

Fenomena Keamanan Informasi Pasca Era Revolusi Industri 5.0

Tri Yusnanto¹⁾, Khoirul Mustofa²⁾, Moch Ali Mahmudi³⁾, Sugeng Wahyudiono⁴⁾

^{1,3,4)} “Manajemen Informatika” STMIK Bina Patria

²⁾ “Sistem Informasi” Universitas Duta Bangsa

Email : yusnanto@stmikbinapatria.ac.id¹⁾, khoirulmustofa@universitasdutabangsa.ac.id²⁾,
aliadinata@gmail.com³⁾, farrosgisaka@gmail.com⁴⁾

Abstract

At this time an Information System Security is very interesting to review relating to the development of technology in the current era and the value of its use, in this paper will discuss the forms of information security threats to information security systems in the post-industrial revolution 5.0 era, this is the foundation we are in information security by understanding several phenomena and trends in the development of internet use, studying the interrelationships of several information security threats after the industrial revolution 5.0, the importance of information security based on the axiological paradigm as a basis for thinking for the application of information security systems in the post-industrial revolution 5.0, this paper contains several suggestions for The direction of information security scientific development in facing the post-industrial revolution 5.0 era is based on the philosophy of science and how to implement an information security system based on information technology and science.

Keywords: *Information Security, Security Threats, Industrial Revolution 4.0, Technology.*

Abstrak

Pada saat ini sebuah Kemanan Sistem Informasi meruakan yang sangat menarik untuk diulas yang berkaitan dengan berkembangnya teknologi pada diera saat ini dan nilai kegunaanya, pada makalah ini akan membahas tentang bentuk ancaman keamanan informasi terhadap sistem keamanan informasi di era pasca revolusi industri 5.0, ini merupakan pondasi kita dalam keamanan informasi dengan memahami beberapa fenomena serta tren perkembangan penggunaan internet, mempelajari keterkaitan beberapa ancaman keamanan informasi pasca revolusi industri 5.0, pentingnya keamanan informasi berdasarkan paradigma aksiologi sebagai dasra berfikir untuk penerapan sistem keamanan informasi pada pasca revolusi industri 5.0, peper ini berisikan beberapa saran terhadap arah perkembangan keilmuan keamanan informasi dalam menghadapi era pasca revolusi industri 5.0 berdasar dari filsafat ilmu serta cara menerapkan sistem keamanan informasi yang berdasar teknologi informasi dan keilmuan.

Kata kunci : *Keamanan Informasi, Ancaman Keamanan, , Pasca Revolusi Industri 5.0, Teknologi.*

1. Pendahuluan

Tiap hari teknologi berkembang sangat cepat ini membuktikan bahwa kita sebagai manusia dapat berfikir dalam kehidupannya, pada saat mereka mendapatkan masalah dan serta solusi apa yang mereka gunakan untuk memecahkan juga menyelesaikan kendala itu, sehingga solusi tersebut menjadi dasar pemikiran terciptanya ide-ide baru, perkembangan akan teknologi informasi dapat memberikan kemudahandidalam kehidupan kita, akan tetapi dengan adanya perkembangan teknologi informasi juga

selalu memiliki aspek negatif salah satunya adalah masalah keamanan (*security*) [2]. Keamanan akan sebuah informasi memang menjadi salah satu hal yang sangatlah penting, terutama pasca era revolusi industri 5.0 menjadi bukti bahwasanya kehidupan dan keberlanjutan perkembangan teknologi informasi itu ada, Revolusi Industri 5.0 merupakan istilah yang relatif baru mungkin saja masih belum banyak diketahui dan dipahami oleh khalayak. Bapak Menteri Perindustrian dan Perdagangan Airlangga Hartarto yang dikutip dari Gliemourinsie [3], bahwa Industri 4.0 penopang utama sebuah proses produksi yaitu menggunakan internet. Dimana kebanyakan obyek yang berjalan dilengkapi perangkat teknologi canggih disertai beberapa sensor serta dapat saling berkomunikasi sendiri dengan sistem teknologi informasi yang berjalan tersebut.

Sekarang Pasca Revolusi industri 4.0 sudah tidak dapat dicegah lagi, Oleh karena berbagai bidang bisnis haruslah siap dalam menghadapi segala perubahan dunia global yang mana mereka mengkombinasikan manufaktur tradisional dan praktik industri dengan dunia teknologi. Hal tersebut dapat memicu berbagai tantangan, ini bukan hanya masalah dalam implementasi berbagai produksi yang menggunakan teknologi digital, *machine learning* serta data yang besar atau dengan istilah *big data*, tapi juga cara membangun sistem keamanan melawan ancaman eksternal dan internet. Dikutip dari ungkapan perusahaan keamanan, Eset, para pelaku industri 4.0 juga mengalami ancaman dunia maya yang sama seperti organisasi lain, karena bisnis dari semua ukuran menjadi sasaran kejahatan siber yang terus meningkat dari tahun ke tahun. Menurut data dari Ponemon Institute dalam studi 2018-nya, rata-rata kerugian akibat pelanggaran data secara global tahun ini mencapai \$3,86 juta, meningkat 6,4 persen dibandingkan tahun 2017[1].

