ofensif.

Koleksi Perpustakaan Universitas Terbuka

5. Mengapa Satuan Siber perlu peningkatan fungsi?Berikan pandangan Bapak.
   Untuk menjawab perkembangan dunia IT dan ancaman kejahatan siber yang semakin meningkat.

6. Bagaimana menurut pandangan Bapak cara untuk peningkatan fungsi Satuan Siber TNI AD?
   Melalui peningkatan kemampuan sumber daya siber baik personel siber maupun peralatannya serta adanya aturan hukum yang jelas.

E. Informasi untuk menggali pandangan mengenai faktor penghambat peningkatan fungsi Satuan Siber TNI AD

1. Apa saja menurut pandangan Bapak yang menjadi faktor penghambat peningkatan fungsi Satuan Siber TNI AD ?
   Sumber daya manusia dan peralatan serta dana yang kurang.

2. Berikan pandangan Bapak, siapa saja yang dapat menghambat dalam peningkatan fungsi satuan siber TNI AD?
   Setiap prajurit yang belum menyadari pentingnya kemanan siber.

3. Pada bagian faktor penghambat mana yang dapat diperbaiki untuk disegerakan dalam peningkatan fungsi Satuan Siber TNI AD?
   Pada peningkatan kualitas SDM dan pendanaan.

4. Mengapa menurut pandangan Bapak, faktor penghambat perlu segera diperbaiki?
   Agar dapat mengamankan data-data rahasia bidang pertahanan dari serangan siber yang masuk ke institusi TNI AD.

5. Bagaimana menurut pandangan Bapak cara untuk mengatasi faktor penghambat agar segera terjadi peningkatan fungsi Satuan Siber TNI AD?
   Peningkatan kualitas SDM baik kualitas dan kuantitasnya memalui rekuitment yang benar dan pendidikan/kursus intelijen, sandi dan siber, serta dukungan dana yang cukup untuk pengadaan sarana dan prasarana yang canggih dan modern.

Koleksi Perpustakaan Universitas Terbuka

TRANSKRIP WAWANCARA
(Informan Kunci: Prajurit Satuan Siber TNI AD/Informan I)

A. Karakteristik Informan

1.	Nama	:	Nofem Sanjaya
2.	Umur	:	31 Tahun
3.	Jenis Kelamin	:	Laki-Laki
4.	Pangkat/Satuan	:	Sersan Satu/Spamad

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   Merupakan suatu tindak negatif yang dilakukan oleh oknum tertentu untuk mencapai tujuannya yang dilakukan *melalui media elektronik*, Sosmed dan pemberitaan lainnya.

2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   Setiap saat, bahkan sudah banyak yang masuk ke institusi TNI AD terutama penyebaran berita *hoax* namun kita banyak yang tidak mengetahui dan menyadari kejahatan ini.

3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   Semua pihak yang menguasai IT, baik pihak sipil atau militer.

4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana menyerang institusi TNI AD?
   Kejahatan siber dapat menyerang infrastruktur sisfo TNI AD, sehingga lawan dapat mengakses data-data yang bersifat rahasia milik TNI AD.

5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   SDM yang dimiliki TNI AD untuk bidang siber masih rendah, infrastruktur siber milik TNI AD belum memadai, sistem keamanan jaringan yang belum ada, sabotase dari pihak luar dan upaya pihak luar lainnya dalam hal mencuri data/informasi pertahanan negara.

6. Apa saja yang bapak ketahui tentang *bagaimana kejahatan siber dapat* menyerang Institusi TNI AD ?
   Kejahatan siber sangat membahayakan institusi TNI yang juga mengikuti perkembangan teknologi di berbagai bidang yang mencakup administrasi data yang rahasia dan Alutsista.

Koleksi Perpustakaan Universitas Terbuka

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   Satuan siber TNI AD adalah satuan yang bertugas melaksanakan tugas pokok TNI AD melalui media elektronik, untuk mencari berita serta mengantisipasi adanya kebocoran dokumen, serta menanggulangi berita *hoax* agar tidak menimbulkan citra negatif TNI AD di masyarakat.

