TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN *GLOBAL CYBERSECURITY INDEX*

Challenges in The Implementation of National Cybersecurity Strategy of Indonesia from The Global Cybersecurity Index Point of View

Maulia Jayantina Islami
Puslitbang Aptika dan IKP, Badan Litbang SDM, Kemenkominfo
Jl. Medan Merdeka Barat No.9, Jakarta Pusat 10110, Telp: 021-3800418
E-mail: maul005@kominfo.go.id

Naskah diterima tanggal 28 November 2017, direvisi tanggal 4 Desember 2017, disetujui tanggal 15 Desember 2017

Abstract

Cyber threat is a national challenge in the 21st century, especially for the policy makers of cybersecurity in Indonesia. The Cybersecurity strategy has been initiated and run, but the Global Cybersecurity Index (GCI) of the year 2017 still shows the lack of the nation's commitment in terms of cybersecurity in Indonesia. With a qualitative approach on the literature review, the purpose of this study is to provide an overview of the current national cybersecurity strategy from the point of view of the GCI framework. The challenges of the strategy implementation will then be identified so the recommendations for the enhancement of the future national cybersecurity strategy can be disclosed.

***Keywords** : Information Security Management System, National Cybersecurity, Indonesia*

Abstrak

Serangan Siber menjadi sebuah tantangan tersendiri bagi Negara pada abad 21 ini, terutama bagi pemangku kebijakan di Indonesia. Strategi keamanan siber sudah mulai diinisiasi dan dijalankan namun penilaian *Global Cybersecurity Index (CGI)* tahun 2017 Indonesia masih menunjukkan kurangnya komitmen bangsa dalam hal keamanan siber. Dengan pendekatan kualitatif literature review, tujuan dari studi ini adalah untuk memberikan gambaran terhadap strategi keamanan siber nasional yang telah diinisiasi pemerintah pada saat ini dari sudut pandang *GCI framework*, kemudian mengidentifikasi tantangan yang dihadapi dalam mengimplementasikan strategi tersebut, dan rekomendasi untuk strategi nasional keamanan siber mendatang.

Kata Kunci : Sistem Manajemen Keamanan Informasi, Keamanan Siber Nasional, Indonesia

PENDAHULUAN

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. Pada bulan Mei 2017, sebuah serangan siber *Ransomware WannaCry* menyebabkan gangguan pada perusahaan dan rumah sakit di lebih dari 150 negara termasuk Indonesia. Serangan tersebut menjadi panggilan untuk melakukan kerjasama dalam hal keamanan siber *(cybersecurity)* yang lebih luas dengan negara-negara di seluruh dunia.

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, transnasional crime (perdagangan narkoba, mafia, *terorisme, money laundering, human trafficking, underground economy*) (ID-SIRTII/CC, 2017).

Dampak kejahatan siber terhadap sektor ekonomi berdasarkan data dari Norton Symantec selama tahun 2015 sampai dengan Februari 2016, kejahatan *online* di Indonesia menimbulkan total kerugian Rp 194.6 miliar (Symantec, 2016).

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 masih berada pada *mature stage*, yang berarti belum termasuk dalam jajaran Negara-negara Asia-Pacific yang dianggap memiliki komitmen tinggi dalam keamanan siber (ITU, 2017).

Dalam kesimpulan hasil penilaian GCI secara keseluruhan, terdapat kesenjangan yang signifikan antara negara-negara dalam hal kesadaran, pemahaman, pengetahuan dan kapasitas untuk menerapkan strategi, kapabilitas dan program yang tepat untuk memastikan penggunaan TIK yang aman dan tepat sebagai pendorong pengembangan ekonomi.

