MODUL PRAKTIKUM



KEAMANAN KETAHANAN SIBER

UNIVERSITAS TEKNOLOGI MATARAM

2019

Jl. Kampus Universitas Teknologi Mataram, Kekalik, Mataram

KATA PENGANTAR

Dengan menyebut nama Allah SWT yang Maha Pengasih lagi Maha Panyayang, kami panjatkan syukur ke hadirat-Nya, yang telah melimpahkan rahmat dan hidayatnya, sehingga modul matakuliah keamanan dan ketahanan cyber ini bisa kami selesaikan dengan baik.

Modul matakuliah keamanan dan ketahanan *cyber* ini diambil dari kajian Pengembangan Keamanan Siber Nasional yang dilaksanakan oleh Dewan Teknologi Informatika dan Komunikasi Nasional (Wantiknas). Adapun keluaran dari modul ini adalah sebagai pembelajaran kepada mahasiswa dalam pengembangan keamanan siber di masa mendatang.

Modul matakuliah keamanan dan ketahanan *cyber* ini telah kami susun dan mendapatkan bantuan dari berbagai pihak. Untuk itu kami menyampaikan banyak terima kasih kepada semua pihak yang telah berkontribusi dan memberikan masukan dalam pembuatan modul ini.

Akhir kata kami berharap semoga modul ini dapat memberikan manfaat ataupun inspirasi kepada seluruh mahasiswa yang mengambil dan mempelajari matakuliah keamanan dan ketahanan *cyber*. Sekian dan terima kasih.

Mataram, November 2019

ABSTRAK

Seiring dengan pesatnya penetrasi jaringan global dan kemajuan mobile Internet di Indonesia, semakin menambah kerentanan keamanan informasi sebuah organisasi dari ancaman siber (*cyber threat*). Serangan siber menjadi tantangan tersendiri untuk pemangku kebijakan pada era informasi. Meningkatnya kejahatan dengan menggunakan teknologi informasi teridentifikasi sejak tahun 2003, sebagai contoh kejahatan *carding* (*credit card fraud*), ATM/EDC *skimming* (awal tahun 2010), *hacking*, *cracking*, *phising* (*internet banking fraud*), *malware* (*virus/worm/trojan/bots*), *cybersquatting*, pornografi, perjudian online, *transnational crime* (perdagangan narkoba, mafia, terorisme, *money laundering*, *human trafficking*, *underground economy*) (IDSIRTII/CC, 2017).

Berdasarkan data ID-SIRTII, jumlah serangan siber semakin meningkat, dari 28,430,843 pada tahun 2015 meningkat menjadi 135.672.984 pada tahun 2016. Dan 47% dari keseluruhan kasus yang terjadi merupakan serangan malware, 44% merupakan penipuan, sedangkan sisanya berbentuk kejahatan siber lainnya, seperti website defacement, dan aktivitas manipulasi data dan kebocoran data (ID-SIRTII, 2017). Tren peningkatan kejahatan siber dalam bentuk penyebaran konten ilegal, *hate speech* dan sejenisnya. Maraknya *cyber crime* memerlukan perhatian dan keseriusan dalam mengembangkan *cybersecurity* bagi sebuah negara termasuk Indonesia.

Berdasarkan permasalahan di atas, Dewan Teknologi Informasi dan Komunikasi Nasional (WANTIKNAS) berupaya untuk mencari jalan keluar agar Keamanan Siber dapat sepenuhnya terjaga di Indonesia. Pengembangan Keamanan Siber Nasional juga selaras dengan 9 Program Reformasi Birokrasi dan Nawacita kelima, yaitu membuat pemerintah tidak absen dengan membangun tata kelola pemerintah yang bersih, efektif, demokratif, dan terpercaya. Untuk itu, WANTIKNAS ingin menyusun sebuah kajian Pengembangan Keamanan Siber Nasional.

Berdasarkan kajian dapat disimpulkan beberapa hal berikut: (1) seiring dengan pesatnya penetrasi jaringan global dan kemajuan mobile Internet di Indonesia, semakin menambah kerentanan keamanan informasi sebuah organisasi dari ancaman siber

(*cyber threat*). Serangan siber menjadi tantangan tersendiri untuk pemangku kebijakan pada era informasi; (2) Indonesia telah memiliki regulasi e-Government berupa Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) yang dapat menjadi acuan dalam pengembangan SPBE bagi seluruh instansi pemerintah. Berdasarkan Perpres SPBE, pembangunan sistem keamanan informasi nasional meliputi: manajemen keamanan informasi, teknologi keamanan informasi, dan budaya keamanan informasi, dilaksanakan oleh BSSN; dan (3) tersedia berbagai standar terkait keamanan siber seperti SNI ISO/IEC 27001 dan NIST *Cybersecurity Framework* yang dapat diadopsi oleh berbagai instansi untuk peningkatan keamanan siber.

Rekomendasi yang telah disumuskan antara lain: (1) memperkuat kelembagaan keamanan siber; (2) meningkatkan kerjasama dan peran aktif dalam peningkatan keamanan siber; (3) meningkatkan penguasaan teknologi keamanan siber; (4) meningkatkan edukasi dan pengembangan kapasitas sumber daya manusia keamanan siber; dan (5) menyusun dan menerapkan strategi pengembangan Keamanan Siber Nasional secara berkelanjutan.

DAFTAR ISI

KATA PENGANTAR i
ABSTRAK ii
DAFTAR ISI iv
DAFTAR GAMBAR vi
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Dasar Hukum 2
1.3 Tujuan 2
1.4 Pelaksana Kegiatan 3
1.5 Jadwal Pelaksanaan 3
1.6 Rencana Anggaran Biaya 3
BAB II PERMASALAHAN 4
2.1 Kemanan Siber 4
2.2 Indeks Keamanan Siber 6
2.3 Standar Keamanan Siber 9
2.4 Best Practices 12
BAB III METODOLOGI 14
3.1 Metodologi Kegiatan 14
3.2 Ruang Lingkup 16
3.3 Panduan Prinsip 16
3.4 Pembiayaan 16
BAB IV ANALISIS KEBIJAKAN ALTERNATIF 17
4.1 Kelembagaan Keamanan Siber 17

4.2 Kerjasama Keamanan Siber 18
4.3 Teknologi Keamanan Siber 18
4.4 Pengembangan Kapasitas 19
4.5 Strategi Pengembangan *Digital Government* 20
BAB V PENUTUP 22
5.1 Kesimpulan 22
5.2 Rekomendasi 22

DAFTAR GAMBAR

Gambar 1 Top 10 Serangan Berdasarkan Klasifikasi Tahun 2017 5
Gambar 2 Heat Map *Global Cybersecurity Index* Tahun 2017 6
Gambar 3 Pilar dan Sub-Pilar *Global Cybersecurity Index* 7
Gambar 4 Area Evaluasi Indeks KAMI 9
Gambar 5 NIST *Cyber Security Framework* 12
Gambar 6 Metodologi kegiatan 14

BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini dunia tengah berada dalam era informasi yang merupakan tahapan lanjutan dari era prasejarah, era agraris, dan era industri. Pada era informasi, keberadaan suatu 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.