Jika mencermati penjelasan di atas mengenai keterkaitan antara munculnya pasca revolusi industri 4.0 yang erat kaitannya dengan perkembangan teknologi informasi, kehadirannya tidak lepas dari pengaruh ilmu pengetahuan di bidang IT. dan jika dilihat dari berbagai titik keamanan informasi, ancaman yang muncul akibat adanya revolusi industri 4.0 yang artinya erat kaitannya dengan ilmu pengetahuan dan kemajuan informasi atau cybersecurity. Ruang lingkup penelitian yang semula sempit diperluas. Kondisi ini menimbulkan pertanyaan apakah perkembangan kejahatan atau sibernetika ada kaitannya dengan munculnya fenomena Industri 4.0. Dan apa pengaruh fenomena Industry 4.0 terhadap ancaman keamanan informasi? Seberapa pentingkah keamanan informasi dilihat dari fenomena yang ada di industri 4.0? Hal ini akan dijawab dengan menelaah dan menganalisis kembali nilai ekuitas berdasarkan risiko yang dialami oleh ancaman terhadap keamanan informasi.

Dalam artikel ini, penulis mencoba menjawab pertanyaan-pertanyaan tersebut berdasarkan evaluasi berdasarkan fenomena yang ada, serta menggali materi melalui studi literatur dan sekaligus memberikan saran tentang arah pengembangan ilmiah di bidang keamanan. informasi sehingga aplikasi keamanan informasi dapat disesuaikan dengan perkembangan dunia maya atau kejahatan di dunia maya..

2. Kajian Literatur

Secara etimologis istilah filsafat berasal dari kata *philosophia* (Yunani) yang terdiri dari kata *philos* (cinta) dan *sophia* (kebijaksanaan), sehingga dapat diartikan sebagai cinta kebijaksanaan. Sedangkan menurut Samir (2002), ilmu adalah suatu usaha untuk memahami, menjelaskan dan meramalkan semua sifat-sifat yang ada di alam semesta dengan menggunakan metode ilmiah. Filsafat dan ilmu merupakan dua hal yang saling berkaitan, sehingga dalam perkembangannya menjadi kajian tersendiri yang disebut filsafat ilmu. Filsafat ilmu memiliki hubungan yang erat dengan metode ilmiah. Samir (2002) memberikan pemahaman sederhana bahwa filsafat ilmu adalah. cara menguji asumsi dan metode yang digunakan ilmuwan untuk menghasilkan pengetahuan. Filsafat ilmu memiliki tiga landasan pemikiran utama, yaitu, (1) Ontologi, suatu analisis terhadap objek yang dipelajari oleh ilmu pengetahuan. (2) Epistemologi, analisis metode yang digunakan untuk membangun pengetahuan. (3) Aksiologi, analisis penerapan dan manfaat temuan ilmu pengetahuan [13].

Perkembangan ilmu tidak terlepas dari rasa keingintahuan yang besar serta diiringi dengan berbagai usaha yang sungguh- sungguh melalui penalaran, percobaan, penyempurnaan, dan berani mengambil resiko tinggi (Karim, 2012). Berdasarkan hal tersebut filsafat ilmu berperan dalam mendorong ilmuwan dan para ahli agar selalu mempelajari dan mengarahkan tentang bagaimana seharusnya memanfaatkan ilmu serta ke mana ilmu harus dikembangkan. *Kattsoff*, sebagaimana dikutip oleh *Associate Webmaster Professional* (2001), menyatakan karakteristik filsafat sebagai berikut. (1) Filsafat adalah berpikir secara kritis, (2) Filsafat adalah berpikir dalam bentuk sistematis, (3) Filsafat menghasilkan sesuatu yang runtut, (4) Filsafat adalah berpikir secara rasional, (5) Filsafat bersifat komprehensif.

Keamanan Informasi

Keamanan informasi adalah perlindungan informasi dari berbagai ancaman untuk menjamin kelangsungan proses bisnis, mengurangi risiko bisnis, dan meningkatkan laba atas investasi (ROI) dan peluang bisnis (Chaeikar, dll., 2012). Dalam merancang suatu sistem keamanan sistem informasi, ada aspek keamanan informasi yang harus diperhatikan. Aspek-aspek tersebut meliputi Kerahasiaan, Integritas, Ketersediaan. Menurut (Whitman & Mattord, 2011) informasi merupakan salah satu aset yang penting untuk menjaga keamanannya. Perusahaan harus memperhatikan keamanan aset informasi mereka, kebocoran informasi dan kegagalan sistem dapat menyebabkan kerugian baik dari segi finansial maupun produktivitas bisnis [10].

Keamanan informasi menurut G.J. Simons adalah upaya untuk mencegah terjadinya kecurangan (cheating) atau untuk mendeteksi kecurangan dalam sistem berbasis informasi, dimana informasi itu sendiri tidak memiliki arti fisik. Aspek-aspek yang harus dipenuhi dalam suatu sistem untuk menjamin keamanan informasi adalah bahwa informasi yang diberikan akurat dan lengkap (correct information), bahwa informasi tersebut berada di tangan orang yang berwenang (appropriate person), dapat diakses. dan digunakan sesuai kebutuhan (tepat waktu), dan memberikan informasi dalam format yang benar.

Revolusi Industri 4.0 dan Kaitannya dengan Ancaman Keamanan Informasi

Pasca revolusi industri 4.0 Ini adalah tren di dunia industri yang menggabungkan teknologi otomasi dengan teknologi siber. Di Industri 4.0, teknologi manufaktur telah memasuki tren otomatisasi dan pertukaran data. Ini termasuk sistem cyber-fisik, Internet of Things (IoT), komputasi awan, dan komputasi kognitif.