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   Segera mungkin, karena kejahatan siber sudah marak menyerang *institusi* TNI AD.

3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?
   Prajurit yang memiliki dasar intelijen, persandian dan pengetahuan IT dan siber.

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?
   Satuan pelaksana fungsi khusus yang berkedudukan dan bertanggungjawab langsung di bawah Kasad.

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?
   Untuk saat ini Satuan Siber TNI AD belum maksimal dalam menghadapi kejahatan siber, masih dalam tahap monitoring dan melakukan pelaporan ke komando atas.

Koleksi Perpustakaan Universitas Terbuka

TRANSKRIP WAWANCARA
(Informan Kunci: Prajurit Satuan Siber TNI AD/Informan J)

A. Karakteristik Informan

1.	Nama	:	Novan Eka
2.	Umur	:	29 Tahun
3.	Jenis Kelamin	:	Laki-Laki
4.	Pangkat/Satuan	:	Sersan Satu/Spamad

B. Informasi untuk menggali pandangan mengenai tren ancaman kejahatan siber

1. Apa saja yang Bapak ketahui mengenai tren ancaman kejahatan siber?
   Merupakan suatu tindak kejahatan dengan menggunakan sistem internet/pihak ketiga dengan melakukan peretasan dan pengambilan data tanpa ijin.

2. Kapan menurut Bapak ancaman kejahatan siber akan mengancam institusi TNI AD?
   Setiap saat, bahkan sudah banyak yang masuk ke institusi TNI AD terutama penyebaran berita *hoax* namun kita banyak yang tidak mengetahui dan menyadari kejahatan ini.

3. Siapa saja yang Bapak ketahui dapat mengancam isntitusi TNI AD dengan kejahatan siber?
   Semua pihak yang menguasai IT, baik pihak sipil atau militer.

4. Bagaimana pandangan Bapak mengenai kejahatan Siber dan pada bagian mana menyerang institusi TNI AD?
   Kejahatan siber sangat berbahaya karena dapat menyerang infrastruktur sisfo TNI AD, sehingga lawan dapat mengakses data-data yang bersifat rahasia milik TNI AD.

5. Bagaimana pandangan Bapak terhadap penyebab ancaman kejahatan siber itu terjadi?
   SDM yang dimiliki TNI AD untuk bidang siber masih rendah, infrastruktur siber milik TNI AD belum memadai, sistem keamanan jaringan yang belum ada, sabotase dari pihak luar dan upaya pihak luar lainnya dalam hal mencuri data/informasi pertahanan negara.

6. Apa saja yang bapak ketahui tentang bagaimana kejahatan siber dapat menyerang Institusi TNI AD ?
   Kejahatan siber sangat membahayakan institusi TNI AD, karena mengancam terjadinya pencurian data, sabotase dan *proxy war*.

Koleksi Perpustakaan Universitas Terbuka

C. Informasi untuk menggali pandangan terhadap Satuan Siber TNI AD

1. Apa saja yang Bapak ketahui tentang Satuan Siber TNI AD?
   Satuan siber TNI AD adalah satuan yang bertugas sebagai badan ofensif dan defensif terhadap tindak kejahatan siber.

2. Kapan menurut pandangan Bapak, Satuan siber TNI AD perlu peningkatan fungsi?
   Segera mungkin, karena kejahatan siber sudah marak menyerang institusi TNI AD.

3. Siapa saja menurut Bapak yang perlu tergabung pada Satuan Siber TNI AD?
   Prajurit yang memiliki dasar intelijen, persandian dan pengetahuan IT dan siber.

4. Pada satuan organisasi TNI AD mana menurut pandangan Bapak sebaiknya posisi Satuan Siber berada?
   Satuan pelaksana fungsi khusus yang berkedudukan dan bertanggungjawab langsung di bawah Kasad.

5. Bagaimana pandangan Bapak mengenai Satuan Siber TNI AD dalam meghadapi kejahatan siber?
   Sudah cukup baik, akan tetapi perlu dikembangkan lagi segi kemampuan dan dibentuk dasar serta tugas yang harus dilakukan seperti penindakan maupun penutupan akun.

Koleksi Perpustakaan Universitas Terbuka