Jurnal Diplomasi Pertahanan,
Volume 7,Number 1, 2021 E-ISSN : 2746-8496

Keamanan dan Ancaman Cyber Bagi Sektor Privat dan Industry Militer Di Era 4.0

(*Security and Cyber Threats for the Private Sector and Military Industry in the Era 4.0*)

Krisna Surya Narindra

Kepala Sub-Bagian Evaluasi Mutu Diklat Pusdiklat Bahasa Badiklat Kemhan

k.narindra2001@gmail.com

Abstract

The development of the internet and digital technology is a representation of the 4.0 revolution. The industrial revolution 4.0 shifts the role of humans and industrial machines which characterized the Industrial Revolution that occurred before. The economic policies of these countries to colonialization by Western European countries such as Britain, France and Germany and the United States were also the effects of the industrial revolution. Oil, metals, textiles supporting factories in the industrial revolution 1.0 to 3.0 the entry of these countries to invade, exploring countries that are rich in natural resource potential.

Keyword : Keamanan siber, revolusi industry, ancaman dan keamanan siber, Artificial Inteligent

1. Pendahuluan

Perkembangan teknologi komputer bergeraak lebih cepat dari pada perkembangan sektor ekonomi. Tiga perempat dari semua komputer digunakan di sektor jasa seperti keuangan dan kesehatan. Peningkatan produktivitas di sektor Iinformasi dan teknologi ditandai munculnya komunikasi massal dan memberikan beberapa pelajaran tentang kemungkinan efek sosial dan politik hari ini yang mengantar era budaya populer massal.

Manusia dalam era digital saat memiliki ketergantungan terhadap perangkat digital, yang praktis dan massif adalah berupa menyampaian layanan pengirim berbasis teks , audio dan video yang terintegrasi dalam sebuah aplikasi. Ketergantungan ini membuka celah baru mengenai keamanan cyber baik secara individu maupun secara organisasi maupun entitas di sebuah negara (Maharsi,2000)

Di dunia sering terjadi peretasan terhadap sejumlah situs-stus yang tercatat memiliki keamanan cyber yang mumpuni, di Indonesia pun pernah terjadi peretasan-peretasan pada sejumlah organisasi pemerintahan maupun media massa. Situs-situs yang dibekali keamanan imasih saja tembus oleh para peretas dengan berbagai motivasi antara seperti motivasi politik yang tidak puas terhadap kebijakan pemerintah. Namun ada juga yang meretas sebuah situs dengan motivasi ekonomi seperti yang menyerang perusahaan untuk menuntut sejumlah uang dalam bentuk *bit coin*.

Indonesia dalam kemajuan dunia digital sebatas penonton dan penikmat saja. Partisipasi sebagai kreator aplikasi juga sangat terbatas. Salah satu masalah paling mendesak dalam hubungan internasional kontemporer adalah ekspektasi era baru persaingan strategis yang semakin intensif, yang ditandai dengan pertemuan persaingan politik, ekonomi, dan militer-teknologi dalam konteks pergeseran besar dalam lingkungan keamanan global. Garis depan persaingan strategis yang berkembang ini adalah persaingan untuk supremasi masa depan atas keamanan global dan jaringan kelembagaan ekonomi antara kekuatan militer utama dunia Amerika Serikat, China, dan pada tingkat yang lebih rendah, Rusia. Di Kawasan Asia, kemajuan teknologi masih untuk sementara dikuasai Korea Selatan dan China serat Kedua negara ini bahkan menjadi ancaman Amerika Serikat dalam dunia industry teknologi informasi dan militer. (Raska, 2020)

Produk digital untuk konsumsi public yang di buat China dan Korea Selatan begitu leluasa dan mendikte selera pasar di dalam indusri tehnologi komunikasi. Korea Selatan dan utamanya China bahkan telah mampu membuat sebuah produk pembayaran digital di Indonesia dan teknologi *finger print* yang disematkan dalam gadget terkininya. Kompetisi harga produk China bahkan dapat mematikan produk domestic Indonesia

jika penduduk Indonesia beralih dan mengunakan produk jual beli online. Kompetisi harga yang ditawarkan kompetitor China relative lebih murah dibanding produk dalam negeri untuk barang yang sejenis. Sehingga pada akhirnya pemerintah Indonesia melakukan dan menerapkan pajak barang yang dibeli secara online untuk melindungi produk–produk Indonesia.

Dalam konteks perdagangan regional, Indonesia harus segera mencanangkan kemandirian bangsa untuk mengimbangi dominasi Korea Selatan dan China. Kemajuan China diberbagai sector seperti tak terukur dan selalu memunculkan inovasi-inovasi produk secara cepat, massif dan harga yang kompetitif. Keamanan dan stabilitas politik China juga mendukung proses produksi sector barang dan jasa. Pemerintah Indonesia harus banyak membenahi kestabilan politik dan beragam kegaduhan vertical dan horizontal dalam negerinya. Di mata para pemimpin China, itu adalah teknologi yang menjadi inti dari kejayaan, kemunduran, dan kebangkitan China.