Gambar 1. Penggunaan Augmen Rality dalam kehidupan.

Era 5.0 merupakan sebuah era *Super Smar Society* adalah sebuah tanggapan dari era 4.0 yang memungkinkan setiap perusahaan untuk mengidentifikasi dan mengimplementasikan berbagai skenario, diantaranya adalah:

1. Elaborasi dengan sistem
2. Interoperabilitas (kesesuaian)
3. *Problem solver*
4. Transparansi Informasi
5. Bantuan Teknis
6. Keputusan Mandiri

Fenomena

adalah suatu fakta atau peristiwa yang dapat diamati fenomena yang secara sadar dan individual dialami oleh sekelompok individu dalam kehidupan mereka Istilah phainomeno ini mulai digunakan dalam filsafat modern melalui Immanuel Kant, yang membandingkan fenomena dengan noumena, yang tidak dapat diamati secara langsung. Sebenarnya Ilmu ditemukan seharuna untuk membantu manusia agar hidup lebih baik. Dengan menggunakan ilmu tersebut semua kebutuhan manusia diharapkan dapat terpenuhi dengan cepat serta mempermudah semua yang dikerjakan. Peradaban manusia akan sangat bergantung pada sejauh mana ilmu ia manfaatkan. Dalam

penggunaan filosofis modern, istilah fenomena berarti "apa yang dialami berdasarkan kenyataan".

Dalam disertasi pertamanya yang berjudul Tentang bentuk dan prinsip dunia yang masuk akal dan dapat dipahami, Immanuel Kant (1770) ber-teori bahwa pikiran manusia terbatas pada dunia logis. Oleh karena itu, pikiran manusia hanya dapat menafsirkan dan memahami peristiwa menurut tampilan fisiknya. Dia menulis bahwa manusia dapat menyimpulkan sebanyak yang indra dapat rasakan, tetapi mereka tidak mengalami atau merasakan objek itu sendiri. [3] Ini mungkin masuk akal dalam hal saluran komunikasi (epistemologi) yang berasal dari seperangkat input realitas (ontologi), tetapi tidak dalam arti menerapkan imajinasi yang bijaksana (gaya Albert Einstein, untuk keberhasilan parsial).

Dengan demikian, istilah fenomena mengacu pada setiap peristiwa yang layak untuk diteliti dan diselidiki, terutama proses dan peristiwa yang sangat tidak biasa atau memiliki arti khusus. Sains dianggap berkaitan dengan moralitas. Menurut data dari Ponemon Institute dalam studi 2018-nya, kerugian rata-rata akibat pelanggaran data secara global tahun ini adalah \$3,86 juta, meningkat 6,4 persen dibandingkan tahun 2017[1].

Nilai suatu ilmu akan tergantung pada sejauh mana para ilmuwan memiliki tanggung jawab sosial atas pengetahuan yang mereka miliki, apakah itu digunakan untuk kebaikan atau sebagai kejahatan. Oleh karena itu, ilmu pengetahuan akan maju jika ilmuwan memiliki peradaban [14].

Mengutip Bramei, aksiologi terbagi menjadi 3 bagian penting, antara lain: (a) Perbuatan moral yang melahirkan etika (b) Ungkapan keindahan yang menimbulkan estetika (c) Kehidupan sosial-politik yang melahirkan sosial politik. filsafat.

Kesimpulannya bahwa secara aksiologi nilai ilmu yang diperoleh seseorang akan melihat dampak manfaat yang diperolehnya tergantung sejauh mana orang tersebut menggunakan ilmunya apakah ilmu tersebut digunakan untuk kebaikan atau sebaliknya. Kaitan Fenomena dengan filsafat ilmu

Nilai bersifat objektif, tetapi terkadang subjektif. Dikatakan objektif jika nilai-nilai itu tidak bergantung pada subjek atau hati nurani yang menilai. Titik acuan suatu gagasan ada pada objeknya, bukan pada subjek yang melakukan evaluasi. Kebenaran tidak tergantung pada kebenaran pendapat individu tetapi pada objektivitas fakta. Sebaliknya, nilai menjadi subjektif jika subjek berperan dalam evaluasi; kesadaran manusia menjadi tolak ukur evaluasi. Oleh karena itu, nilai subjektif selalu memperhatikan berbagai pendapat yang dimiliki pikiran manusia, seperti perasaan yang akan menajam menjadi suka atau tidak suka, suka atau tidak suka.

Salah satu faktor pembeda antara pernyataan ilmiah dan asumsi umum adalah objektivitasnya. Seorang ilmuwan harus melihat realitas empiris dengan mengesampingkan kesadaran ideologis, agama, dan budaya. Nilai-nilai objektif hanya merupakan tujuan utama, tidak terikat pada nilai-nilai subjektif.

