Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0

Cynthia Rahmawati[1]
[1] Universitas Dirgantara Suryadarma, Jakarta Timur, Indonesia

e-mail : **cynthiarahma23@gmail.com**

Abstrak— Revolusi Industri 4.0 dan peningkatan konektivitas antara bisnis dan kehidupan kita sehari-hari kini tengah mendorong transformasi bisnis dan memajukan kehidupan para karyawan dan pelanggan di seluruh dunia. Oleh karena itu, Pemerintah, Swasta, Pelaku Bisnis, dan Masyarakat Digital Indonesia dapat menjadi tolak ukur kedepannya terhadap tantangan dan ancaman keamanan siber yang terjadi. Penulisan ini menggunakan metode penelitian deskriptif kualitatif dengan mengumpulkan data, mengulas masalah terkait dengan pemerintah, pelaku bisnis/perusahaan swasta, dan masyarakat digital terhadap tantangan dan ancaman keamanan siber di era revolusi industri 4.0, meneliti data, menganalisis dan ditutup dengan kesimpulan. Simpulan yang diperoleh yaitu dalam hal tantangan dan ancaman siber Indonesia saat ini yakni cara membangun sistem keamanan melawan ancaman eksternal dan internet. Tantangan tersebut di bidang ekonomi, sosial, teknis, lingkungan, politik & aturan. Data tantangan industri tersebut terhadap keamanan siber dikategorikan dalam 3 tantangan: target serangan, ransomware, dan orang dalam. Oleh karena itu, dalam mengatasi tantangan dan ancaman keamanan siber di era Revolusi Industri, maka keterlibatan Indonesia mulai dari sektor pemerintah, pelaku bisnis, dan masyarakat digital antar lain: kesiapan masyarakat digital yang mandiri dan pengetahuan tinggi terhadap bahaya serangan siber, setiap perusahaan memerlukan sertifikasi kesiapan memasuki revolusi industri 4.0, sinergitas, perencanaan dan strategi sesuai dengan implementasi yang baik di setiap Kementerian dan lembaga terkait bidang keamanan siber. Sebagai contoh adanya 10 inisiatif *Making Indonesia* 4.0 didukung dengan peningkatan keamanan siber, kapasitas dan kualitas SDM/pekerja Indonesia. Saran dari penulisan ini adalah masih perlu dibahas lebih lanjut bagaimana implementasi peningkatan kapasitas dan kualitas SDM di bidang keamanan siber yang siap untuk dipekerjakan di era Revolusi Industri. Dengan demikian, Pemerintah, khususnya Kementerian Perindustrian lebih jelas dalam memberikan indikator penilaian kesiapan Industri 4.0 di Indonesia.

Kata Kunci— Tantangan, Ancaman Keamanan Siber Indonesia, Revolusi Industri 4.0

I. PENDAHULUAN

Kondisi keamanan informasi di Indonesia di Era Revolusi Industri 4.0 dapat diketahui salah satunya dengan pembahasan dalam penyelenggaraan CEOTalk oleh *Center for Digital Society* (CfDS) Fisipol UGM bersama Presiden Direktur Microsoft, Haris Izmee, mengangkat tema *"Cybersecurity in Indonesia: Are We Ready for It?*". Acara tersebut bertujuan untuk memberikan pengetahuan mengenai keamanan siber dan bagaimana cara mempersiapkan diri di era komputasi [1]. Dengan demikian, dalam mempersiapkan diri terhadap perubahan lingkungan industri di era digitalisasi, maka akan mempengaruhi perubahan pola perilaku yang muncul dalam masyarakat. Perubahan pola perilaku itu khususnya ada di lingkungan yang berbeda dan generasi yang berbeda tersebut tumbuh dan berkembang.

Generasi saat ini yaitu generasi Z: generasi yang lahir tahun 1996-sekarang memiliki karakteristik etos kerja: hobi membuat pekerjaan, kewirausahaan tinggi, dan mementingkan kualitas [2]. Dizik (2017) mengungkapkan bahwa generasi z merupakan generasi yang akan mengisi profesi yang belum terpetakan saat ini, akan muncul profesi baru dengan karakteristik

Received August 19th, 2019; Revised September 3rd, 2019; Accepted September 8th, 2019

baru di masa mendatang [2]. Haris juga menyatakan masa depan akan dipegang oleh mereka yang mampu untuk menjawab tantangan *cyber* dan menilai setiap hal dalam aspek kehidupan akan mengalami digitalisasi atau disrupsi oleh Revolusi Industri 4.0. Pemerintah juga mencanangkan *Making Indonesia* 4.0 yang bertujuan menghasilkan kualitas *output* yang lebih tinggi di sektor industri dengan integrasi antara konektivitas dan teknologi informasi komunikasi [1].