Pada Abad Pertengahan, China berada dalam peradaban yang sangat maju kala itu di bidang, kompas, bubuk, kertas. Namun ketika batu bara, mesin uap, pabrik, dan listrik telah ditemukan pergeseran teknologi yang menyebabkan kemerosotan kekuatan ekonomi China, dan kemudian kekalahan militer dihampir semua kekaisaran China (Vitori, 2019)

2. Tinjauan Pustaka

Keamanan siber dan kaitan dengan politik keamanan. Jauh dari memberikan jawaban langsung, pertanyaan membuka ruang perdebatan politik dan akademis tentang masalah tersebut. Pertama, keamanan cyber adalah praktik konvensional seputar keamanan jaringan komputer

Kedua, pada kalangan terbatas ahli membahas keamanan dunia maya terutama sebagai masalah manajemen risiko teknis dalam informasi penting perlindungan infrastruktur. Pemerintah dan sector privat dan industri saat ini harus berurusan dengan dunia maya sebagai lapis pertama tantangan utama keamanan nasional. Ketiga, berbanding lurus digitalisasi yang semakin maju dari lebih banyak aspek ekonomi, masyarakat,dan politik, masalah keamanan dunia maya meluas ke kebijakan perluasan

domain. Keamanan dunia maya ada disaat yang sama bergerak ke atas dalam agenda politik dan berkembang ke samping sebagai area masalah bagi banyak individu dan korporasi.

Dunia militer erat kaitannya dengan teknologi digital, sejak pertam kali ditemukannya bubuk mesiu perkembangan teknologi militer seakan tidak pernah berhenti dari rangakain inovasi baik yang berupa hardware maupun software. Keunggulan teknologi militer membuat negara-negara produsen alutsista seperti Amerika Serikat, China dan Rusia dan disusul Korea Selatan menjadi incaran bagi negara-negara non produsen untuk berlomba-lomba memperkuat strategi pertahanannya.

Perang telah memberikan bukti bahwa, teknologi memainkan peran yang penting, misalnya pada perang di era Uni Sovyet dan Amerika Serikat, Sovyet melakukan inovasi yang menakjubakan saat itu dengan mengirim manusia pertama ke luar angkasa dan Amerika Serikat bereaksi dengan mengirim manusia pertama ke bulan delapan tahun kemudian.

3. Metode Penulisan

Penulis menggunakan analisis teks terhadap artikel yang mengangkat tema siber, perkembangan teknologi khskeamanan siber dan ancamannya, serta fenomena-fenomena kejahatan siber yang dialami oleh pribadi maupun oleh industry public maupun militer. Artikel-artikel tersebut dianalisa untuk mendapatkan masalah-masalah dan kemungkinan solusi yang bisa diambil dengan cepat maupun solusi yang bersifat jangka Panjang dan strategis

4. Hasil dan Diskusi

4.1. Revolusi Industri 1.0, 2.0, 3.0

Revolusi industri 1.0 bercirikan produksi mekanis seperti penambangan batu bara dan penggunaan mesin uap. Tenaga manusia banyak terganti dengan adanya sector-sektor industry berbasis tenaga batu bara. Sehingga target produksi lebih efisien

disbanding dengan tenaga manusia. Akibatnya kebijakan Negara pada saat itu adalah memperkuat industri dan memperkaya stok batu bara sebagai cadangan strategis negaranya. Inggris dan Negara Eropa Barat mulai melirik Negara lain yang kaya sumber daya alam dan melakukan ekspansi dan invasi mereka.

Revolusi industri 2.0 bercirikan penggunaan minyak dan listrik sebagai penggerak alat produksi Pabrik-pabrik otomotif mulai bangkit, Negara Eropa benar-benar mulai bangkit tanpa terhalang oleh hambatan dalam bentuk penjajahan sehingga mereka dapat melanjutkan pembangunan yang dmuai pada era industry 1.0. Berbeda dengan bangsa Asia yang justru pad saat itu kaya dengan sumber daya alam namun masih sibuk dengan kebebasan dan kemerdekaan negerinya. Kebijakan luar negeri Negara-negar industry benar-benar terkonsentrasi untuk

Revolusi industri 3.0 ditandai dengan munculnya kegiatan produksi berbasis elektronik dan teknologi komputer. Tenaga manusia terbantu berkat penemuan mesin dan sangat mendukung produksi dalam volume besar. Selain itu para pemimpin besar negar-negara Eropa, terutama Eropa Barat semakin gencar memperluas kekuasan kolonialisme nya, Afrika dikuasai oleh Inggris dan Prancis karena tergiur oleh sumber daya alam yang mereka miliki. Sementara Amerika Selatan hamper semua dikuasai oleh Spanyol dan sebagian kecil oleh Portugal. Era 3.0 merupakan era transisional yang merupakan pertemuan antara era 2.0 yang sedikit "kuno" dan merupakan fondasi teknologi di era 4.0. Dominasi Amerika Serikat dan Eropa Barat masih mewarnai persaingan di era 3.0. Namun, ketergantungan terhadap minyak mash sangat besar dan tidak bisa lepas begitu saja di era ini. Pembicaraan mengenai ancaman ekologi juga mulai dipikirkan oleh actor negar dalam membuat kebijakan, tentu saja kebijakan yang diambil selalu saja berpihak kepada kepentingan untuk meindungi perekonomian domestic mereka.