Kendala dan juga tuntutan bagi organisasi pemerintah dalam pelaksanaan *e-Government* salah satunya adalah faktor keamanan informasi yang meliputi kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) dari informasi. Oleh karena hal tersebut, strategi implementasi *e-Government* juga harus meliputi Sistem Manajemen Keamanan Informasi atau *Information Security Management System* (ISMS) yaitu suatu pendekatan yang sistematis untuk mengelola dan mengamankan informasi yang bersifat rahasia dan sangat penting dalam organisasi, meliputi aspek Sumber Daya Manusia (*people),* prosedur standar (*process), dan* Sistem Teknologi Informasinya *(technology).*

Memfokuskan hanya pada aspek teknologi untuk mengatasi permasalahan keamanan informasi siber tidaklah mencukupi. *Cybersecurity* semestinya adalah sebuah ekosistem dimana hukum *(laws),* organisasi *(organizations),* kemampuan *(skills),* kerjasama *(cooperation),* dan *technical implementation* berjalan secara selaras untuk dapat menjadi efektif (ITU, 2017). Dan hal tersebut bukan hanya menjadi tanggung jawab pemerintah, tapi memerlukan komitmen dari *private sector* dan *consumers*. Oleh karena itu sangat penting untuk menumbuhkan *cybersecurity culture* sehingga warga negara memiliki kesadaran untuk turut memonitor dan menyadari resiko saat menggunakan jaringan elektronik.

Studi mengenai strategi keamanan siber nasional yang telah dilakukan sebelumnya menyebutkan sudah ada usaha pemerintah Indonesia untuk mengatasi meningkatnya kejahatan siber yaitu dengan strategi yang ditinjau dari lima aspek yaitu hukum, teknikal dan prosedural, struktur organisasi, peningkatan kapasitas, dan kerjasama inernasional, namun dalam implementasinya belum sesuai dengan harapan (Setiadi, Sucahyo, & Hasibuan, 2012). Selanjutnya strategi keamanan siber dalam pelaksanaannya memerlukan sinergi antara pemerintah, keterlibatan sector swasta, dan keaktifan masyarakat (Harknett & Stever, 2009).

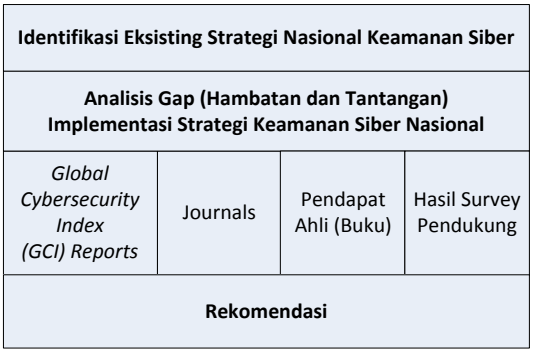
Sedangkan studi ini bertujuan untuk memberikan gambaran tentang bagaimana strategi pemerintah dalam menghadapi tantangan keamanan siber di Indonesia saat ini dan peluang peningkatan strategi yang dapat dilakukan di masa depan dipetakan dari aspek *people, process, technology.*

Metode Penelitian

Pendekatan kualitatif dilakukan dalam studi ini, yaitu didasarkan pada *non-numeric* data yaitu dapat berupa tulisan dan gambar, dan penyaringan terhadap data dilakukan untuk membuat interpretasi dari tinjauan pustaka (*literature review)* (Creswell, 2003). Kajian dilakukad dari sumber literatur seperti jurnal,

report, buku, maupun artikel dari sumber yang *reliable*.

Langkah kajian dimulai dari memetakan piliar-pilar dalam GCI framework ke dalam elemen *people, process, technology* yang merupakan pendekatan holistik tatakelola Teknologi Informasi. Selanjutnya strategi pemerintah yang telah berjalan diidentifikasi, dan analisis dilakukan untuk menemukan hambatan-hambatan dalam implementasi strategi tersebut, kemudian rekomendasi diusulkan untuk peningkatan implementasi strategi di masa depan.



Gambar 1. *Building Block* Penelitian

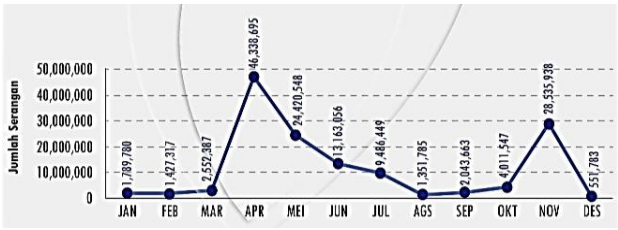
Keamanan Siber dalam Perspektif *People, Process, Technology*

Pengertian tentang keamanan Keamanan Siber *(cybersecurity)* dapat disimpulkan sebagai sebuah rangkaian aktifitas dan pengukuran yang dimaksudkan untuk melindungi dari serangan, disrupsi, atau ancaman yang lainnya melalui elemen-elemen *cyberspace (hardware, software, computer network)* (Fischer, 2009).