Perlu diketahui bahwa ada 10 Prioritas Nasional *Making Indonesia 4.0* terdapat beberapa *layer,* diantaranya *wearable tech, advanced robotics, 3D printing, Artificial Intelligence* , dan *Internet of Things*. Oleh karena itu, menyadari pentingnya digitalisasi dalam aspek kehidupan, pemerintah dan korporasi sepakat bahwa transformasi digital merupakan prioritas utama [1]. Dengan demikian, dalam mencanangkan 10 Prioritas Nasional *Making Indonesia* 4.0 agar berhasil, maka harus berkaitan dengan bagaimana kesiapan Indonesia, baik di pihak Pemerintah, Pelaku Bisnis dan Masyarakat dalam menghadapi tantangan *cyber security* di era revolusi Industri 4.0 ini. Berdasarkan fakta di lapangan dan permasalahan yang ada, maka penulis tertarik mengangkat kajian tentang tantangan dan ancaman keamanan siber Indonesia di era revolusi Industri 4.0.

II. LANDASAN TEORI

A. Cyber Space

Serangan di ruang siber (*cyberspace*) sendiri merupakan konsekuensi logis dari berkembangnya era teknologi informasi. Identifikasi bentuk serangan siber dapat terlihat pada hal-hal seperti kriminalitas siber, botnets, serangan terhadap institusi finansial-keuangan, penyebaran *Multi Purpose Malcode,* aktivitas siber yang disponsori oleh negara, dan aktivitas hacking. Berbagai bentuk trend ini menggunakan instrumen *cyberspace* sebagai saluran utama dalam melaksanakan tindakannya.

B. Keamanan Siber

Sesuai dengan definisinya, *cyber security* adalah aktifitas pencegahan dan pengamanan terhadap sumber daya telematika agar tidak terjadinya kriminalitas di dunia *cyber (Cyber Crime*). *Cyber security* juga dapat diartikan upaya untuk menahan dari penyerangan-penyerangan di dunia cyber. Berikut adalah elemen-elemen pokok dari *cyber security.*

- *Security Policy Document*
- *Information Infrastructure*
- *Perimeter Defense*
- *Network Monitoring System*
- *System Information and Event Management*
- *Network Security Assessment*
- *Human Resource and Security Awareness*

Dalam sistem informasi dikenal istilah "*Hardening"* yaitu sebuah cara untuk memperkuat keamanan infrastruktur sistem informasi seperti komputer maupun hal lainnya. Keamanan yang diperkuat biasanya pada sisi jaringan, sistem komputer, penutupan port yang rentan akan serangan, maupun dari segi firewall nya. Dilihat dari sisi sumber daya manusia, praktisi *cyber security* dapat dikelompokkan menjadi 3 kelompok besar.

- Analis Keamanan.
- Spesialis Forensik.
- *Hacker* (peretas).