Dimensi Ilmu, Teknologi, dan Ancaman Keamanan Informasi

Penggunaan teknologi oleh manusia berkembang sangat pesat. Banyak teknologi baru yang diciptakan oleh manusia untuk memudahkan kebutuhan Anda. Misalnya teknologi telekomunikasi, teknologi internet, teknologi industri, teknologi pertanian dan lain-lain. Teknologi merupakan hasil pemikiran manusia yang mengolah suatu keadaan sehingga dapat beradaptasi dengan dirinya sendiri. Teknologi juga merupakan instrumen bagi manusia untuk memenuhi tidak hanya kebutuhan dasarnya yaitu pangan, mobilitas, komunikasi dan pertahanan, tetapi juga kebutuhan untuk meningkatkan kualitas hidupnya. Teknologi menjadi topik penting untuk kepentingan manusia. Teknologi itu sendiri adalah kemampuan menerapkan suatu ilmu pengetahuan dan kependaian membuat sesuatu yang berkenaan dengan pengetahuan dalam suatu produk, yang berhubungan dengan tren perkembangan serta berlandaskan pengetahuan

ilmu eksakta berdasarkan pada aplikasi dan implikasi ilmu pengetahuan itu sendiri. Ilmu pengetahuan yang dimiliki jika digunakan ilmu pengetahuan tersebut dengan sebaik mungkin maka permasalahan yang ada dalam kehidupan manusia akan teratasi dengan mudah. Keamanan informasi belakangan ini menjadi isu yang sangat penting untuk dibahas, perkembangan ilmu pengetahuan yang dipengaruhi oleh lingkungan merupakan penyebab kemunculan teknologi yang merupakan dasar berkembangnya pola pikir manusia dalam memanfaatkan teknologi yang berkembang untuk kemudahan dalam kehidupan sehari-hari, untuk membeli sesuatu benda misalnya seseorang tidak perlu untuk datang ke toko atau tempat yang menjual benda tersebut melalui teknologi e-commerce seseorang sudah dapat dengan mudah untuk memperoleh benda yang ia inginkan, transaksi keuangan atau perbankan saat ini sudah tersedia mobile banking, e-banking dan internet banking. Namun dibalik kemudahan itu semua ternyata membuka peluang yang besar bagi ancaman keamanan informasi, tidak semua perkembangan teknologi yang didasarkan oleh perkembangan ilmu pengetahuan memiliki dampak yang baik, ada hal yang harus di perhatikan dalam memanfaatkan ilmu pengetahuan tersebut dalam perkembangan teknologi

3. Metode Penelitian

Berdasar latar belakang di atas, tulisan ini berusaha melihat permasalahan dari sudut pandang filsafat ilmu mengenai bagaimana sebenarnya kemunculan jenis ancaman keamanan informasi yang baru akibat dari keberadaan revolusi industri 5.0 jika dikaitkan dengan perkembangan keilmuan teknik keamanan informasi dan apa tantangan apa yang akan dihadapi dalam mengamankan informasi terkait hadirnya Revolusi Industri 5.0. Langkah-langkah yang dilakukan adalah sebagai berikut,

1. Mengumpulkan informasi melalui literatur buku, artikel dan website terkait filsafat ilmu, perkembangan keilmuan Ilmu Komputer, Keamanan Informasi dan Revolusi Industri 5.0,
2. Menarik keterkaitan antara perkembangan keilmuan keamanan informasi dengan munculnya fenomena Revolusi Industri 5.0,
3. Menguraikan hubungan aksiologi terhadap perkembangan pengguna internet dan ancaman keamanan informasi di era revolusi industri 5.0
4. Menyusun gambaran mengenai tantangan ancaman keamanan informasi yang akan dihadapi dalam menghadapi Revolusi Industri 5.0,
5. Memberikan saran terhadap arah perkembangan keilmuan keamanan informasi.

4. Hasil dan Pembahasan

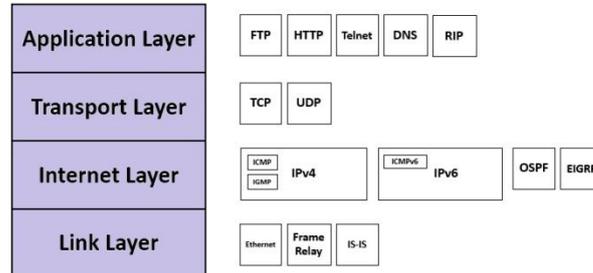
4.1 Filsafat Ilmu Keamanan Informasi

Penyebaran ilmu pengetahuan merupakan salah satu penyebab terjadinya tindakan kejahatan yang dimanfaatkan oleh pihak yang memiliki tujuan dan maksud yang tidak baik. Perkembangan ilmu mendorong terjadinya perubahan manusia dalam bertansaksi secara elektronik dan sebagai upaya mempermudah manusia untuk berbagi sumberdaya informasi, namun sebagian pihak memanfaatkan ilmu pengetahuan untuk tindakan kejahatan sehingga mengancam privasi seseorang dan mengakibatkan dampak kerugian yang cukup besar bagi personal dan organisasi, Upaya pengamanan sebuah sistem informasi didorong oleh adanya ancaman keamanan sebuah sistem informasi

Tujuan yang paling nyata dari keamanan informasi adalah meminimasi dan mencegah adanya modifikasi, pemanfaatan informasi bagi yang tidak berhak, karena sebuah sistem informasi dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sistem ini harus terintegrasi pada keseluruhan subsistem untuk mempersempit atau bahkan menutup adanya celah-celah *unauthorized actions* yang merugikan.