Keamanan Siber dapat digambarkan di satu sisi sebagai kebijakan, pedoman, proses, dan tindakan yang diperlukan agar transaksi elektronik dapat dilakukan dengan risiko pelanggaran, intrusi, atau pencurian minimum. Dan di sisi lain, keamanan siber adalah alat, teknik, atau proses yang digunakan untuk melindungi aset sistem informasi. Keamanan siber terdiri dari infrastruktur "lunak" dan "keras". Komponen infrastruktur lunak adalah Sumber Daya Manusia pengelola maupun pembuat kebijakan *(people)*; dan kebijakan, proses, protokol, dan pedoman yang menciptakan lingkungan pelindung untuk menjaga sistem dan data *(process)*. Sedangkan infrastruktur keras adalah *technology* yang terdiri dari perangkat keras dan perangkat lunak, yang dibutuhkan untuk melindungi sistem dan data dari ancaman eksternal dan internal siber.

Serangan Siber

Jumlah serangan siber di Indonesia 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 2. Jumlah Serangan Siber di Indonesia tahun 2016 (ID-SIRTII, 2017)

Global Cybersecurity Index (GCI)

Survey yang dilakukan *International Telecommunication Union* (ITU) untuk mengukur komitmen Negara-negara anggota 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 (hukum)***, 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.*

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).

HASIL DAN PEMBAHASAN

Tabel 1. Identifikasi Strategi Nasional Keamanan Siber Eksisting

	Pilar–pilar *GCI*	Strategi Nasional Keamanan Siber Eksisting	Tantangan / Hambatan
People	*1. Capacity Building*	*1.1. 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) 1.2. Bimbingan teknis keamanan informasi (Indeks KAMI, APRISMA, SNI ISO 27001, ISO 22301) bagi instansi pemerintah (Chendramata, 2016) 1.3. Program awareness bagi legislatif, pimpinan instansi dan pimpinan industri sektor strategis melalui koordinasi dengan LEMHANAS dan LAN (Chendramata, 2016) 1.4. Penerapan program pendidikan untuk SDM Keamanan Informasi yang terakreditasi, sesuai standar kompetensi industri melalui *centre of Excellence* di Perguruan Tinggi (Chendramata, 2016) 1.5. Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Sektor Keamanan Informasi (KEMNAKER, 2015) 1.6. 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) 1.7. Pembentukan 1500 agen perubahan Internet Cerdas, Kreatif, dan Produktif (i-CAKAP) di daerah perbatasan, tertinggal, dan terluar (KOMINFO, 2015)	▪ 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)

	Pilar–pilar *GCI*	Strategi Nasional Keamanan Siber Eksisting	Tantangan / Hambatan
Process	*2. Legal*	2.1. UU No.19/2016 tentang perubahan atas UU No.11/2008 tentang Informasi dan Transaksi Elektronik (ITE) (UU ITE, 2016) 2.2. UU Telekomunikasi No. 36/1999 (UU Telekomunikasi, 1999) 2.3. Peraturan Menteri Kominfo No.5 tahun 2017 tentang Perubahan keempat atas Peraturan Menteri Kominfo No.26 tahun 2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet (PERMENKOMINFO No.5, 2017)	▪ Jumlah *policy* dan regulasi untuk *cybersecurity* belum mengakomodasi segala bentuk ancaman siber, sementara kecepatan perkembangan TIK berbanding lurus dengan meningkatnya kejahatan siber ▪ Urgensi pengesahan RUU Perlindungan Data dan informasi pribadi perlunya kepastian hukum perlindungan data pribadi
	3. Organizational Structure	3.1. 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) 3.2. Fungsi BSSN dalam pelaksanaan kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi e-ommerce, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber	▪ Kurang jelasnya tenggat waktu peralihan penggabugan fungsi direktorat keamanan informasi dan Lembaga Sandi Negara menjadi BSSN sebagai organisasi baru ▪ 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
	4. International Cooperation	4.1. *Indonesia Computer Emergency Response Team (ID-CERT)* 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) 4.2. *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)	▪ 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.