C. Road Map Making Indonesia 4.0 di Era Revolusi Industri 4.0

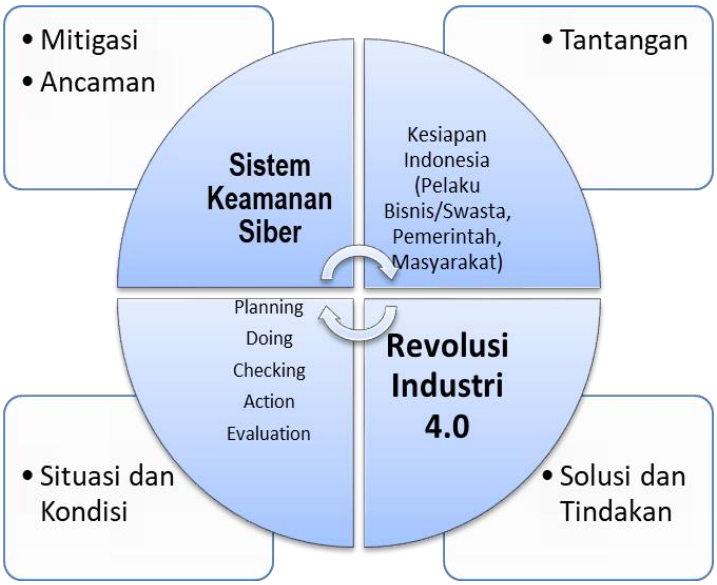
Secara luas, digitalisasi akan berpengaruh pada aspek bisnis dan ekonomi, baik itu ke negara, pemerintah, organisasi bisnis, dan masyarakat. Data menunjukkan pada 2017 produk atau layanan digital menyumbang 4% dari PDB Indonesia dan pada 2021 diperkirakan akan meningkat menjadi 40%. Tentunya hal ini merupakan potensi besar. Tingginya angka digitalisasi ternyata juga membawa dampak negatif. Sebanyak 49% organisasi di Indonesia pernah mengalami serangan-serangan siber yang merugikan Indonesia sebesar US$ 43,2 miliar

atau 3,7% dari total PDB Indonesia menurut data Frost & Sullivan [3]. Namun demikian, perlu diingat juga bahwa akhir-akhir ini marak terjadi serangan siber serta adanya penyalahgunaan data. Dengan demikian, dalam mewujudkan kesadaran akan keamanan siber dapat dimulai dari diri sendiri. Hal yang paling sederhana adalah dengan memahami pemanfaatan *Internet of Things* di sekitar untuk menjamin keamanan dari data dan privasi di dunia maya. Contohnya, adalah dengan secara rutin mengganti kata sandi akun email dan media sosial serta memanfaatkan *software* yang resmi [3].

Oleh karena itu, kehadiran pelaku bisnis di Indonesia juga bukan hanya ingin memberikan efisiensi dan biaya yang lebih rendah kepada perusahaan, tapi diharapkan juga ingin mengamankan data, jaringan, serta sistem produksi yang dimiliki pelanggan. Contoh lain yang menjadi tolak ukur Indonesia dalam kemampuan meraih peluang bisnis di era Industri 4.0 yakni ada pada TUV Rheinland. TUV Rheinland merupakan perusahaan asal Jerman yang lebih dari 145 tahun fokus pada penyedia layanan pengujian, inspeksi, dan sertifikasi. Khusus untuk meningkatkan kemampuan meraih peluang bisnis di era Industri 4.0 melalui transformasi digital [3]. Selain Perusahaan, Negara juga akan menerima limpahan dampak atas perubahan Revolusi Industri 4.0 tersebut. Namun demikian, roadmap tersebut perlu diturunkan dalam agenda dan tataran praktis agar pada saat dikonversi menjadi kebijakan publik mampu diimplementasikan secara komprehensif dan menyeluruh serta terintegrasi dengan seluruh instrument Negara dan Pemerintah. Sehingga mitigasi risiko yang akan muncul dari dampak masuknya era Revolusi Industri 4.0 dapat terukur dan terkendali [4]. Konsep mempersiapkan Republik Indonesia dalam menghadapi revolusi industri 4.0 yang sangat bergantung kepada digitalisasi, khususnya *cyber* yang harus dipahami tantangan dalam keamanan cyber dan perlu diselaraskan dengan fokus pembangunan SDM dan infrastruktur yang selama ini dilakukan pemerintah.

III. METODOLOGI

Naskah penelitian ini menggunakan penelitian deskriptif kualitatif dengan mengumpulkan data berupa bagaimana kesiapan semua sektor dalam menghadapi tantangan (mitigasi dan ancaman) sebagai sebuah sistem keamanan siber, mengulas masalah terkait dengan tantangan dan ancaman keamanan siber di era revolusi industri 4.0, meneliti data dari segi sistem keamanan siber, kesiapan, situasi dan kondusi terhadap tantangan keamanan siber di era revolusi industry 4.0, menganalisis situasi dan kondisi dimulai dari *planning, doing, checking, action, & Evaluation* dan ditutup dengan kesimpulan sebagai solusi dan tindakan. Berikut kerangka pemikiran dalam penulisan artikel ilmiah ini, disajikan pada Gambar 1.1 sebagai berikut :