Keamanan pribadi dapat dilakukan dari tahap instalasi sistem hingga terakhir tahap keamanan fisik dan keamanan data. Pengamanan sistem melalui jaringan juga

dapat dilakukan dengan pengamanan FTP, SMTP, Telnet, dan Keamanan Web Server Berikut ini adalah struktur TCP/IP untuk komunikasi informasi atau data.



Gambar 2. Komunikasi TCP/IP dalam Pendistribusian Informasi.

Kebanyak orang menginginkan informasi privasi yang mereka miliki dapat terjamin keamanannya tetapi apa yang dimaksud dengan “informasi aman”? berdasarkan prinsip utama dasar keilmuan keamanan sistem informasi terdapat tiga prinsip utama, jika ketiga prinsip ini terpenuhi maka informasi tersebut dapat dijamin keamanannya ketiga prinsip tersebut yaitu :

1. Kerahasiaan (*Confidentiality*) : Hanya pengguna yang berwenang yang dapat melihat informasi.
2. Integritas (*Integrity*) : Hanya pengguna yang sah yang dapat mengubah informasi.
3. Ketersediaan (*Availability*) : Informasi dapat diakses oleh pengguna yang berwenang kapan pun mereka meminta informasi.



Gambar 3. Tiga Prinsip Keanan Sistem Informasi

4.2 Penanggulangan Global

OECD (*The Organization for Economic Cooperation and Development*) member beberapa rekomendasi yang perlu dilakukan oleh beberapa negara dalam penanggulangan *Cybercrime*, yaitu :

1. Modernisasi hukum pidana nasional dengan hukum acaranya yang diselaraskan dengan konvensi internasional.
2. Meningkatkan sistem keamanan jaringan komputer nasional sesuai standar internasional.
3. Meningkatkan pemahaman dan pengalaman aparat penegak hukum mengenai upaya pencegahan, penyidikan, dan penuntutan kasus-kasus yang berkaitan dengan *cybercrime*.
4. Meningkatkan kesadaran masyarakat akan masalah kejahatan dunia maya dan pentingnya mencegah terjadinya.
5. Meningkatkan kerja sama antar negara, baik di tingkat bilateral, regional maupun

multilateral, dalam upaya penanggulangan kejahatan dunia maya, antara lain melalui perjanjian ekstradisi dan perjanjian bantuan timbal balik.

4.3 Ancaman Kemanan Informasi Pasca Revolusi Industri 4.0

Pasca Revolusi Industri 4.0 adalah konvergensi teknologi informasi kedalam dunia perindustrian. "Mulai dari keamanan siber, *augmented reality* hingga *big data* sudah menjadi bagian dari industri agar menjadi lebih efisien dan *cost-effective*", Kemampuan secara *smart* akan membuat efisien secara konsumsi energi, hal ini menjadi sebuah nilai kewajaran jika dilihat dari kondisi saat ini yaitu penghematan energi bias mengurangi dampak krisis energi, terutama di dunia yang semakin rusak akibat eksploitasi, efisiensi energi menjadi kebutuhan untuk meminimalkannya. Melalui Internet of Things (IoT) dan Big Data, teknologi dapat mengumpulkan data sebelumnya dan kemudian memprediksi apa yang harus dilakukan di masa depan, yang biasa kita sebut machine learning.

Ada dampak negatif dari Revolusi Industri 4.0, meski bukan dari sisi bisnis. Salah satunya terkait privasi individu, masalah privasi di Uni Eropa. Privasi di Uni Eropa dilindungi oleh Peraturan Perlindungan Data Umum (GDPR), yang mengharuskan perusahaan untuk meminta persetujuan konsumen dan memberi tahu mereka bagaimana data mereka disimpan, termasuk kepada siapa mereka mengirimkannya. Peraturan ini sangat ketat dan ketat, terutama untuk perusahaan seperti Google dan Facebook. Kemudian, seiring dengan perkembangan teknologi, ancaman kejahatan menggunakan teknologi juga semakin kompleks. Pelakunya bahkan tidak harus secara fisik berada di tempat kejadian, tetapi melalui koneksi internet mereka dapat merusak sistem, mempengaruhi semua mesin dan teknologi di jaringan. Terdapat tindakan kejahatan dunia maya/siber yang tercatat dari tahun 2017 dan 2018.