4.2. Periodisasi Revolusi Industri 4.0

Revolusi industri 4.0 transformasi digital. Revolusi ini sebagian besar dilakukan dengan pengkodean dan algoritma. Industri 4.0 dikaitkan Internet dan jaringan siber. Di

era 90 an teknologi computer melakukan revolusi di bidang aplikasi berbasis DOS, pengolah kata dan data, Word, Lotus dan D Base, namun aplikasi ini belum terintegrasi dan menjadi bagian yang terpisah, sebuah langkah yang praktis dalam membantu pekerjaan. Menjelang tahun 2000 Microsoft Office membuat inovasi yang hasilnya bias dirasakan hingga saat dan belum tergoyahkan meskipun pernah mendapatkan sainga dari sebuah pengolah data dan kata yang berifat open source.

China belum mampu menggeser dominasi Microsoft Office dalam hal aplikasi layanan pengolah data dan kata yang tentu saja menjadi pundi-pundi dollar bagi penguasa Microsoft Corporation. China bergerak dibidang lain seperti menggunakan IT sebagai sarana jual beli produk mereka dan membuat sistem pembayaran online yang tentunya Indonesia menjadi pangsa pasar produk mereka dengan memanfaat kan jumlah penduduk Indonesia yang sangat besar. Sehingga bias dikatakan transformasi digital sebagai prioritas strategis.

Namun China menjadi saat ini masih memimpin dalam sektor jual beli barang melalui penyedia barang terbesar di situs jual beli online. China menawarkan hamper semua barang yang dibutuhkan oleh Indonesia, dengan harga yang kompetitif bahkan lebih murah dalam pembelian kuantitas yang lebih besar. Sehingga Indonesia, dalak hal ini Ditjen Pajak harus membuat regulasi penerapan pajak bagi barang-barang yang dibeli dari China tersebut guna melindungi industry domestic Indonesia.

4.3 Ancaman kemanan siber sebagai Artificial Inteligent

Articial Inteligent (AI beryjuan untuk menduplikasi kecerdasan yang dimiliki oleh manusia dan membangun sistem cerdas. AI juga melibatkan banyak subdisiplin saat ini. Kesulitan dalam kursus pengantar AI terletak pada penyampaian cabang sebanyak mungkin tanpa kehilangan terlalu banyak kedalaman dan presisi**. (Wolfgang, 2016).** Adopsi dan akselerasi pada tiga dekade terakhir beserta cara teknologi dalam ikut mengubah kehidupan dan lingkungan bukanlah fenomena baru kemajuan dalam biologi, fisika elektronika dan adopsi massal komputer pribadi**.** (Skilton, 2016).

Penggunaan internet berkembang dan mempermudah urusan manusia dari sebatas pengolah kata maupun pengolah data. Pengolahan data pribadi dalam sebuah data base merupakan efek dari berkembangnya internet public menjadi sebuah ancaman tersendiri. Fakta-fakta actual mengungkapkan pencurian data-data pribadi yang dilakaukan pula oleh kemajuan teknologi internet baik menggunakan digital maupun dengan pencurian data yang dilakukan oleh internal.

Kejahatan peratasan email di tengah pandemic Covid 19 juga menyerang perusahaan penyedia ventilator corona dari Italia dan China oleh warga negara Indonesia yang menyebabkan kerugian 58 miliar. Keamanan email juga mengharuskan pengguna pribadi harus membuat beberapa layer keamanan pribadi. Keamanan secara privat bias dilakukan dengan kewaspadaan pada system password dan update kombinasi password, serta dengan tidak mengklik link-link yang disebar sebagai spam yang dikirim dengan menyebutnya sebagi link give away (hadiah). Keamanan sederhana yang bisa dilakukan oleh individu diantaranya adalah dengan melakukan pemeriksaan keamanan akun email secara rutin menambahkan nomor ponsel dan alamat email pemulihan akun, serta mengaktifkan verifikasi dua langkah (two step verification). Selain itu diyakini dengam pembuat kata sandi yang rumit namun dapat diingat dengan baik dan tidak membagikan akun kepada pihak lain. Pihak privat juga wajib memeriksa device yang terhubung dengan layanan ponsel agar tidak terjadi pencurian data pada setting keamanan dan memastikan penggunaan browsing untuk tidak memilih penyimpanan data dalam computer pribadi maupun public. Kewaspadaan individu masih menjadi kunci utama bagi keamanan data Individu di Indonesia, dan belum ada satupun korporasi dan insitusi resmi negara yang menjamin keselamatan data individu.