Gambar 1.1 Kerangka Berpikir

IV. HASIL DAN PEMBAHASAN

A. Tantangan dan Ancaman Keamanan Cyber Indonesia di Era Revolusi Industri 4.0

Sistem keamanan siber harus dapat dibangun dengan terpadu dalam melawan ancaman eksternal dan internal, maupun menghadapi tantangan yang terjadi di era revolusi Industri 4.0. Tantangan ini terjadi pada aspek bisnis di segala bidang yang harus bersiap menghadapi perubahan global dunia yang mengkombinasikan manufaktur tradisional dan praktik industri dengan dunia teknologi. Berdasarkan Breach Level Index, 945 pelanggaran data publik menyebabkan 4,5 miliar catatan data dikompromikan di seluruh dunia pada semester pertama 2018. Dibandingkan periode sama pada 2017, jumlah data yang hilang, dicuri atau dikompromikan meningkat sebesar 133%. Oleh karena itu, berdasarkan beberapa penjelasan tersebut maka sesuai dengan yang disampaikan oleh Zhou dkk (2015) bahwa secara umum ada lima tantangan besar yang akan dihadapi yaitu aspek pengetahuan, teknologi, ekonomi, sosial, dan politik [5].

Selain itu, guna menjawab tantangan tersebut, diperlukan usaha yang besar, terencana, dan strategis baik dari sisi regulator (pemerintah), kalangan akademisi maupun praktisi. Kagermann dkk (2013) menyampaikan diperlukan keterlibatan akademisi dalam bentuk penelitian dan pengembangan untuk mewujudkan Industri 4.0. Menurut Jian Qin dkk (2016) roadmap pengembangan teknologi untuk mewujudkan Industri 4.0 masih belum terarah. Hal ini terjadi karena Industri 4.0 masih berupa gagasan yang wujud nyata dari keseluruhan aspeknya belum jelas sehingga dapat memunculkan berbagai kemungkinan arah pengembangan [6]. Berikut penjelasan tantangan industri disajikan pada Tabel 1.1:

Tabel 1.1 Tantangan Industri 4.0 (Heckeu et al, 2016) [7]

No	Jenis Tantangan	Keterangan
1	Tantangan ekonomi	1. Globalisasi yang terus berlanjut: a. Keterampilan antarbudaya b. Fleksibilitas waktu c. Keterampilan jaringan. 2. Meningkatnya kebutuhan akan inovasi: a. Pemikiran wirausaha b. Kreativitas, c. Pemecahan masalah d. Bekerja di bawah tekanan e. Pengetahuan mutakhir 3. Permintaan untuk orientasi layanan yang lebih tinggi: a. Pemecahan konflik b. Kemampuan komunikasi c. Kemampuan berkompromi d. Keterampilan berjejaring 4. Tumbuh kebutuhan untuk kerja sama dan kolaboratif: a. Mampu berkompromi dan kooperatif b. Kemampuan bekerja dalam tim c. Kemampuan komunikasi d. Keterampilan berjejaring
2	Tantangan Sosial	1. Perubahan demografi dan nilai sosial: a.Kemampuan mentransfer pengetahuan b.Penerimaan rotasi tugas kerja dan perubahan pekerjaan yang terkait c. Fleksibilitas waktu dan tempat d. Keterampilan memimpin 2. Peningkatan kerja virtual: a. Fleksibilitas waktu dan tempat b. Keterampilan teknologi

No	Jenis Tantangan	Keterangan
		c. Keterampilan media d. Pemahaman keamanan TI 3.Pertumbuhan kompleksitas proses: a. Keterampilan teknis b. Pemahaman proses c. Motivasi belajar
3	Tantangan Teknis	1. Perkembangan teknologi dan penggunaan data eksponensial: a. Keterampilan teknis b. Kemampuan analisis c. Efisiensi dalam bekerja dengan data d. Keterampilan koding e. Kemampuan memahami keamanan TI f. Kepatuhan 2. Menumbuhkan kerja kolaboratif: a. Mampu bekerja dalam tim b. Kemampuan komunikasi virtual c. Keterampilan media d. Pemahaman keamanan TI e. Kemampuan untuk bersikap kooperati
4	Tantangan Lingkungan	Perubahan iklim dan kelangkaan sumber daya: a. Pola pikir berkelanjutan b. Motivasi menjaga lingkungan c. Kreativitas untuk mengembangkan solusi keberlanjutan baru
5	Tantangan Politik dan Aturan	1. Standarisasi: a. Keterampilan teknis b. Keterampilan koding c. Pemahaman proses 2. Keamanan data dan privasi: a.Pemahaman keamanan teknologi informasi b. Kepatuhan