Salah satu temuan yang memberikan pengaruh paling besar dalam masyarakat informasi adalah ditemukannya internet. Hadirnya internet sebagai bentuk teknologi baru menyebabkan manusia tidak mampu terlepas dari arus komunikasi dan informasi.

Terkait dengan internet terdapat sejumlah konsep yang berhubungan yaitu telematika, multimedia dan cyber space. Istilah telematika dikenal sebagai the new hybrid of technology yang muncul karena perkembangan teknologi digital yang membuat perkembangan teknologi telekomunikasi dan informatika semakin terpadu atau yang biasa disebut dengan konvergensi. Konvergensi antara teknologi telekomunikasi, media dan informatika tersebut akhirnya mendorong penyelenggaraan sistem elektronik berbasis teknologi digital yang kemudian di kenal dengan istilah the net. Konvergensi itu sendiri adalah merupakan gejala yang mengemuka dalam industri jasa Teknologi Informasi Komunikasi (TIK) yang muncul sejalan dengan pesatnya kemajuan teknologi elektronika pada akhir abad 20.

Dampak konvergensi secara sosial telah dirasakan masyarakat baik itu positif maupun negatif. Salah satu dampak negatif yang muncul dalam cyber-space adalah terjadinya cyber crime. Maraknya cyber crime memerlukan perhatian dan keseriusan dalam mengembangkan ***cybersecurity*** bagi sebuah negara termasuk Indonesia.

Indonesia sebenarnya saat ini tengah dalam keadaan mendesak cyber-security atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau cyber crime di Indonesia sudah mencapai tahap memprihatinkan. Namun

berbeda dengan penangganan kejahatan lainnya, cyber-security membutuhkan pemikiran yang komprehensif untuk menangganinya.

Berdasarkan permasalahan di atas, Dewan Teknologi Informasi dan Komunikasi Nasional (WANTIKNAS) berupaya untuk mencari jalan keluar agar Keamanan Siber dapat sepenuhnya terjaga di Indonesia. Pengembangan Keamanan Siber Nasional juga selaras dengan 9 Program Reformasi Birokrasi dan Nawacita kelima, yaitu membuat pemerintah tidak absen dengan membangun tata kelola pemerintah yang bersih, efektif, demokratif, dan terpercaya. Untuk itu, WANTIKNAS ingin menyusun sebuah kajian Pengembangan Keamanan Siber Nasional.

1.2 Dasar Hukum

Berikut merupakan beberapa dasar hukum yang melandasi kajian ini:

- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi
- Peraturan Menteri Komunikasi dan Informatika Nomor 29/PER/M.KOMINFO/12/2010 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet

1.3 Tujuan

Tujuan dari penyusunan kajian Pengembangan Keamanan Siber Nasional antara lain:

- mengidentifikasi kebijakan, peraturan, roadmap (peta jalan), yang mendukung Keamanan Siber
- sejauh mana capaian kebijakan tersebut, serta apa tantangan dan permasalahan yang dihadapi
- merumuskan rekomendasi arah strategis Keamanan Siber.

1.4 Pelaksana Kegiatan

Pelaksana kegiatan penyusunan kajian Pengembangan Keamanan Siber Nasional adalah Dewan Teknologi Informasi dan Komunikasi Nasional.

1.5 Jadwal Pelaksanaan

Kegiatan penyusunan kajian Pengembangan Keamanan Siber Nasional dilaksanakan dalam kurun waktu 4 (empat) bulan mulai dari bulan Agustus hingga November 2018.

1.6 Rencana Anggaran Biaya

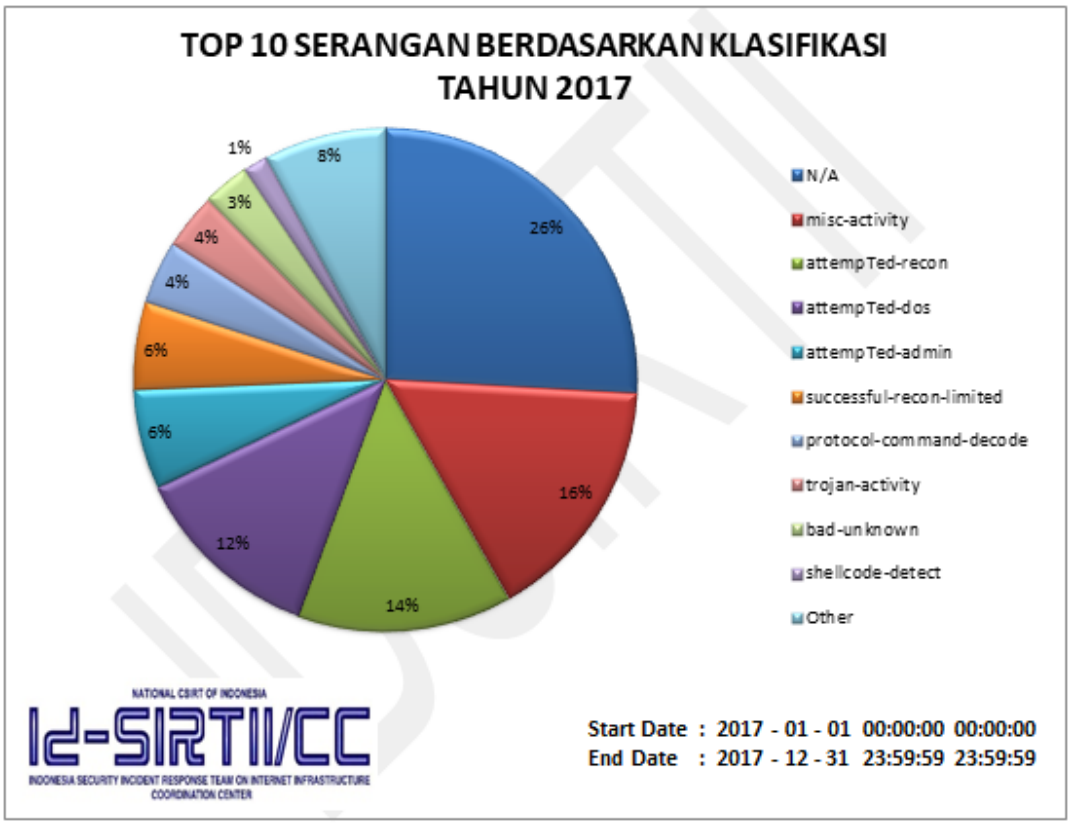
Kegiatan penyusunan kajian Pengembangan Keamanan Siber Nasional dilaksanakan menggunakan Honorarium Tenaga Ahli sebesar Rp 10.000.000 (sepuluh juta rupiah) selama 4 (empat) bulan.