Penggunaan digital money maupun jasa kredit online juga mengharuskan privat, korporasi dan negara membuat system keamanan berlapis Dilaporkan 800 ribu lebih data nasabah Kredit Plus bocor di sebuah forum internet. Data pribadi menjadi peluang bisnis bagi kejahatan di era 4.0 dan peluang bisini bagi sector jasa keamanan siber. Kasus yang keamanan data pribadi masih sangat jarang diketahui oleh awam, tanpa banyak orang menyadari ancaman data bahkan dana sering dating tidak hanya oleh pihak ekternal

sebuah korporasi, namun sering kali melibatkan pihak internal perbankan. Contoh kasus adalah pengurangan nominal rekening yang jumlahnya sangat kecil yang dibebankan pada sekian juta nasabah bank tertentu perhari. Hal ini tidak akan menimbulakn kecurigaan terhadap nasabah tersebut, namun secara akumulatif keuntungan yang didapat dari modus ini jumlahnya sangat besar.

Keamanan privat data transaksi online situs jual beli juga mencatat angka fantastis dalam jumlah pencurian data konsumen, setidaknya link tautan untuk mengunduh data Tokopedia sebanyak 91 juta secara bebas. Hal ini menjadi sebuah catatan bagi individu, korporasi dan negara bahwa keamanan data pribadi tak lagi bersifat privat. Negara harus benar-benar membuat sebuah system jaringan yang kuat dan bila perlu mengubah kembali system kodifikasi dalam NIK. Pencurian data harus segera diwaspadai sebagai ancaman nasional karena dari data-data tersebut mampu memunculkan kejahatan Informasi dan Teknologi baru seperti pemalsuan data perbankan guna melakukan transfer kepada nasabah fiktif untuk kepentingan pencucian uang.

Keamanan sector korporasi dalam bidang Informasi dan Teknologi dapat dibedakan menjadi dua sector yaitu korporasi BUMN dan korporasi swasta. Tanpa melakukan dikotomi kedua jenis korporasi tersebut, kedua jenis korporasi tersebut terutama yang menggunakan data pribadi harus memiliki skema keamanan siber yang jelas. Sektor keamanan siber negara menjadi ranah Badan SIber dan Sandi Negra (BSSN), Lembaga ini tidak bekerja pada ranah perlindungan data pribadi karena tugas pokok dan fungsinya. Kemenkominfo menjadi leading sector pengamanan informasi dan menciptakan regulasi yang dapat mengamankan transaksi finansial dan data pribadi pelanggan. Regulasi tersebut dikembangkan secara terintegrasi.

Ranah keamanan siber dimulai dari negara dengan mengembangkan industry teknologi yang mandiri baik berupa hardware mulai dari perangkat satelit mandiri yang benar-benar diproduksi oleh Indonesia, perangkat lunak berupa software, operating system mandiri, Bahasa pemrograman mandiri dan didukung oleh brain ware sebagi pengawak keamanan siber negara yang harus memiliki integritas tinggi dalam melindungi negara, korporasi dan sector privat.

Ketergantungan terhadap produk hardware dan software buatan luar negeri dalam dunia IT memiliki nilai kepraktisan, namun harus disadari juga bahwa vendor produk tersebut tidak serta merta menjual produk aplikasi tanpa menyertakan bug dalam programnya yang bertujuan melindungi kepetingan nasionalnya. Dalam posisi perang non militer yang bersifat perang tehnologi peluang mematikan seluruh komponen jaringan computer yang ada di Indonesia sangat besar. Kendali satelit yang menggerakan sector komunikasi, sector perbankan dalam keadaan perang teknologi bisa dilumpuhkan jika masiih bergantung pada produk luar negeri. Dampaknya akan sangat merugikan Indonesia, kejadian yang pernah terjadi adalah ketika Indonesia mengalami kerusakan pada jaringan distribusi listrik dimana Indonesia tidak memiliki contingency palnning menghadapi kasus yang diklaim sebagi force majeure.

Keamanan korporasi yang rentan terhadap serangan siber sejauh ini masih pada sector perbankan adalah kejahatan skimming. Kejahatan ini sebenarnya termasuk kejahatan perbankan yang tergolong tradisional dimana pelakunya masih menggunakan duplikasi kartu ATM dan mengecoh calon korbannya. Kejahatan yang menyerang korporasi adalah pembekuan situs korporasi yang dilakukan oleh *hacker* tujuannya adalah untuk meminta tebusan sejumlah uang digital, serangan ini lebih dikenal dengan Ransomware. Kasus Ransomware terakhir kali menyerah perusahaan yang justru terkenal dengan system keamanannya, yaitu Garmin. Perusahaan ini sempat diambil alih hampir satu minggu meskipun dalam situs resminya perusahaan ini menyatakan bahwa perusahaan sedang melakukan perbaikan system.

Ancaman siber korporasi di Indonesia memerlukan kolaborasi pengampu kebijakan Informasi dan Teknologi, artinya setiap korporasi harus menggandeng penyedia jasa keamanan siber dibawah naungan pemerintah. Sehingga negara, mampu melakukan pembangunan keamanan siber yang dibutukan korporasi dan mewujudkan keamanan tersebut secara berkesinambungan yang dituangka dalam regulasi dan blue print keamanan siber jangka Panjang.