Tabel 4.1. Rangkuman catatan Kegagalan kemanan informasi

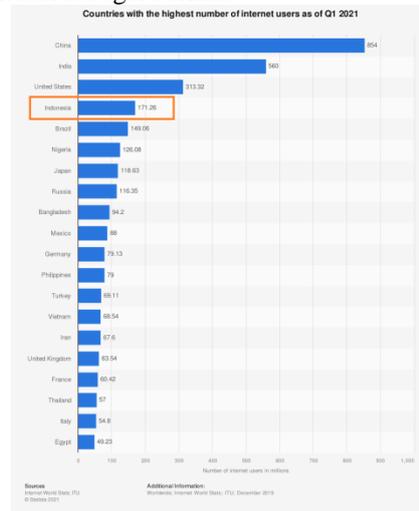
No	Organisasi	Bentuk Kejahatan dan Kegagalan Keamana Informasi
1	BSSN Tahun 2021	Direktorat Operasi Keamanan Siber BSSN mendeteksi indikasi peningkatan jumlah serangan siber yang dilakukan oleh kelompok peretas yang terindikasi berasal dari Brazil. Kelompok tersebut menargetkan sistem elektronik berbagai Kementerian dan Lembaga, Militer, Akademik, serta sektor lain di Indonesia.
	Tahun 2018 BadaSiber dan Sandi Negara (BSSN)	Sesui perkiraan BSSN pada Tahun 2017 Di Indonesia ada 143,4 juta kejahatan siber yang terjadi sejak bulan Januari hingga Juni 2018. BSSN memprediksi bahwa frekuensi serangan akan meningkat di tahun 2019
2	Tahun 2017 Badan Siber dan Sandi Negara (BSSN)	Serangan ransomware WannaCrypt atau WannaCry di tahun 2017 yang berlangsung hingga tahun 2018
3	Kaspersky Lab 2018	Melaporkan bahwa Indonesia berada di peringkat ke-6 dalam daftar negara dengan serangan crypto malware terbanyak pada kuartal ke-3 tahun 2018
4	Sekitar tahun 2017 kampus di Amerika Serikat	Mengalami masalah di jaringan internalnya Perangkat IoT ternyata diretas (dengan cara mencoba-coba password menggunakan metode brute-force). Kemudian perangkat tersebut menyerang DNS di kampus.
5	Layanan cloud dari Amazon.com 2017 Berhenti berfungsi (down) selama beberapa jam	Berbagai perusahaan yang menyediakan layanan untuk publik dan kebetulan menggunakan layanan cloud (S3) dari Amazon ikut berhenti. Setelah diteliti, penyebabnya adalah salah ketik (typo) dari salah seorang operator
6	Sebuah perguruan	Beberapa kasus mahasiswa meminta bantuan cracker untuk

	tinggi	mengubah nilainya.
7	Layanan ISP di Jakarta 2017	Layanan Listrik dari tempat data center dari sebuah <i>Intrnet Services Provider</i> mati sehingga layanannya terhenti. Beberapa electronic market places ikut terkena imbasnya karena mereka ISP tersebut

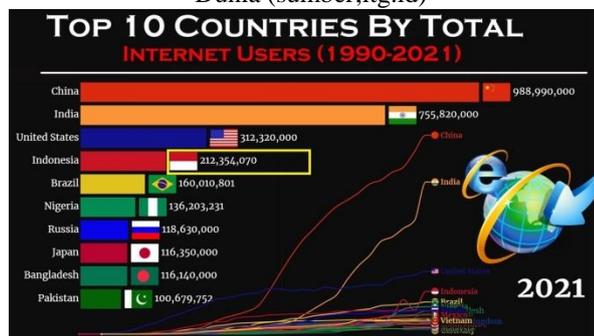
Berdasarkan data tindak kejahatan dan kegagalan keamanan sistem informasi bahwasanya yang memiliki peran penting dalam hal keamanan informasi yaitu pengetahuan para pengguna sistem tersebut, pada dasarnya perkembangan teknologi informasi dan ancaman keamanan sistem informasi tidak dapat terlepas dari ilmu pengetahuan sebagai induk berkembangnya sebuah teknologi.

4.4 Hubungan Fenomena Dengan Perkembangan Pengguna Internet Pasca Revolusi Industri 5.0

Perkembangan pengguna internet di Indonesia berkembang cukup pesat. Berdasarkan laporan informasi dari lembaga riset *Nielsen*, tahun 2021, dan laporan *internet world statistics* Indonesia memiliki catatan meyakinkan untuk penggunaan internet dan teknologi informasi. Hal ini terlihat dari snapshot internet indicator sebagai berikut.



Gambar 4.4 Internet Users di berdasarkan Negara di Dunia (sumber;itg.id)



Gambar 4.5. Grafik posisi Indonesia berdasarkan jumlah penggunaan internet (sumber;itg.id)

Dari gambar 1 dan gambar 2 menunjukkan Indonesia merupakan Negara yang memiliki jumlah pengguna internet di peringkat ke 4 atau Negara yang masuk kedalam 10 besar pengguna internet terbanyak di seluruh dunia, hal ini dipengaruhi oleh kebutuhan masyarakat di Indonesia saat ini, jika dilihat dari segi kewajaran mengapa masyarakat di Indonesia untuk penggunaan

internet dalam beberapa tahun diprediksikan meningkat 12,38% hal tersebut dikarenakan tren perkembangan teknologi, Berdasarkan layanan yang diakses, pengguna terbanyak adalah layanan obile conectin sebesar 125,6% atau sekitar 345.3juta pengguna. Urutan kedua adalah pengguna Social Media sebesar 61,8% atau sekitar 170 juta pengguna. Serta pengguna internet sebesar 73,7% atua sekitar 202,6 juta pengguna.



Gambar 4.6. Grafik Pengelompokan pengguna Internet (sumber, barakata.id)

Peningkatan pengguna internet disebabkan tren perkembangan teknologi dan beragam kebutuhan, jika dilihat dari segi aksiologi peningkatan pengguna internet sangat lah wajar perkembangan teknologi akan berdampak besar terhadap cara mereka memanfaatkan teknologi tersebut berdasarkan kebutuhan dan tren hidup pada eranya.