Berdasarkan data-data di atas, Eset menilai ada tiga tantangan yang akan di hadapi perusahaan di Industri 4.0:

1. Target serangan

Bukan rahasia lagi, manufaktur adalah industri yang menjadi tujuan *targeted atttack* dalam serangan siber. Menurut studi *Enterprise Enviromental Factor* (EEF), 48% produsen di beberapa titik telah mengalami insiden keamanan, dan setengah dari organisasi tersebut menderita kerugian finansial atau gangguan terhadap bisnis mereka. Menurut survei, industri manufaktur adalah yang paling ditargetkan untuk serangan siber, tepat berada di belakang sektor publik dan bisnis keuangan. *Industrial Control System* (ICS) atau *Supervisory Control And Data Acquisition* (SCADA) adalah perangkat lunak yang paling sering digunakan dalam industri manufaktur, infrastruktur dan berbagai bidang lain, merupakan titik terlemah dalam sistem keamanan perusahaan. Contoh kasusnya adalah serangan malware *BlackEnergy* (2015) dan *Industroyer* (2016) yang memadamkan listrik di Ukraina atau serangan Stuxnet di Iran. Kasus terbaru adalah *GreyEnergy* (2018), yang dirancang untuk sasaran lebih luas. Perlu dicatat bahwa ICS/SCADA digunakan bukan hanya di manufaktur, tetapi juga pada pembangkit listrik, perusahaan transmisi, pengolahan minyak dan gas, pabrik-pabrik, bandara sampai layanan pengiriman.

2. Ransomware

Menurut laporan Verizon 2018, 56% insiden malware melibatkan ransomware, sehingga menjadikannya sebagai bentuk *malware* yang paling umum. Selain itu, hal paling memprihatinkan adalah peretas mengalihkan perhatian mereka ke sistem penting seperti server daripada perangkat karyawan. Dalam praktiknya, *ransomware* oleh pengembangnya

dikolaborasikan dengan botnet, bahkan CryptoJacking untuk mendapatkan keuntungan ganda. Oleh karena itu, menghadapi *ransomware* memang bukan perkara mudah, sehingga bagi sebuah perusahaan memiliki alat proteksi dari *ransomware* bukan suatu hal yang bisa ditawar karena *ransowmare* tidak pernah pilih-pilih ketika menyerang korbannya.