BAB II
PERMASALAHAN

2.1 Kemanan Siber

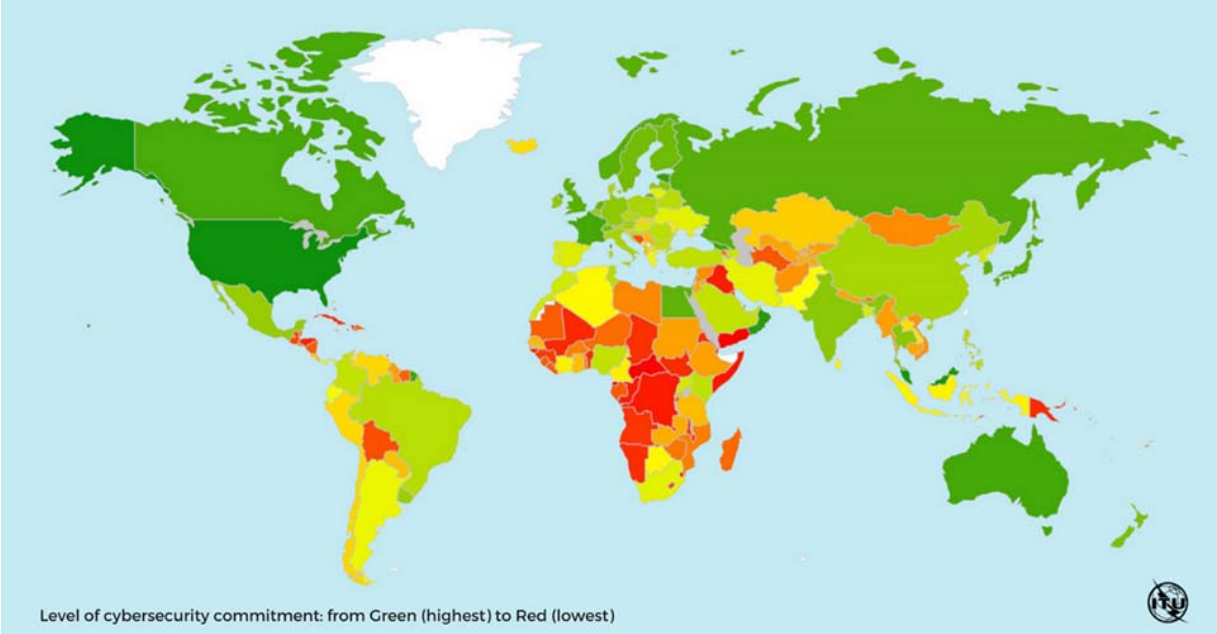
Seiring dengan pesatnya penetrasi jaringan global dan kemajuan mobile Internet di Indonesia, semakin menambah kerentanan keamanan informasi sebuah organisasi dari ancaman siber (*cyber threat*). Serangan siber menjadi tantangan tersendiri untuk pemangku kebijakan pada era informasi. Meningkatnya kejahatan dengan menggunakan teknologi informasi teridentifikasi sejak tahun 2003, sebagai contoh kejahatan *carding* (*credit card fraud*), ATM/EDC *skimming* (awal tahun 2010), *hacking*, *cracking*, *phising* (*internet banking fraud*), *malware* (*virus/worm/trojan/bots*), *cybersquatting*, pornografi, perjudian online, *transnational crime* (perdagangan narkoba, mafia, terorisme, *money laundering*, *human trafficking*, *underground economy*) (IDSIRTII/CC, 2017).

Berdasarkan data ID-SIRTII, jumlah serangan siber semakin meningkat, dari 28,430,843 pada tahun 2015 meningkat menjadi 135.672.984 pada tahun 2016. Dan 47% dari keseluruhan kasus yang terjadi merupakan serangan malware, 44% merupakan penipuan, sedangkan sisanya berbentuk kejahatan siber lainnya, seperti website defacement, dan aktivitas manipulasi data dan kebocoran data (ID-SIRTII, 2017). Tren peningkatan kejahatan siber dalam bentuk penyebaran konten ilegal, *hate speech* dan sejenisnya.



Gambar 1 Top 10 Serangan Berdasarkan Klasifikasi Tahun 2017

Usaha untuk meningkatkan komitmen dunia dalam keamanan siber, dilakukan dengan pemeringkatan *Global Cybersecurity Index* (GCI) oleh *International Telecommunication Union* (ITU) kepada 193 negara-negara anggotanya. Penilaian tersebut didasarkan pada lima pilar GCI *framework* yaitu *legal*, *technical and procedure*, *organizational*, *capacity building*, dan *international cooperation*. Dari hasil penilaian GCI pada tahun 2017, Indonesia berada pada peringkat 70 dengan skor 0,424 (*mature stage*).