4.5 Hubungan Fenomena Tdengan Ancaman Keamanan Informasi pasca era Revolusi Industri 5.0

Perkembangan ilmu pengetahuan dan teknologi memiliki tujuan yang sangat mulia yaitu membudahkan orang dalam menjalani kehidupannya. Hal tersebut menjadi sangatlah wajar dikarenakan semua orang menginginkan kemudahan dalam berbagai kebutuhan dalam kehidupannya, seperti dalam bekerja, berbisnis, berbelanja, pendidikan, penelitian, hiburan, infomasi atau kabar berita. Peningkatan transaksi bisnis dan belanja secara online via internet yang sangat tinggi serta energi dan semangat pertumbuhan digital, namun hal tersebut tidak diiringi dengan kesadaran pelaku bisnis dan masyarakat akan risiko dari serangan *cyber*. Sebagai contoh menurut sebuah laporan menunjukan masyarakat Indonesia menempati peringkat pertama sebagai negara paling berisiko mengalami serangan *cyber*.

Salah satu risiko yang terkait dengan pelaksanaan kegiatan internet banking adalah kemungkinan terjadinya tindak pidana dengan menggunakan teknologi internet atau yang lebih dikenal dengan *cybercrime* atau penipuan internet.

Peningkatan tindak pidana melalui penggunaan teknologi internet (*malware*, pencurian identitas, penyalahgunaan internet, *hacking*, dll) menjadi lebih dan lebih umum, hal ini dapat dilihat dalam berbagai kasus serangan *cyber* seperti pencurian dan sinkronisasi token, menunjukkan tren perubahan pola serangan siber, yang sebelumnya menyasar perusahaan dan pemerintah, kini semakin gencar menyasar konsumen secara langsung. Berikut ini grafik 10 negara yang memiliki resiko terhadap serangan IT Security.



Gambar 4.7. Grafik 10 Negara yang memiliki resiko terhadap serangan keamanan IT

Dari grafik tersebut ada hal yang menarik dimana dalam perkembangan pengguna internet Indonesia menduduki peringkat ke 5, namun jika dilihat dari grafik kemungkinan resiko serangan terhadap beberapa Negara didunia Indonesia merupakan Negara teratas yang dianggap sebagai Negara paling beresiko mengalami serangan IT Security, ini disebabkan karena minimnya kesadaran pengguna internet di berbagai Negara terutama Indonesia. Mengapa Indonesia menjadi Negara yang memiliki dampak paling beresiko mengalami serangan? jika dilihat dari nilai kesadaran menurut survey “*Information Week (USE) 2018*” yaitu di beberapa Negara maju dan berkembang bahwasanya tingkat kesadaran pengguna internet dan sistem informasi hanya sebesar 22% yang menganggap keamanan sistem informasi merupakan hal yang penting dan di Negara berkembang kawasan asia hanya sebesar 16,3% tingkat kesadaran keamanan informasi dari pengguna internet yang menganggap keamanan sistem informasi merupakan hal yang penting, dari gambar diatas bisa dilihat 10 negara paling beresiko mengalami serangan hamper seluruhnya adalah Negara yang berada dikawasan asia.

4.6 Saran terhadap arah perkembangan keilmuan keamanan informasi

Saat ini Industri 5.0 keberadaanya sudah hampir menyeluruh diberbagai bidang bahkan pemerintah Indonesia mencanagkan menjadi Negara energi digital Asia (berdasarkan data diri web <https://itgid.org/serangan-cyber-crime-di-indonesia/>) . Industri 5.0 membutuhkan tahapan penelitian yang cukup panjang untuk menghasilkan konsep yang matang dan hasil konkrit untuk diterapkan di suatu Negara yang berkembang harus dapat diperhatikan dari segi aksiologi kebutuhan penggunanya, keamanan dan perlindungan data privasi, sistem keamanan yang selalu *uptodate* terhadap perkembangan siber, pengetahuan pengguna sistem, undang-undang yang berlakuk dinegara tersebut. Pemerintah, ilmuwan dan masyarakat pengguna internet memiliki andil yang cukup besar dalam hal mewujudkan penggunaan teknologi informasi yang aman ,Namun, Sackey (2016) menegaskan bahwa ilmuwan harus mulai membekali diri dengan pengetahuan dan kecakapan (terutama) dalam bidang analisis *big data* dan *human-machine interface*. Mendoza dkk (2016) juga menyarankan hendaknya keilmuan teknologi Informasi dan teknik industri ke depannya harus mampu mengintegrasikan konten rekayasa, sains dan teknologi dengan kemanusiaan. Beberapa hal yang dapat menjadi bentuk peran keilmuan IT yaitu,

1. Berperan ikut membangun platform Industri 5.0 untuk berbagai jenis dan tingkatan industri, terutama industri/usaha kecil menengah.
2. Pengembangan sistem keamanan informasi yang memperhatikan tren perkembangan serangan dan ancaman keamanan informasi.
3. Pengembangan sistem manajemen sumber daya bersama dalam hal efisiensi energi untuk mendukung program mengurangi resiko kerisis energi.

4. Turut serta mengkonstruksi algoritma sistem informasi yang diperlukan dalam penerapan Revolusi Industri 5.0 terutama untuk implementasi sistem keamanan informasi dalam mendukung revolusi industri 5.0.