Pilar–pilar *GCI*		Strategi Nasional Keamanan Siber Eksisting	Tantangan / Hambatan
Technology	5. *Technical and Procedural Measures*	5.1. Standar Nasional Indonesia (SNI) IEC/ISO 27001:2013 persyaratan untuk penetapan, penerapan, pemeliharaan, dan perbaikan berkelanjutan terhadap Sistem Manajemen Keamanan Informasi (SMKI) (BSN, 2016) 5.2. 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) 5.1. Trust Positive (Trust+); Workshop penggunaan internet sehat dan aman; DNS filtering Nawala; program Kementerian komunikasi dan informatika (KOMINFO, 2015) 5.2. Indeks Keamanan Informasi (Indeks KAMI). Alat evaluasi untuk menganalisis kesiapan pengamanan informasi di instansi pemerintah berbasis ISO/IEC 27001:2009 (Dirjen Aplikasi Telematika, 2013)	▪ Perkembangan Machine-to-Machine (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)

PENUTUP

Simpulan

Pemerintah Indonesia telah menginisiasi strategi nasional keamanan siber dan menjalankan program-program jangka pendek maupun panjang, namun dalam implementasinya masih terdapat tantangan-tantangan dan hambatan.

Tantangan dan hambatan implementasi strategi nasional keamanan siber dari sisi sumber daya manusia, prosedur dan kebijakan pencegahan dan keamanan yang masih memerlukan koordinasi dengan seluruh pemangku kebijakan bagi dari sektor swasta, pemerintah, masyarakat, dan institusi luar negeri yang merupakan pengembang dari aplikasi-aplikasi yang seringkali dipergunakan sebagai media kejahatan siber, dan teknologi yang harus dikembangkan seiring dengan meningkatnya jenis serangan siber.

Keamanan siber merupakan sebuah ekosistem dimana aspek legal, organisasi, skill, kerjasama, dan implementasi teknik berjalan secara selaras untuk hasil yang efektif.

Saran

Berdasarkan identifikasi strategi nasional keamanan siber dan analisis tantangan-tantangan dan hambatan dalam implementasinya, dapat direkomendasikan langkah-langkah sebagai berikut:

1. Pilar *Capacity Building*:
   - Pelatihan profesional keamanan siber bagi Aparatur Sipil Negara terutama yang mengelola data strategis, tenaga penyidik bidang ITE,
   - Peningkatan sosialisasi keamanan informasi (termasuk aspek hukum, promosi SKKNI bidang Keamanan Informasi dan Auditor TI) bagi masyarakat dan Sektor yang mengelola data Strategis
   - Edukasi Publik untuk menumbuhkan kesadaran keamanan, pemahaman kebhinekaan, dan anti terorisme diterapkan secara sistemastis dimulai dari usia dini dengan memasukkan kurikulum keamanan siber esensial dimulai dari Sekolah Menengah Pertama
2. Pilar *Legal:*
   - Urgensi pengesahan RUU Perlindungan Data dan informasi pribadi perlunya kepastian hukum perlindungan data pribadi untuk mendukung UU ITE dan UU Telekomunikasi

3. Pilar *Organizational Structure*:
   - Urgensi peran BSSN sebagai Lembaga Pemerintah Non Kementerian diharapkan dapat berfungsi sebagai *National Cyber Security Centre* sebagai rujukan utama penanganan keamanan siber dan *clearing house information exchange* sebagai wujud nyata pembangunan ekosistem ranah siber Indonesia. Dan segera menginisiasi Peta jalan pedoman penanganan keamanan siber
4. Pilar *International Cooperation*:
   - Penguatan kerjasama antara swasta (melalui ID-CERT), pemerintah (BSSN), masyarakat, dan stakeholder internasional (seperti pemilik aplikasi *media social* yang seringkali dimanfaatkan untuk media kejahatan (twitter, Facebook, dan sebagainya), serta lembaga terkait di dunia international dalam pencegahan maupun penanganan kejahatan siber
5. Pilar Teknikal dan Pengukuran Prosedural:
   - Pembaharuan penguasaan teknologi keamanan siber selaras dengan ragam ancaman siber yang menyerta teknologi *Machine-to-Machine (M2M), Internet of Things (IoT), Cloud Computing*.