4.3 Ancaman dan keamanan multi layer bagi industry militer.

Saat ini istilah *Defense in Depth (DiD)* mulai dikenal, dimana *Defense in Depth (DiD)* ini merupakan sebuah pendekatan keamanan siber yang melakukan serangkaian mekanisme pertahanan berlapis untuk melindungi data dan informasi yang berharga. Pada pola ini apabila satu mekanisme gagal untuk membendung sebuah serangan siber pada sebuah instansi, maka diharapkan layer atau lapis berikutnya dapat mulai bertindak untuk menggagalkan serangan dengan rangkaian kegiatan yang lebih efektif.

Pendekatan multi-layer atau pendekatan berlapis-lapis dibentuk dengan keamanan sistem secara keseluruhan dan menangani banyak vektor serangan yang berbeda. Defense in Depth digambarkan atau diilustrasikan sebagai “pendekatan benteng" karena cara kerjanya yang melakukan pertahanan berlapis dari sebuah banteng pada masal lalu di Eropa.

Sebelum musuh dapat menyerang obyek keamanan vital sebuah negara maka musuh siber ini terlebih dahulu dihadapkan pada layer-layer keamanan pada level awal, menegah dan level akhir. Dunia militer yang erat kaitannya dengan penggunaan tehnologi digital tidak saja diuntungkan denga kemajuan digital tersebut namun juga menghadapi sebuah celah potensial untuk diserang, dan pada saat ini terdapat begitu banyak penyerang potensial, dan negara harsu menjamin bahwa negara telah memiliki keamanan yang tepat untuk mencegah sistem dan jaringan disusupi. Namun perlu disadari bahwa tidak ada metode tunggal yang berhasil melindungi dari setiap jenis serangan. Penjelasan tersebut membuat negara harus memiliki road map dan pembangunan arsitektur pertahanan mendalam (Defense in Depth)

Pendekatan berlapis untuk keamanan dapat diterapkan ke semua tingkat sistem TI karena tidak ada sebuah negara yang dapat sepenuhnya dilindungi oleh satu lapisan keamanan. Sistem keamanan yang digunakan peretas adalah mencari celah keamanan siber yang ada, karena penguatan di sebuah layer keamanan akan memungkinkan seuah celah keamanan di lapis yang lain mesipun pada system keamanan telah dilengkapi dengan firewall, pemindai malware, sistem deteksi intrusi, enkripsi data, dan solusi audit

integritas, namun semua itu masih bisa diretas jika terdapat sebuah celah kecil pada system keamanan.

Elemen pertahanan mendalam *Defense in Depth (DiD)* diperlukan dalam dunia militer dan harus terus berinovasi dalam mengembangkan teknologinya misalnya adalah dengan melakukan Kontrol Keamanan Jaringan seperti analisis lalu lintas jaringan. Firewall mencegah akses ke dan dari jaringan yang tidak sah dan akan mengizinkan atau memblokir lalu lintas berdasarkan sekumpulan aturan keamanan. Sistem perlindungan intrusi sering kali bekerja bersama-sama dengan firewall untuk mengidentifikasi potensi ancaman keamanan dan meresponsnya dengan cepat.

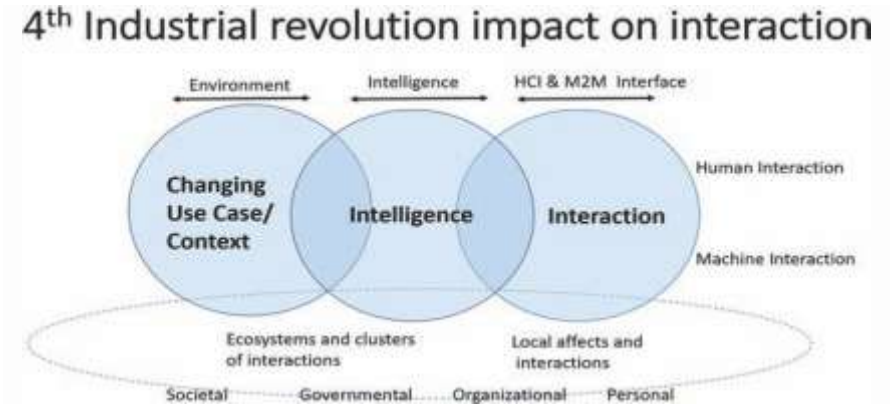
Amerika Serikat yang dikenal dengan system keamanan pertahanan yang sangat canggih juga masih dapat ditembus oleh para peretas yang bermuatan politis, sebagaimana yang terjadi pada kasus peretasan situs Trumps yang berisi mengenai informasi palsu dari *Federal Bureau of Investigation* (Porter, 2020) yang menyatakan sebuah informasi yang mengklaim memiliki bukti bahwa pemerintah Trump terlibat dalam asal mula virus korona, dan bahwa presiden telah terlibat dengan "aktor asing yang memanipulasi pemilu 2020.