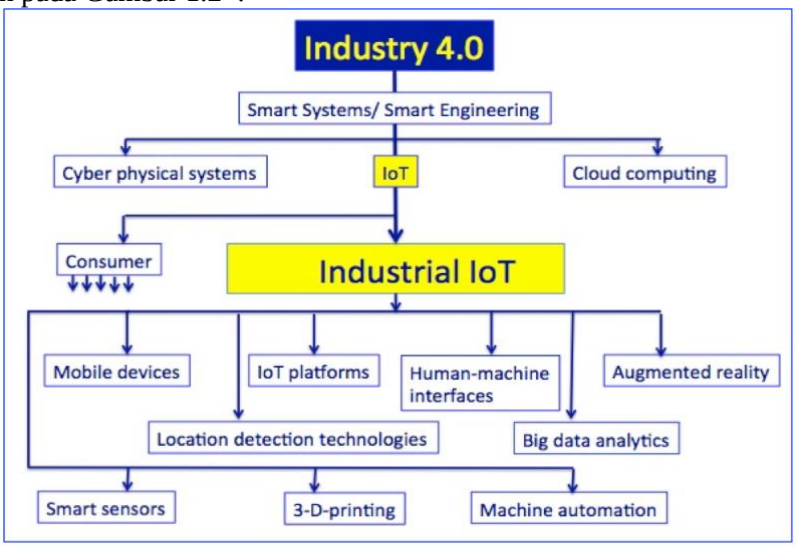
3. Orang dalam

Menurut Eset, ada kesenjangan antara pengetahuan karyawan dan perkembangan keamanan siber. Akar masalah dari kerentanan, 52% diantaranya dinilai berasal dari kesalahan karyawan yang dilakukan secara tidak sengaja, seperti salah copy file, salah kirim file, meninggalkan komputer dalam keadaan terbuka saat tidak dipakai, dan lain-lain. Ponemon Institute dalam studinya mengatakan, satu dari empat kebocoran data disebabkan oleh orang dalam yang dilakukan sengaja dengan motivasi finansial, spionase dan persaingan bisnis. Oleh karena itu, untuk menghadapi tantangan keamanan di Industri 4.0, pelaku bisnis diimbau untuk menggunakan solusi keamanan [9]. Perlu diketahui juga ada enam langkah penting dalam merencanakan dan merancang keamanan siber. Keenam langkah itu adalah penaksiran aset dan risko, membangun kebijakan, pemilihan perangkat dan pelaksanaan, implementasi, edukasi ke seluruh pemangku kebijakan, dan pengujian sistem secara berkelanjutan [4].

B. Kesiapan Indonesia: Sektor Pemerintah, Pelaku Bisnis/Swasta/Perusahaan, dan Masyarakat Digital

Indonesia diakui masih banyak mempunyai permasalahan yang harus diselesaikan di sisi keamanan siber. Dalam dokumen Global *Cybersecurity Index* 2017 yang diterbitkan oleh ITU-D, Indonesia mendapatkan nilai 0.424 dan berada di posisi nomor 69 dari 164 negara dengan status *Maturing* (sedang menuju kesiapan). Komponen-komponen yang masih mendapatkan penilaian merah adalah: CERT sektor, standar organisasi, strategi keamanan siber, matriks keamanan siber, good practice, program edukasi, industri dalam negeri, perjanjian bilateral, perjanjian multilateral, serta kerjasama antara pemerintah dan swasta [4].

Hal lain yang penting juga bahwa perusahaan-perusahaan di Indonesia mesti mempunyai sertifikasi kesiapan memasuki revolusi industri 4.0, karena saat masyarakat menikmati manfaat *Internet of Things* (IoT) yang nirkabel dan *Industrial Internet of Things* (IIoT), berbagai risiko tidak dapat dihindari. Hal ini membuat para pelaku bisnis menuntut adanya solusi untuk mengamankan sistem suplai pusat, pertukaran data yang aman, dan adanya sistem produksi yang bisa diandalkan [4]. Berikut Gambaran mengenai Penjelasan Industri 4.0 dengan Industri IoT disajikan pada Gambar 1.2 :



Gambar 1.2 Industri 4.0 dengan Industri IoT

Kementerian Perindustrian telah merancang *Making Indonesia* 4.0 sebagai sebuah *roadmap* yang terintegrasi untuk mengimplementasikan sejumlah strategi dalam memasuki era Industri 4.0. Peneliti *Center for Indonesian Policy Stuides* (CIPS) Imelda Freddy menyatakan pada dasarnya industri 4.0 [10] memperkenalkan era *smart factories* di mana

mekanisme robot atau sistem fisik siber akan mengawasi proses fisik yang terjadi di dalam pabrik. Sistem itu memiliki kemampuan untuk membuat keputusan sendiri sehingga dengan adanya perubahan tren industri seperti ini muncul kekhawatiran kalau peluang pekerjaan akan berkurang karena diambil alih robot dan mesin. Ia menjelaskan peningkatan kapasitas bisa dilakukan lewat pelatihan, kursus, dan sertifikasi. Para pelaku industri harus ikut serta dalam upaya ini karena peningkatan kapasitas pekerja akan berdampak positif terhadap industri itu sendiri [8]. Berikut kesiapan Pemerintah Indonesia dalam menghadapi ancaman dan tantangan siber di era revolusi Industri 4.0, antara lain:

1. Pembentukan Kinas

Menko Perekonomian menjelaskan pihaknya ingin membangun komunikasi yang berkelanjutan dalam kaitannya dengan revolusi industri keempat. Oleh karena itu, pemerintah telah membentuk Kinas untuk mendorong penyelarasan lintas kementerian dan lembaga maupun pemangku kepentingan agar sektor industri mendapatkan manfaat dari era kecanggihan teknologi 4.0.

2. Perekonomian Jasa

Satu faktor yang perlu dilihat pula adalah sektor jasa pada saat ini dinilai mulai mendominasi kondisi perekonomian nasional sehingga merupakan hal yang bagus karena negara-negara maju pada saat ini juga didominasi sektor jasa.