Gambar 2 Heat Map *Global Cybersecurity Index* Tahun 2017

2.2 Indeks Keamanan Siber

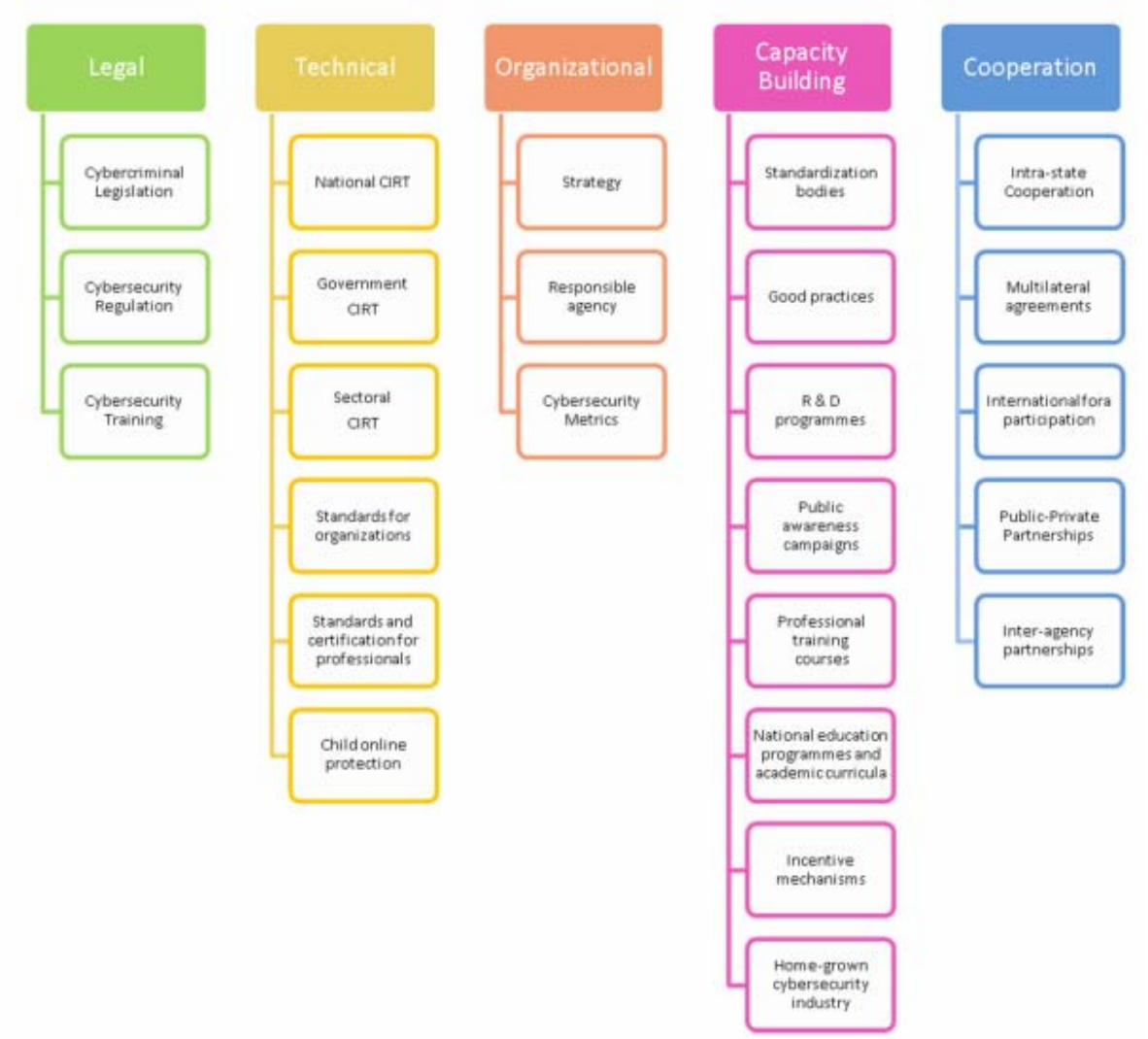
Global Cybersecurity Index (GCI) merupakan survey yang dilakukan oleh *International Telecommunication Union* (ITU) untuk mengukur komitmen negara-negara anggota ITU terhadap keamanan siber. Tujuan GCI adalah untuk membantu negara-negara mengidentifikasi area yang harus diperbaiki dalam dunia keamanan siber, sehingga membantu meningkatkan tingkat komitmen keseluruhan terhadap keamanan siber di seluruh dunia.

Penilaian didasarkan pada lima pilar yaitu:

- *Legal*, diukur dari keberadaan institusi legal dan *framework* keamanan siber
- *Technical*, diukur berdasarkan keberadaan institusi teknis dan penerapan teknologi
- *Organizational*, diukur berdasarkan koordinasi pembuat kebijakan dan pengembangan strategi keamanan siber
- *Capacity Building*, diukur berdasarkan penelitian dan pengembangan, pendidikan dan program pelatihan, profesional dan aparatur yang tersertifikasi.

– *Cooperation*, diukur dari adanya partnership, kerangka kerjasama dan information sharing network.

Setiap pilar dibagi lagi menjadi sub-pilar berikut.



Gambar 3 Pilar dan Sub-Pilar *Global Cybersecurity Index*

Hasil penilaian dikategorikan secara berurutan menjadi tiga stage yaitu kategori tertinggi adalah *leading stage* untuk negara-negara yang mempunyai komitmen sangat tinggi terhadap keamanan infomasi siber. Berikutnya adalah *maturing stage* untuk negara-negara yang telah mempunyai inisiatif dan sedang mengembangkan program-

program keamanan siber namun belum berkomitmen tinggi. Penilaian terendah adalah kategori *initiating stage* yaitu negara-negara yang baru memulai membuat komitmen terhadap keamanan siber (ITU, 2017).

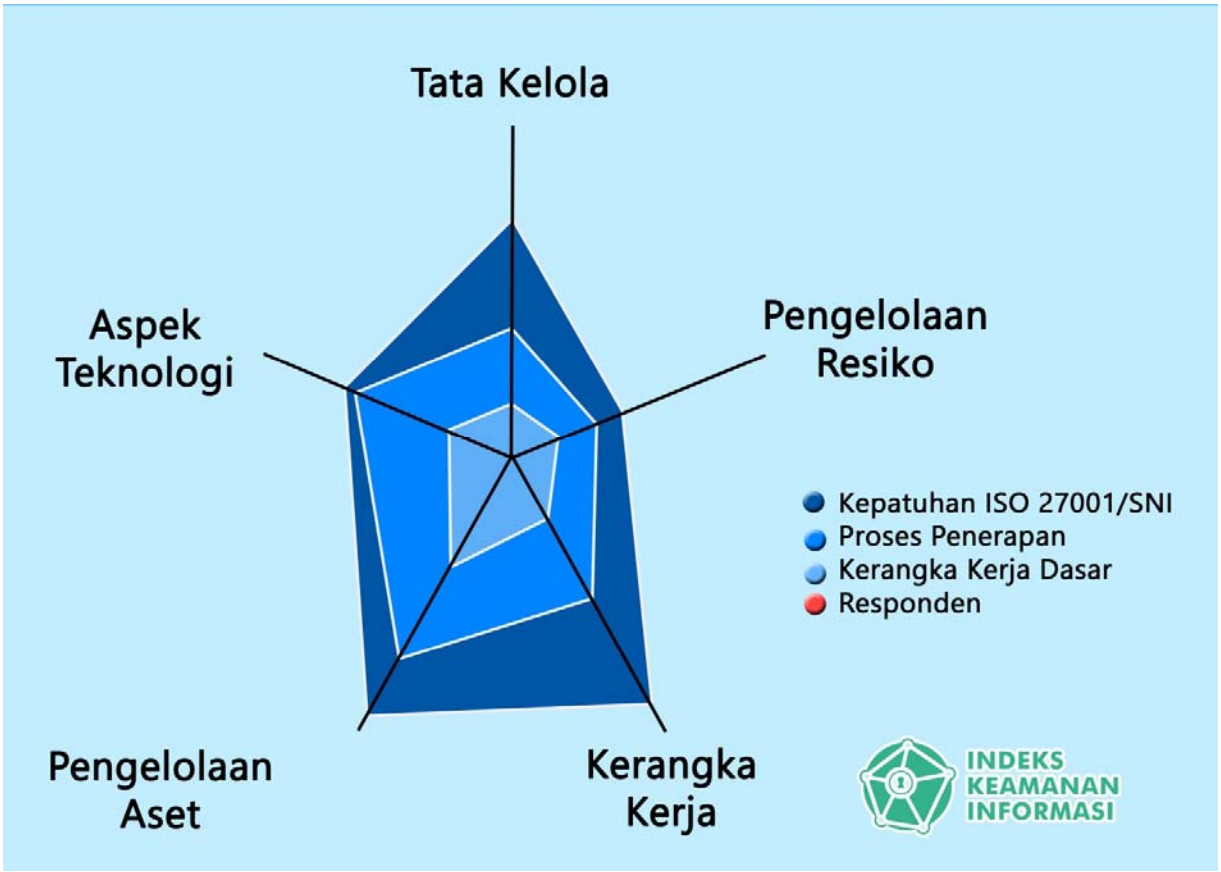
Di tingkat nasional, Kementerian Komunikasi dan Informatika menyusun indeks keamanan informasi atau indeks KAMI. Indeks KAMI merupakan suatu aplikasi untuk mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 serta peta area tata kelola keamanan sistem informasi di suatu instansi pemerintah. Evaluasi dilakukan terhadap beberapa area target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2009, yaitu:

1) Tata Kelola Keamanan Informasi
2) Pengelolaan Risiko Keamanan Informasi
3) Kerangka Kerja Keamanan Informasi
4) Pengelolaan Aset informasi
5) Teknologi dan Keamanan Informasi
6) Peran TIK

Dari Hasil Pemeringkatan Indeks KAMI tahun 2017, rata-rata nilai area yang paling tinggi yaitu Teknologi Keamanan Informasi. Nilai Pengelolaan risiko kemanan informasi mengalami peningkatan pada tahun 2017 sehingga tidak lagi menjadi area dengan nilai rata-rata terkecil. Area dengan nilai rata-rata paling kecil pada Pemeringkatan Indeks KAMI 2017 yaitu kerangka kerja keamanan informasi.

Saat ini, Indeks KAMI dikoordinasikan oleh Badan Siber dan Sandi Negara (BSSN). Acuan telah disesuaikan berdasarkan kriteria pada SNI ISO/IEC 27007, yaitu:

1) Tata Kelola
2) Pengelolaan Risiko
3) Kerangka Kerja
4) Pengelolaan Aset
5) Aspek Teknologi



Gambar 4 Area Evaluasi Indeks KAMI

2.3 Standar Keamanan Siber

SNI ISO/IEC 27001 yang diterbitkan tahun 2009 dan merupakan versi Indonesia dari ISO/IEC 27001:2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan. Standar ini dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang (*review*), pemeliharaan dan

peningkatan suatu SMKI. Pendekatan proses mendorong pengguna menekankan pentingnya :

a) Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi
b) Penerapan dan pengoperasian kontrol untuk mengelola risiko keamanan informasi dalam konteks risiko bisnis organisasi secara keseluruhan
c) Pemantauan dan tinjau ulang kinerja dan efektivitas SMKI, dan
d) Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran

Standar menyatakan persyaratan utama yang harus dipenuhi menyangkut :

a) Sistem manajemen keamanan informasi (kerangka kerja, proses dan dokumentasi)
b) Tanggung jawab manajemen
c) Audit internal SMKI
d) Manajemen tinjau ulang SMKI
e) Peningkatan berkelanjutan

Disamping persyaratan utama di atas, standar ini mensyaratkan penetapan sasaran kontrol dan kontrol-kontrol keamanan informasi meliputi 11 area pengamanan sebagai berikut:

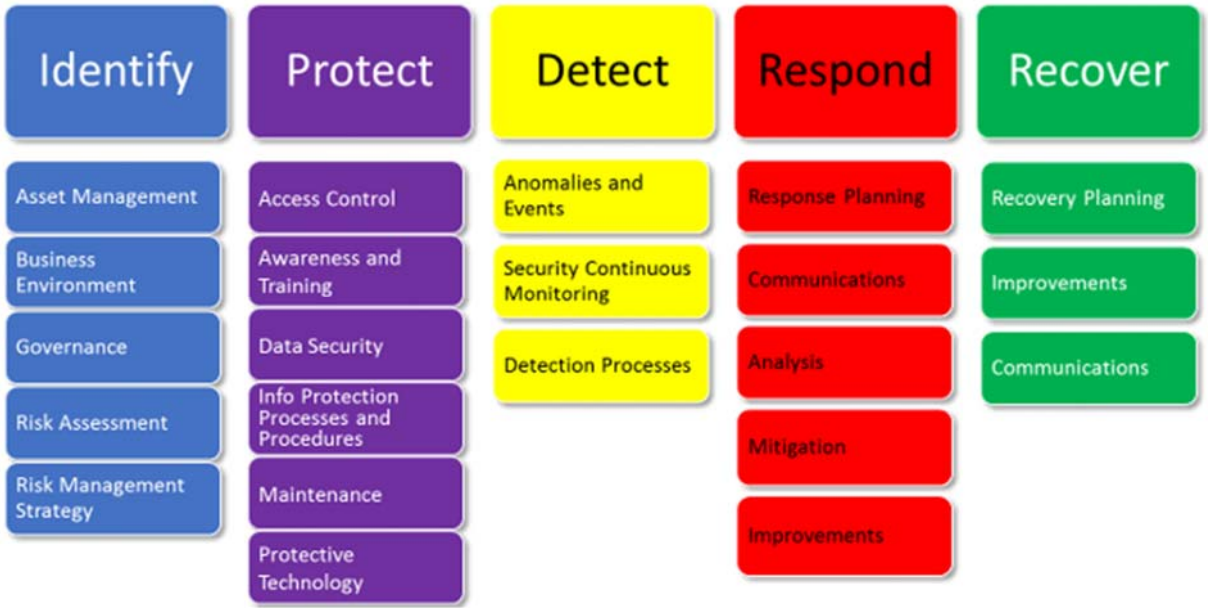
a) Kebijakan keamanan informasi
b) Organisasi keamanan informasi
c) Manajemen aset
d) Sumber daya manusia menyangkut keamanan informasi
e) Keamanan fisik dan lingkungan
f) Komunikasi dan manajemen operasi
g) Akses kontrol
h) Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
i) Pengelolaan insiden keamanan informasi