DAFTAR PUSTAKA

BSN. (2016). *Buletin Informasi SNI Terbaru.* Jakarta: Pusat Informasi dan Dokumentasi Standardisasi Badan Standardisasi Nasional (BSN).

Chendramata, A. (2016). Indonesia Cybersecurity Strategy. Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika.

Creswell, J. W. (2003). *Research Design Qualitative, Quantitative, and Mixed Methods Approaches* (2nd ed.). Thousand Oaks, California: Sage Publishing.

Dirjen Aplikasi Telematika. (2013, Oktober 23). *Indeks Keamanan Informasi*. Retrieved from kominfo.go.id: https://www.kominfo.go.id/content/detail/3326/indeks-keamanan-informasi-kami/0/kemanan_informasi

Drucker, P. F. (1999). *Management Challenges for 21st Century.* New York: HarperCollins.

Fischer, E. A. (2009). *Creating a National Framework for Cybersecurity: an Analysis of Issues and Options* . New York: Nova Science Publishers, Inc.

Harknett, R. J., & Stever, J. (2009). The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal of Homeland Security and Emergency Management, 6*, Article 79.

ID-CERT. (2015). *profil ID-CERT*. Retrieved November 25, 2017, from cert.or.id: https://www.cert.or.id/tentang-kami/id/

ID-SIRTII. (2017). *Tren Serangan Siber Nasional 2016 dan Prediksi 2017.* ID-SIRTII.

ID-SIRTII/CC. (2017). Retrieved November 15, 2017, from http://www.idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html

ITU. (2017). *Global Cybersecurity Index 2017*. International Telecommunication Unit.

Kautsarina, & Gautama, H. (2014). Journal of Information Security Readiness of Government of Government Institution in Indonesia. *Institute of Electrical and Electronics Engineers (IEEE)*.

KEMNAKER. (2015). Retrieved from standarkompetensinaker.naker.go.id: http://standarkompetensi.naker.go.id/index.php/skkni2?page=12

KOMINFO. (2015). *Rencana Strategis Kementerian Komunikasi dan Informatika Tahun 2015-2019.* Kementerian Komunikasi dan Informatika.

KOMINFO. (2015). *SIARAN PERS NO.44/PIH/KOMINFO/6/2015*. Retrieved from kominfo.go.id: https://www.kominfo.go.id/content/detail/5100/siaran-pers-no44pihkominfo62015-

tentang-forum-penanganan-situs-internet-bermuatan-negatif/0/siaran_pers

KOMINFO. (2016). *Indikator TIK Rumah Tangga dan Indovidu.* Kementerian Komunikasi dan Informatika Republik Indonesia.

Murphy, T. (2010). Security Challenges in the 21st Century Global Commons. *Yale Journal of International Affairs*.

Obiso, M. (2015). *Cybersecurity Challenges and Capacity Building.* International Telecommunication Union.

PERMENKOMINFO No.5. (2017, Januari 24). Peraturan Menteri Komunikasi Republik Indonesia tentang Perubahan keempat atas Peraturan Menteri Komunikasi dan Informatika No.26 tahun 2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Perpres No.53. (2017, Mei 19). Peraturan Presiden No.53 tahun 2017 tentang Badan Siber dan Sandi Negara.

Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. (2012, December). An Overview of the Development Indonesia National Cyber Security. *International Journal of Information Technology & Computer Science (IJITCS), 6*, 106.

SIARAN PERS NO.12 /HM/KOMINFO/01/2017. (2017, Januari 25). "Born To Control" Penjaringan 10.000 Kandidat Gladiator Cyber Security Indonesia. Biro Humas Kementerian Kominfo.

Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *The Royal Institute of International Affirs*.

Symantec, N. (2016). *Norton Cyber Security Insights Report Global Corporation.* Symantec Corporation.

UU ITE. (2016, November 25). Undang-Undang No.19 tahun 2016 Tentang Perubahan Atas Undang-Undang No.11 tahun 2008 Tentang Informasi dan transaksi Elektronik. President Republik Indonesia.

UU Telekomunikasi. (1999, September 8). Undang-Undang No.36 tahun 1999 Tentang Telekomunikasi. President Republik Indonesia.