3. Revitalisasi manufaktur

Sementara itu, Kepala Badan Penelitian dan Pengembangan Industri (BPPI) Ngakan Timur Antara mengatakan, implementasi Industri 4.0 akan membawa peluang besar untuk merevitalisasi sektor manufaktur dan menjadi akselerator dalam mencapai visi Indonesia menjadi 10 besar ekonomi dunia pada tahun 2030. “Jadi, akan meningkatkan produktivitas industri kita dan dapat menciptakan lapangan kerja baru yang lebih bernilai tambah tinggi sebagai dasar dari fondasi pertumbuhan ekonomi Indonesia di masa datang,” tuturnya [9].

C. Solusi (Kebijakan, Antisipasi, dan Tindakan)

BSSN ada rencana untuk mengantisipasi keamanan siber seluruh provinsi di Indonesia. BSSN akan tawarkan ke provinsi-provinsi, sebuah data center yang nanti dikoneksikan langsung ke BSSN, penjelasan tersebut dari Bapak Djoko Setiadi (Kepala BSSN) di Jakarta. Selain itu, dapat dikaji juga dari sisi perspektif US mengenai Cyber Domain. Cyber Domain berdasarkan penjelasan Aziz Rahmani dalam materi pertemuan sekolah Keamanan Nasional, Universitas Bhayangkara Jakarta tahun 2019, Aziz menjelaskan bahwa ada 4 kategori cyber domain yang mungkin dapat diadopsi oleh Indonesia dari US [10].

a. Operasional Siber (*Cyber Operation*)
- ICT/ TIK : *Defending ICT networks*, sistem, dan informasi TIK.
- Operasi Jaringan: Menyediakan dan mengoperasikan jaringan militer sistem global (C4ISR)
- Operasi Defensif siber: Melestarikan dan melindungi kemampuan ruang *cyber* yang mencakup data, *net-centric, sistem,* dan jaringan.

b. Intelijen Siber (*Inteligence Cyber*)
- Penggunaan kemampuan siber untuk mendukung operasi intelijen.

c. Cyber Crime
- Keamanan dan penegakan hukum di area dunia maya.

d. Operasional Informasi (*Information Operation*)
- Penggunaan teknologi informasi dan informasi di arena politik, ekonomi, (ilmu & teknologi), diplomatik, budaya, dan militer untuk mengamankan keuntungan informasi.
- Persaingan informasi di masa perang dan / atau perdamaian dan bersifat global.
- Operasi psikologis (PSYOP), Urusan Publik, dan Komunikasi Strategis.

V. KESIMPULAN

Tantangan Indonesia saat ini dalam keamanan siber di era revolusi industri 4.0 yakni cara membangun sistem keamanan melawan ancaman eksternal dan internet. Tantangan tersebut di bidang ekonomi, sosial, teknis, lingkungan,d& politik. Tantangan industri tersebut terhadap keamanan siber dikategorikan dalam 3 tantangan: target serangan, ransomware, dan orang dalam. Oleh karena itu, dalam mengatasi tantangan keamanan siber di era Revolusi Industri, maka kesiapan Indonesia mulai dari sektor pemerintah, pelaku bisnis, dan masyarakat digital antar lain: kesiapan masyarakat digital yang mandiri dan pengetahuan tinggi terhadap bahaya serangan siber, setiap perusahaan memerlukan sertifikasi kesiapan memasuki revolusi industri, 4.0, sinergitas, perencanaan dan strategi sesuai dengan implementasi yang baik di setiap Kementerian dan lembaga terkait bidang keamanan siber. Sebagai contoh adanya 10 inisiatif Making Indonesia 4.0 didukung dengan peningkatan keamanan siber, kapasitas dan kualitas SDM/pekerja Indonesia. Contoh lainnya adalah pembentukkan Kinas (Komite Industri Nasional), revitalisasi manufaktur, dan adanya pembentukkan data center oleh BSSN di setiap daerah. Saran dari penulisan ini adalah masih perlu dibahas lebih lanjut bagaimana implementasi peningkatan kapasitas dan kualitas SDM di bidang keamanan siber yang siap untuk dipekerjakan di era Revolusi Industri. Dengan demikian, Pemerintah, khususnya Kementerian Perindustrian lebih jelas dalam memberikan indikator penilaian kesiapan Industri 4.0 di Indonesia.