j) Manajemen kelangsungan usaha (*business continuity management*)
k) Kepatuhan

Standar internasional lainnya adalah NIST Cybersecurity Framework. NIST Cybersecurity Framework menyediakan kerangka kerja kebijakan pedoman keamanan komputer untuk bagaimana organisasi sektor swasta di Amerika Serikat dapat menilai dan meningkatkan kemampuan mereka untuk mencegah, mendeteksi, dan menanggapi serangan cyber. Versi 1.0 diterbitkan oleh Institut Nasional Standar dan Teknologi AS pada tahun 2014, awalnya ditujukan untuk operator infrastruktur kritis. Pada 2017, versi konsep kerangka kerja, versi 1.1, diedarkan untuk komentar publik. Versi 1.1 diumumkan dan tersedia untuk umum pada 16 April 2018. Versi 1.1 masih kompatibel dengan versi 1.0. Perubahan tersebut mencakup panduan tentang cara melakukan penilaian mandiri, detail tambahan tentang manajemen risiko rantai pasokan, dan panduan tentang cara berinteraksi dengan pemangku kepentingan rantai pasokan.

Berikut adalah fungsi dan kategorinya, bersama dengan pengidentifikasi dan definisinya yang unik, sebagaimana dinyatakan dalam kolom kategori pada tampilan spreadsheet inti dari standar:

- ***Identify***: mengembangkan pemahaman organisasi untuk mengelola risiko keamanan siber terhadap sistem, aset, data, dan kemampuan;
- ***Protect***: mengembangkan dan menerapkan perlindungan yang sesuai untuk memastikan pengiriman layanan infrastruktur penting;
- ***Detect***: mengembangkan dan menerapkan kegiatan yang sesuai untuk mengidentifikasi terjadinya peristiwa keamanan siber;
- ***Respond***: mengembangkan dan menerapkan kegiatan yang sesuai untuk mengambil tindakan terkait peristiwa keamanan siber yang terdeteksi;
- ***Recover***: mengembangkan dan menerapkan kegiatan yang sesuai untuk memelihara rencana ketahanan dan untuk mengembalikan kemampuan atau layanan apa pun yang terganggu karena peristiwa keamanan siber.



Gambar 5 NIST *Cyber Security Framework*

2.4 Best Practices

Benchmark Negara Amerika Serikat

Amerika Serikat meluncurkan Cybersecurity National Action Plan (CNAP) untuk mengambil langkah-langkah jangka pendek dan strategi jangka panjang untuk memberikan kontrol yang lebih baik pada keamanan cyber.

Langkah penting dalam CNAP tersebut antara lain adalah:

(1) Membentuk komisi nasional cybersecurity,

(2) Modernisasi sistem IT pemerintah senilai USD 3,1 miliar;

(3) Memperkuat warga Amerika untuk mengamankan akun onlinenya;

(4) Investasi lebih dari USD 19 miliar untuk cybersecurity.

Benchmark Negara Malaysia

Malaysia membentuk The Malaysian Computer Emergency Response Team (MyCERT) untuk menangani isu keamanan siber bagi pengguna internet.

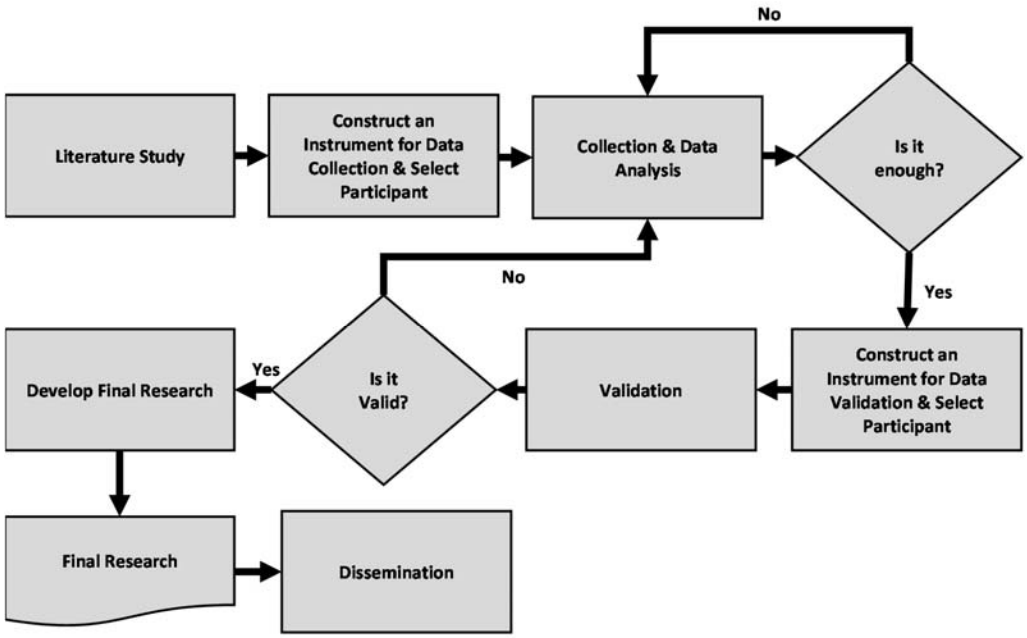
Benchmark Negara Canada

Canada memiliki Public Safety Canada yang memberikan sosialisasi dan edukasi tentang dunia siber, dan juga punya Canadian Cyber Incident Response Centre yang berfungsi mirip dengan Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center (Id-SIRTII/CC) di Indonesia.

BAB III
METODOLOGI

3.1 Metodologi Kegiatan

Metodologi penyusunan kajian Pengembangan Keamanan Siber Nasional menggunakan metodologi penyusunan kajian di lingkungan WANTIKNAS seperti pada Gambar 6 berikut.



Gambar 6 Metodologi kegiatan

Literature Study

Tahap ini merupakan tahap awal kajian. Pada tahap ini dilakukan studi terhadap penelitian sebelumnya yang terkait Keamanan Siber. Dokumen-dokumen yang dianalisis adalah journal, whitepaper, regulasi dan lain-lain.

Construct an Instrument for Data Collection & Select Participant

Tahap ini adalah tahap menyusun instrumen untuk pengambilan data serta menyeleksi ahli untuk kebutuhan pengambilan data. Instrumen dibuat berdasarkan hasil literatur dan contoh-contoh instrumen dalam pengambilan data.