4.4. Persaingan Teknologi Militer dan kebangkitan Arificial Inteligent di era 4.0.

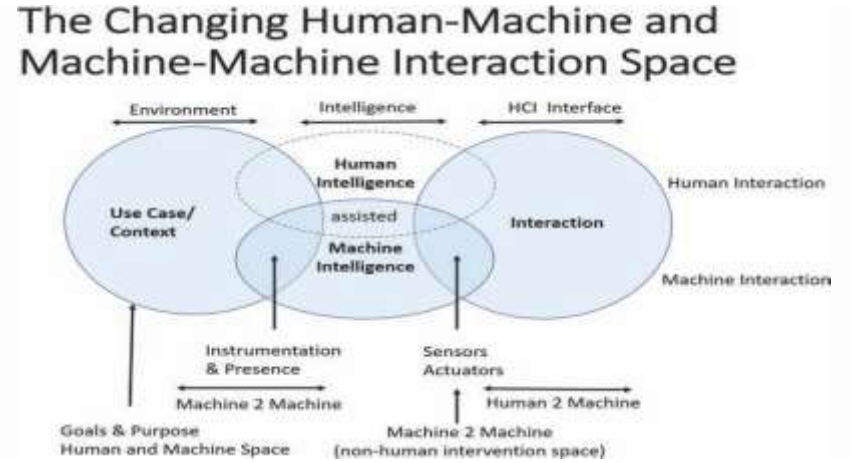
Revolusi digital membawa evolusi sistem yang sangat, persenjataan militer dan perencanaan militer mengalami perubahan besar yang merevolusi konsepsi perang dan pertahanan. Persaingan strategis telah lama ada dari abad 5 SM hingga perpecahan Uni Soviet dan Amerika Serikat dalam Perang Dingin selama paruh kedua abad ke-20. Amerika Serikat hanya berfokus pada memaksimalkan pada menekan Uni Soviet pada ranah politik, ekonomi, ideologis, dan militer. Ketika revolusi industry 4.o hadir dan menciptakan teknologi Arificial Inteligent atau kecerdasan buatan (Artificial Iinteligent) membuat perubahan yang signifikan yang dampaknya dapat dirasakan oleh masyarakat umum. merupakan sebuah manipulasi fisik baru dalam ilmu material dalam nanoteknologi, manipulasi tidak hanya berkembang pada perekaman pembacaan struktur wajah semata namun juga pada hal yang bersifat biologis dalam bioteknologi

gen, bedah robotik, prostetik, dan perangkat yang dapat dikenakan semuanya memiliki asal-usul yang dapat ditelusuri kembali melalui beberapa langkah evolusi (Skilton, 2016).

Interaksi sosial dan sosial kini menyatu dalam media sosial dan domain yang terhubung dengan telekomunikasi yang dapat menjangkau, dan dampak negatifnya dapat memecah komunitas sosial dan ekonomi Cloud Sistym atau Big Data generasi informatika dari domain digital, fisik, dan bio-logis memunculkan bentuk-bentuk informasi dan kecerdasan baru tentang lingkungan makro dan mikro tersebut pada tingkat yang otentik. Inilah ciri prinsip dari era industri ke-4 yang berbeda dengan era-era sebelumnya. Hal ini dapat dilihat proses perubahan social yang diakibatkan oleh adanya penemuan Articial Inteligent. (Skilton 2016)



Meskipun demikian perkembangan Teknologi akan mengubah pola interaksi antara produk digital (machine), yang saat ini pola interkasi terjadi antara manusia dan gawai (gadget) menjadi mesin/gawai/produk digital ke mesin/gawai/produk.



Kemanjuan teknologi militer berbasis internet menurut Thomas A. Johnson (2018) diantaranya meiputi Cyberspace, Cyber Battle Space Offensive Operations Defensive Operations Intelligence and Counter Intelligence Cyberspace and Cyber Intelligence New Drone Wars. Amerika Serikat yang meiliki hampi kesemuanya itu masih juga menghadapi serangkaian tantangan keamanan saat ini dan jangka panjang di berbagai wilayah geografis, terlebih saat ini hubungan China-AS lebih kompleks dalam hal mengintegrasikan berbagai pendorong kerja sama, persaingan, dan konflik secara bersamaan termasuk di dalam nya persaingan perangkat berbasi internet dan peralatan berbasis teknologi internet dan peaswat tanpa awak.

Dengan kata lain, pola global dari persaingan strategis di abad ke-21 lebih kompleks, tidak dapat diprediksi, dan beragam, yang mencerminkan berbagai kompetisi di bawah perangkat aturan yang berbeda atau tumpang tindih, hingga persaingan politik-militer-teknologi yang tajam untuk mendapatkan kekuasaan dan status. Amerika Serikat melihat perkembanga teknologi industry militer China dan Rusia akan memiliki kemampuan yang diperlukan untuk memproyeksikan kekuatan di Indo-Pasifik setara dengan Amerika Serikat. China, Rusia, dan Amerika Serikat berusaha untuk mencapai atau memperpanjang margin keunggulan teknologi militer mereka dalam persaingan strategis untuk teknologi canggih yang muncul seperti kecerdasan buatan (*Artificial Inteligent*), robotika, manufaktur aditif. Teknologi digital yang muncul seperti *Defense in Depth (DiD)* secara luas dianggap sebagai elemen penting dari efektivitas dan keuntungan militer di masa depan. *Artificial Inteligent* merupakan sebuah jalan menuju sistem senjata otonom dimana peralatan tempur, mesin, dan perangkat lunak dapat melakukan tugas tanpa campur tangan manusia. Sistem otonom adalah sebuah rancangan mesin yang dapat berjalan secara otomatis.