DAFTAR PUSTAKA

[1] Gloria. 2019. *Kesiapan Keamanan Siber Indonesia di Era Revolusi Industri 4.0* diakses dari https://www.ugm.ac.id/id/news/17376kesiapan.keamanan.siber.indonesia.di.era.revolusi.industri.40, pada tanggal 10 Maret 2019 pukul 21.35 WIB.

[2] Marsudi, Almatius Setya dan Yunus Widjaja. *Industri 4.0 dan Dampaknya Terhadap Financial Technology serta Kesiapan Tenaga Kerja Indonesia*. Ikraith Ekonomika,Vol.2, No.2, Bulan Juli. PPAK Universitas Katolik Indonesia Atma Jaya Jl. Jendral Sudirman 51 Jakarta. Hlm. 8.

[3] Koran Jakarta. 2019. Perusahaan Mesti Punya Standar Digital Industri 4.0 diakses dari http://www.koran-jakarta.com/perusahaan-mesti-punya-standar-digital-industri-4-0/ pada tanggal 12 Maret 2019 pukul 22.49 WIB.

[4] Karyoto. 2019. *Ancaman Cyber Security di Era Industri 4.0 Bakal Semakin Beragam dan Masif.* Diakses dari https://eksekutif.id/ancaman-cyber-security-di-era-industri-4-0-bakal-semakin-beragam-dan-masif/. Pada tanggal 17 Maret 2019, pukul 18.59 WIB.

[5] Suparjono. 2019. *Revolusi Industri 4.0 dan Dampak terhadap Sumber Daya Manusia*. Diakses dari : https://www.kompasiana.com/suparjono46018/5b3fa2fecaf7db4f2b538085/revolusi-industri-4-0-dan-dampak-terhadap-sumber-daya-manusia. Pada tanggal 20 maret 2019, pukul 22.39 WIB.

[6] Prasetyo, Hoedi dan Wahyudi Sutopo.2018. *Industri 4.0: Telaah Klasifikasi Aspek dan Arah Perkembangan Riset.* J@ti Undip: Jurnal Teknik Industri, Vol. 13, No. 1, Januari 2018. Hlm 18.

[7] Yahya, Muhammad. 2018. E*ra Industri 4.0: Tantangan dan Peluang Perkembangan Pendidikan Kejuruan Indonesia*. Orasi Ilmiah Professor bidang Ilmu Pendidikan Kejuruan Universitas Negeri Makassar Tanggal 14 Maret 2018.

[8] Librianty, Andina. 2019. *Ini 3 Tantangan Keamanan Siber di Industri 4.0*. Diakses dari https://www.liputan6.com/tekno/read/3689405/ini-3-tantangan-keamanan-siber-di-industri-40, tanggal 19 Maret 2019, Pukul 18.40 WIB.

[9] Kementerian Perindustrian. 2019. *Making Indonesia 4.0 Strategi RI Masuki Revolusi Industri ke-4*. Diakses dari http://www.kemenperin.go.id/artikel/18967/Making-Indonesia-4.0:-Strategi-RI-Masuki-Revolusi-Industri-Ke-4, pada tanggal 22 Maret 2019, pukul 17.45 WIB

[10] Rahmani, Aziz. 2019. I*nformation Warfare and Cyber Security.* Materi Sekolah Keamanan Nasional, Universitas Bhayangkara Jakarta, Puskamnas Ubhara Jaya, 3 Januari 2019.

Cynthia Rahmawati, S.Si,M.Si (Han). adalah lulusan Magister Ilmu Pertahanan, Universitas Pertahanan Tahun 2016 dengan predikat sangat memuaskan nilai IPK 3,78. Gelar Sarjana Biologi diraih dengan predikat *Sangat Memuaskan* nilai IPK 3.35 di Fakultas MIPA Jurusan Biologi Universitas Lampung tahun 2009. Bidang penelitian yang sedang ditekuni saat ini adalah *Biosecurity, Cyber Security, National Security System, Statistic, Human Resources & Development, and Industry Technology*, serta masih aktif sebagai dosen tetap untuk Prodi Teknik Industri, Manajemen Informatika dan Prodi Sistem Informasi di Universitas Marsekal Dirgantara Suryadarma, Halim, Jakarta.