Collection & Data Analysis

Tahap ini adalah proses dilaksanakan pengambilan data serta analisis data. Pengambilan data dilakukan dengan menggunakan metode *Focus Group Discussion* (FGD). Metode digunakan hingga data dirasakan cukup untuk dibawa ke proses selanjutnya. Setelah didapat data dari hasil FGD, data kemudian dianalisis dengan menggunakan teknik analisis *Grounded Theory*.

Construct an Instrument for Data Validation & Select Participant

Apabila data primer yang dihasilkan di dalam proses pengambilan data dirasakan cukup, langkah selanjutnya adalah memvalidasi data tersebut. Namun, sebelum melakukan hal tersebut, perlu dilakukan untuk membuat instrumen untuk melakukan validasi data serta memilih ahli untuk proses validasi tersebut.

Validation

Tahap ini adalah tahap untuk memvalidasi data primer yang ada, sehingga data tersebut bisa dijamin keabsahannya. Teknik untuk memvalidasi yang digunakan adalah teknik *Delphi*, yaitu dengan cara mengumpulkan para ahli dan mencari konsensus untuk mencari kesepakatan.

Develop Final Research

Setelah mendapatkan data yang tervalidasi pada proses sebelumnya, langkah selanjutnya adalah memfinalisasi kajian dengan menuangkan ke dalam dokumen yang sesuai dengan sistematika penulisan yang telah ditentukan.

Dissemination

Tahap ini merupakan tahap akhir, tahap di mana untuk menyebarluaskan hasil kajian agar diketahui oleh masyarakat luas, sehingga manfaat yang diharapkan bisa dirasakan oleh umum.

3.2 Ruang Lingkup

Kajian Pengembangan Keamanan Siber Nasional memiliki ruang lingkup sebagai berikut:

1) mengkaji peraturan perundang-undangan terkait
2) mengkaji *best practice* pengembangan *Digital Government*
3) mengkaji kelembagaan dan tata kelola dalam pengembangan *Digital Government*.

3.3 Panduan Prinsip

Kajian Pengembangan Keamanan Siber Nasional memiliki prinsip sebagai berikut:

1) menjamin pemerintahan yang transparan, terbuka, dan inklusif
2) mendorong partisipasi publik, swasta, dan masyarakat dalam penyusunan kebijakan serta perancangan dan penyelenggaraan layanan publik
3) menciptakan *data-driven culture* dalam layanan publik
4) mengadopsi keamanan informasi untuk meningkatkan kepercayaan masyarakat.

3.4 Pembiayaan

Kegiatan penyusunan Kajian *Digital Government* dibebankan melalui anggaran Dewan Teknologi Informasi dan Komunikasi Nasional tahun anggaran 2018.

BAB IV
ANALISIS KEBIJAKAN ALTERNATIF

4.1 Kelembagaan Keamanan Siber

Badan Siber dan Sandi Negara (BSSN) dibentuk berdasarkan Perpres No.53 tahun 2017. Lembaga pemerintah non kementerian yang berada di bawah dan bertangung jawab kepada Presiden. Merupakan penguatan dari Lembaga Sandi Negara ditambah dengan Dit. Keamanan Informasi, Ditjen Aplikasi Informatika, Kementerian Komunikasi dan Informatika (Perpres No.53, 2017). Fungsi BSSN dalam pelaksanaan kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi e-commerce, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber. Tantangan yang dihadapi terkait organisasi antara lain:

- Urgensi pembangunan ekosistem ranah siber Indonesia yang tahan dan aman, dan diharapkan dapat segera menginisiasi Peta jalan pedoman penanganan keamanan siber.
- Seperti halnya di Negara-negara maju seperti UK, masyarakat memerlukan pusat keamanan siber nasional (National Cyber Security Centre) sebagai rujukan utama yang mapan dan jelas untuk penanganan ancaman siber (Stoddart, 2016).
- Pengawasan dan evaluasi oleh seluruh stakeholder.

Rekomendasi:

Memperkuat kelembagaan keamanan siber dalam wujud pusat keamanan siber nasional sebagai rujukan utama dalam penanganan ancaman keamanan siber.

4.2 Kerjasama Keamanan Siber

Indonesia Computer Emergency Response Team (IDCERT) adalah tim CERT pertama yang berdiri di Indonesia, pada 1998, merupakan tim koordinasi teknis berbasis komunitas yang bersifat independen untuk melakukan koordinasi penanganan insiden yang melibatkan pihak Indonesia dan luar negeri (ID-CERT, 2015). Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). asistensi/ pendampingan untuk meningkatkan sistem pengamanan dan keamanan di instansi/lembaga strategis (*critical infrastructure*) di Indonesia; sentra koordinasi (Coordination Center/CC) untuk inisiatif dari dalam dan luar negeri dan sebagai single point of contact (ID-SIRTII/CC, 2017). Tantangan yang dihadapi terkait organisasi antara lain:

- ID-CERT hanya bersifat volunteer (*come and go*).
- Urgensi peran ID-SIRTII dalam masa peralihan ke BSSN (Perpres No.53, 2017)
- Kolaborasi Antara private sector, pemerintah, masyarakat, dan dunia international dalam pencegahan maupun penanganan kejahatan siber masih kurang terwadahi (Murphy, 2010). Koordinasi dengan stakeholder aplikasi atau software, sebagai contoh twitter atau Facebook yang digunakan untuk media kejahatan memerlukan koordinasi antar Negara.

Rekomendasi:

Meningkatkan kerjasama dan peran aktif dalam peningkatan keamanan siber melalui kerjasama bilateral, multilateral, dan *public-private partnership*, termasuk kerjasama di tingkat nasional untuk mengembangkan *national interconnected global intranet*.

4.3 Teknologi Keamanan Siber

Beberapa standar teknis keamanan siber telah teridentifikasi. Standar Nasional Indonesia (SNI) IEC/ISO 27001:2013 persyaratan untuk penetapan, penerapan, pemeliharaan, dan perbaikan berkelanjutan terhadap Sistem Manajemen Keamanan Informasi (SMKI) (BSN, 2016). SNI ISO/IEC 27018:2016, Teknologi informasi - Teknik

keamanan - Petunjuk praktik perlindungan informasi personal (PII) dalam public cloud yang berperan sebagai pemroses PII (BSN, 2016). Trust Positive (Trust+); Workshop penggunaan internet sehat dan aman; DNS filtering Nawala; program Kementerian komunikasi dan informatika (KOMINFO, 2015). Indeks Keamanan Informasi (Indeks KAMI). Alat evaluasi untuk menganalisis kesiapan pengamanan informasi di instansi pemerintah berbasis ISO/IEC 27001:2009 (Dirjen Aplikasi Telematika, 2013). Tantangan yang dihadapi terkait organisasi antara lain:

- Perkembangan Machine-toMachine (M2M) technologi, Internet of Things (IoT), Cloud Computing diikuti perkembangan ragam serangan siber, dan malware semakin kompleks (Obiso, 2015)
- Hasil penilaian indeks KAMI pada 41 organisasi pemerintah pada tahun 2012, dari 5 area kunci menunjukkan bahwa hanya 3% organisasi yang memenuhi standar, sedangkan selebihnya masih fokus hanya pada area teknologi (Kautsarina & Gautama, 2014).