Mengimplementasikan prinsip *human factor* dan *Security threat* (sebagai contoh dalam mendesain sistem keamanan informasi berdasarkan nilai kebutuhan dan kewajiban pengguna pada era revolusi industri 5.0)

5. Kesimpulan

Ditinjau dari filsafat ilmu, keilmuan teknologi informasi berkembang pesat dengan obyek kajian yang semakin luas akibat munculnya fenomena industri 4.0 atau *cyber physical system* gabungan industri dan teknologi informasi, metode yang semakin kaya dan peran yang semakin besar dalam berbagai bidang, kebutuhan dan tren perkembangan teknologi bagian dari akasiologi yang menyebabkan berkembangnya pengguna internet dan tindakan kejahatan di dunia maya. Perkembangan teknik keamanan dalam melindungi data dan informasi selalu bersinergi dengan disiplin ilmu sains dan ilmu kerakyasaan yang lainnya.

Keilmuan teknologi informasi telah membuktikan peranannya dalam melahirkan fenomena pasca Revolusi Industri 5.0. Terlepas dari segala keuntungan dan kemudahan yang akan diberikan pasca Revolusi Industri 5.0, tetap ada konsekuensi dan dampak negatif yang harus dihadapi. Tidak terkecuali terhadap keilmuan teknologi informasi dan keamanan sistem informasi itu sendiri. Di sinilah tantangan keilmuan dalam bidang IT untuk terus mengkaji dan mengembangkan bidang keilmuannya. Meskipun ada pengaruh dari perubahan zaman dan perkembangan keilmuan yang lainnya, hendaknya ilmu komputer sebagai induk ilmu dari teknologi informasi dan keamanan informasi tetap mempertahankan keunikannya yaitu fokus mengkaji dalam perkembangan dan keefektifan dalam pendistribusian informasi dan transaksi elektronik yang aman yang terintegrasi f pasca Revolusi Industri 5.0. Diharapkan dimasa yang akan datang penerapan teknologi keamanan informasi dengan memperhatikan nilai kewajiban berdasarkan kegunaannya menjadi fokus utama dalam mendukung pasca Revolusi Industri 5.0.

Daftar Pustaka

Jurnal (Time News Rowman 11):

- Annisa Eka Syafrina, Irwansyah, (2018)“Ancaman Privasi Dalam Big Data Privacy Threats In Big Data”, Jurnal Penelitian Komunikasi dan Opini Publik Vol. 22 No. 2, Desember 2018 :132-143
- Budi Raharjo,(2017) “Keamanan Informasi”, PT Insan Infonesia,
- David Kim, Michael G Solomon,(2018) “Fundamentals of Information systems security”, United States of America,
- Erwin, gunadhi H. arranuri. (2015). Pengamanan Basis Data Pengelolaan Hak Akses Dengan Metode Role - Based Access Control. *Algoritma*, 12(1).
- F. Reni and R. Anggraini,(2006) “Pengungkapan Informasi Sosial dan Faktor-Faktor yang Mempengaruhi Pengungkapan Informasi Sosial dalam Laporan Keuangan Tahunan (Studi Empiris pada Perusahaan-Perusahaan yang terdaftar Bursa Efek Jakarta),” Simp. Nas. Akunt. 9 PADANG, vol. 21, pp. 23–26, 2006.
- F. T. Informasi,(2016) “Universitas Bina Darma Filsafat Teknologi Informasi,”.
- Glienmourinsie, D. (2016). Industri Nasional Harus Siap Hadapi Era Industri 4.0. <https://ekbis.sindonews.com/read/1141743/34/industri-nasional-harus-siap-hadapi-era-industri-40-1474630359>, Diakses pada 9 Maret 2017.
- Mendoza, JH., Ramirez, JF., Flore, HS.(2016) Developing and evolution of industrial engineering and its paper in education. *Ingeniería Y Competitividad*, Vol. 18, No. 2, pp. 89 – 100.
- Michael E. Whitman, Herbert J. Mattord.(2011) “Principles of Information Security”. Cengage Learning,.
- Kunjojo, (2009)“Filsafat Ilmu”, Kediri-Indonesia,
- Okasha, Samir.(2002.) *Philosophy of Science a Very Short Introduction*. New York:



Oxford University Press.

Permadi, A. F., Raharjo, D. S., & Christyowidiasmoro. (2013). Keamanan Jaringan pada IPTV. *Jurnal Teknik POMITS*.

Suaedi Fachruddin,(2016) “Penagantar Filsafat Ilmu”, Bogor-Indonesia,

Sackey, SM., Bester, A.(2016) Industrial Engineering Curriculum in Industry 4.0 in A South African Context. *South African Journal of Industrial Engineering*, Vol. 27, No. 4, pp. 101-114..

Zamroni, Mohammad,(2009) “Filsafat komunikasi: pengantar ontologis, epistemologis, aksiologis”, Yogyakarta: Graha Ilmu,

Welhendri Azwar Muliono,(2018) “Filsafat Ilmu Cara mudah memahami Filsafat Ilmu”, Padang-Indonesia,

<https://bssn.go.id/peringatan-indikasi-peningkatan-aksi-peretasan-sistem-elektronik-di-indonesia/> Diakses 12 November 2021

<https://itgid.org/serangan-cyber-crime-di-indonesia/>

<http://isparmo.web.id/2018/08/01/data-statistik-pengguna-internet-di-indonesia-2017-berdasarkan-survey-ap.>

<https://www.nielsen.com/id/en/press-releases/2017/tren-baru-di-kalangan-pengguna-internet-di-indonesia/>.