Kemampuan negara dalam penguasaan teknologi militer yang mutakhir akan berbanding lurus dengan sistem persenjataan yang lebih efektif, yang membawa dampak pada pembangunan kekuatan militer yang lebih besar, sehingga dampak menyusun kekuatan geopolitik yang lebih besar pula. Penemuan teknologi baru yang belum pernah ada sebelumnya dalam hal kecepatan pemrosesan informasi, otomatisasi untuk platform senjata dan sistem pengawasan, serta pengambilan keputusan daya tembak yang lebih presisi.

Kemajuan teknologi dalam dunia militer yang dapat dikembangkan adalah pengunaan *Artificial Inteligent* yang dapat menganalisa secara real-time serangan siber canggih dan deteksi citra penipuan hingga mengarahkan platform otonom seperti drone, hingga bentuk komando dan kontrol baru seperti sistem manajemen pertempuran otomatis yang menganalisis data besar dan memberikan rekomendasi untuk tindakan manusia.

Teknologi *Artificial Inteligent* dapat dikembangkan sebagai teknologi pertahanan strategis, seperti peringatan dini, pertahanan rudal dan pencegahan nuklir dan kecerdasan buatan bisa dikembangkan sebagai aplikasi dalam system informasi dan sistem komando strategis (Command and Control) komunikasi, navigasi, intelijen dan pengawasan serta dalam seluruh area kemampuan pertahanan dan serangan siber. *Artificial Inteligent* akan memiliki implikasi yang mendalam tentang bagaimana militer mengadopsi teknologi baru; bagaimana pada tingkat operasional, militer beradaptasi dan menerapkan teknologi baru, dan pemahaman kita tentang ruang pertempuran di masa depan yang mengedepankan kemajuan teknologi dan informasi. Evolusi dinamis yang menjadikan perangkat lunak akan semakin mampu menghasilkan program komputer secara otomatis yang membuat kecerdasan buatan mungkin bisa mencapai dan bahkan melebihi kinerja kognitif otak manusia. Namun, teknologi dan kemampuan yang dihasilkan jarang menyebar secara merata di seluruh garis geopolitik.

China, Rusia, dan Amerika Serikat, dan Korea Selatan saat in masih mendominasi penguasaan berbasis *Artificial Inteligent* kemajuan teknologi industri, informasi dan digital ternyata relevan dengan teknologi militernya dan akan menjadi semakin sulit

untuk diidentifikasi dan diklasifikasikan bagi negara lainnya. Kemajuan teknologi, terutama di bidang sistem militer, merupakan proses yang dinamis dan berkelanjutan, inovasi dan dampak terhadap efektivitas militer dan keunggulan komparatif bisa jadi signifikan dan sulit diprediksi pada tahap permulaannya. Teknologi canggih banyak digunakan pada sektor komersial, dan hal ini mendorong kemajuan pada sektor industri militer, menawarkan peluang baru dan berpotensi signifikan untuk aplikasi pertahanan guna meningkatkan keunggulan militer kepada negara lain. Kini teknologi militer hadir pada era "Revolusi Industri Keempat" (4IR *Four Industrial Revolution*) di bidang-bidang yang dapat dilihat pada kehadiran-kehadiran teknologi China, Amerika Serikat, Rusia dan Korea Selatan.

Perception, Processing, Cognition	Performance and Materials	Communication, Navigation and Targeting
• Cloud Computing	• Quantum Computing	• Precision Position, Navigation and Timing
• Big Data Analytics	• Autonomy	• Directed Energy
• Artificial Intelligence	• Novel / Smart / BioMaterials	• Electro-Magnetic Weapons
• Cyber capabilities	• Meta-technologies	• Cyber Capabilities
• Virtual and Augmented Reality	• Composites for Aerospace	• Unmanned Systems
• Robotics / Unmanned Systems	• Internet of things	• Hypersonics
• Advanced Sensors	• Energy capture and storage	• Optical satellite links
• Internet of things		• Visible light communication

Kemajuan teknologi digital militer yang tidak merata secara alami memengaruhi bagaimana teknologi dan kemampuan ini dapat memengaruhi keamanan dan stabilitas kawasan. Bagaimana dengan negara yang belum memilikipersenjataan dengan teknologi yang kuat? Pilihannya adalah dengan melakukan aliansi dengan melakukan hubungan melalui berbagi teknologi dan keharusan interoperabilitas, sementara konsep strategis tradisional seperti pencegahan dapat diuji melalui munculnya berbagai jenis konflik yang dibawa oleh teknologi baru. Negara harus memapu menilai kemampuan relatif militer regional untuk mengakses dan memanfaatkan teknologi kritis baru dan yang muncul, kemungkinan kemajuan mereka dalam melakukannya, dan hambatan yang

mungkin mereka hadapi, pada akhirnya dengan memperhatikan bagaimana hal itu akan mempengaruhi keuntungan dan kerugian dalam kemampuan militer regional.