Rekomendasi:

Meningkatkan penguasaan teknologi keamanan siber untuk mengantisipasi berbagai ancaman serangan siber yang berasal dari dalam maupun luar negeri.

4.4 Pengembangan Kapasitas

Telah teridentifikasi berbagai kegiatan pengembangan kapasitas SDM keamanan siber. Talent Pool Born to control: Gladiator Cyber Security Indonesia (GCSI). Peningkatan kemampuan keamanan siber dengan target penjaringan 10.000 kandidat untuk peningkatan kapasitas keamanan siber lebih lanjut (SIARAN PERS NO.12 /HM/KOMINFO/01/2017, 2017). Bimbingan teknis keamanan informasi (Indeks KAMI, APRISMA, SNI ISO 27001, ISO 22301) bagi instansi pemerintah (Chendramata, 2016). Program awareness bagi legislatif, pimpinan instansi dan pimpinan industri sektor strategis melalui koordinasi dengan LEMHANAS dan LAN (Chendramata, 2016). Penerapan program pendidikan untuk SDM Keamanan Informasi yang terakreditasi,

sesuai standar kompetensi industri melalui centre of Excellence di Perguruan Tinggi (Chendramata, 2016). Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Sektor Keamanan Informasi (KEMNAKER, 2015). Edukasi Publik sosialisasi konten berkualitas, pemahaman kebhinekaan, dan anti terorisme. Mentargetkan 40 daerah serta melalui media sosial dengan target pengguna twitter di Indonesia 19,1 juta, dan 232 ribu pengguna instagram (KOMINFO, 2015). Pembentukan 1500 agen perubahan Internet Cerdas, Kreatif, dan Produktif (i-CAKAP) di daerah perbatasan, tertinggal, dan terluar (KOMINFO, 2015). Tantangan yang dihadapi terkait organisasi antara lain:

- Sosialisasi keamanan informasi (termasuk aspek hukum, promosi SKKNI bidang Keamanan Informasi dan Auditor TI) bagi masyarakat dan Sektor Strategis masih sangat terbatas
- Prosedur pembaharuan unit kompetensi dalam SKKNI membutuhkan waktu yang lama, sementara laju perkembangan teknologi informasi dan komunikasi dan jenis ancaman siber sangat pesat
- Edukasi Publik sosialisasi konten berkualitas, keamanan siber, pemahaman kebhinekaan, dan anti terorisme belum diterapkan secara sistemastis dimulai dari usia dini padahal pengguna internet di Indonesia usia 9 – 15 tahun cukup tinggi yaitu sebesar 27.5 % (KOMINFO, 2016).

Rekomendasi:

Meningkatkan edukasi dan pengembangan kapasitas sumber daya manusia keamanan siber dan sarana prasarana penunjang lainnya seperti standar kompetensi kerja nasional serta lembaga pelatihan dan sertifikasi kompetensi keamanan siber.

4.5 Strategi Pengembangan *Digital Government*

Saat ini, Indonesia telah memiliki regulasi e-Government berupa Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). Regulasi ini yang menjadi pedoman dalam penerapan e-Government yang dikoordinasikan oleh Kementerian Pemberdayaan Aparatur Negara dan Reformasi

Birokrasi (Kemen PANRB). Berdasarkan Perpres SPBE, pembangunan sistem keamanan informasi nasional meliputi: manajemen keamanan informasi, teknologi keamanan informasi, dan budaya keamanan informasi, dilaksanakan oleh BSSN. Namun, BSSN belum memiliki rencana induk pengembangan keamanan siber nasional. Untuk itu, diperlukan suatu rencana induk pengembangan siber nasional yang dapat menjadi acuan seluruh instansi pemerintah secara nasional.

Rekomendasi:

Menyusun dan menerapkan strategi pengembangan Keamanan Siber Nasional secara berkelanjutan untuk melindungi infrastruktur kritis nasional dan kedaulatan Negara Kesatuan Republik Indonesia.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan kajian Pengembangan Keamanan Siber Nasional dapat disimpulkan beberapa hal berikut:

1) Seiring dengan pesatnya penetrasi jaringan global dan kemajuan mobile Internet di Indonesia, semakin menambah kerentanan keamanan informasi sebuah organisasi dari ancaman siber (*cyber threat*). Serangan siber menjadi tantangan tersendiri untuk pemangku kebijakan pada era informasi;
2) Indonesia telah memiliki regulasi e-Government berupa Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) yang dapat menjadi acuan dalam pengembangan SPBE bagi seluruh instansi pemerintah. Berdasarkan Perpres SPBE, pembangunan sistem keamanan informasi nasional meliputi: manajemen keamanan informasi, teknologi keamanan informasi, dan budaya keamanan informasi, dilaksanakan oleh BSSN; dan
3) Tersedia berbagai standar terkait keamanan siber seperti SNI ISO/IEC 27001 dan NIST *Cybersecurity Framework* yang dapat diadopsi oleh berbagai instansi untuk peningkatan keamanan siber.

5.2 Rekomendasi

Terdapat 5 (lima) rekomendasi yang telah dirumuskan pada kegiatan penyusunan kajian Pengembangan Keamanan Siber Nasional antara lain:

1) **memperkuat kelembagaan keamanan siber** dalam wujud pusat keamanan siber nasional sebagai rujukan utama dalam penanganan ancaman keamanan siber;

2) **meningkatkan kerjasama dan peran aktif dalam peningkatan keamanan siber** melalui kerjasama bilateral, multilateral, dan *public-private partnership*, termasuk kerjasama di tingkat nasional untuk mengembangkan *national interconnected global intranet*;
3) **meningkatkan penguasaan teknologi keamanan siber** untuk mengantisipasi berbagai ancaman serangan siber yang berasal dari dalam maupun luar negeri;
4) **meningkatkan edukasi dan pengembangan kapasitas sumber daya manusia keamanan siber** dan sarana prasarana penunjang lainnya seperti standar kompetensi kerja nasional serta lembaga pelatihan dan sertifikasi kompetensi keamanan siber; dan
5) **menyusun dan menerapkan strategi pengembangan Keamanan Siber Nasional secara berkelanjutan** untuk melindungi infrastruktur kritis nasional dan kedaulatan Negara Kesatuan Republik Indonesia.