Persaingan strategis yang berkembang dan persaingan untuk supremasi masa depan antara Amerika Serikat, Rusia, dan China membentuk perspektif yang berbeda terhadap terobosan teknologi. Diperlukan sebuah konsep kerangka kerja komparatif untuk inovasi pertahanan yang mengintegrasikan berbagai tahapan, jalur, dan pola. Pertama-tama, mengkonseptualisasikan teknologi yang muncul ke dalam kemampuan militer melibatkan proses internal inovasi militer serta proses pembandingan eksternal adaptasi atau persaingan. Inovasi militer yang mengganggu mungkin tidak selalu membutuhkan terobosan teknologi, doktrinal, dan organisasi secara simultan, tetapi dapat menjangkau spektrum. antara modernisasi inkremental dan transformasi terputus-putus. Berdasarkan asumsi ini, seseorang dapat melakukan triangulasi lintasan inovasi pertahanan di sepanjang tiga komponen yaitu: jalur konseptual yang meliputi persaingan, adaptasi, dan inovasi, kemdian pola teknologi seperti spekulasi, eksperimen, dan implementasi serta perubahan organisasi, eksplorasi, modernisasi dan transformasi.

Badan Siber dan Sandi Negara (BSSN) merupakan Lembaga yang perlu menilik 4 kekuatan besar penguasaan tekonologi digital dan teknologi informasi. Indoensia Pada abad ke-21, China, Rusia, Amerika Serikat dan Korea Selatan saat ini masih dalam tahap pengembangan, akuisisi, penyebaran, dan penerapan teknologi baru sebagai sarana untuk menciptakan keuntungan dan memengaruhi actor-aktor negara atau pilihan strategis pesaing mereka

Terdapat ada empat strategi bersaing yang berbeda tetapi saling mendukung: (1) strategi penolakan; (2) strategi pembebanan biaya; (3) menyerang strategi pesaing; dan (4) menyerang sistem politik pesaing. Strategi penolakan berusaha untuk mencegah lawan mencapai tujuan politik dengan menunjukkan kemampuan teknologi militer, strategi yang membebankan biaya yan, bertujuan untuk meyakinkan pesaing bahwa biaya tersebut sangat murah, pendekatan ketiga, menyerang strategi pesaing, berusaha mempersempit opsi strategis pesaing menjadi perilaku yang dapat merugikan diri

sendiri. Strategi yang menyerang sistem politik pesaing berusaha mengeksploitasi faksi subversif dalam sistem itu.

Teknologi digital baru akan juga masuk ke bidang militer dan kebijakan keamanan.

4.5. Negara sebagai dalam menghadapi ancaman dan tantangan keamanan siber.

Dalam melindungi dafri ancaman siber Indonesia memiliki Strategi Keamanan Siber Nasional (SKSN) yang meiliki tugas seperti : Melindungi jaringan infrastruktur Strategis Pemerintah, Data Nasional, Data Pribadi, Data Penduduk, dan Data Industri , Memajukan dan Menum- buhkan Ekonomi Digital, Meningkatk an Daya Saing dan Inovasi siber, Mencerdaskan dan Membangun karakter SDMBangsa Indonesia dalam ruang siber. (Asep Chaerudin 2019). Adanya tugas tersebut merupakan bentuk kehadiran negara yang wajib untuk memberikan perlindungan dalam keamanan data personalnya dari penyalahgunaan oleh pihak yang ingin memanfaatkan data karena latar belakang ekonomi maupun tindakan criminal lainnya, seperti pembuatan indentitas diri palsu, indentitas perbankan, identitas international seperti passport

Masih menurutnya, bahwa ada 5 prinsip dasar yang harus disiapkan negara dalam mengadapi ancaman dan tantangan siber seperti dalam diagram di bwaah ini :

Negara telah membuat regulasi dan system yang tersusun dengan rapi penanganan data identitas melalui satu pintu sehingga pengawasan keamanannya lebih mudah dikelola.

Ini merupakan system yang dapat dibangun dengan mudah dibanding dengan menciptakan sebuah jaringan makro yang meliputi pembangunan mandiri, brain ware dan software hasil rancang bangun domestik. Elemen individu dan badan atau perusahaan yang menjadi objek vital, harus mendapatkan payung hokum terhadap insiden pencurian data sehingga terdapat kepastian hokum untuk dapat dengan mudah melaporkan dan mendapatkan solusi jika mendaptkan kerugian atas identitas diri yang dipakai. Regulasi negara ini lah yang menjadi layer berikutnya selain pada pengamanan secara fisik atas serangan siber yang terjadi.

Perang yang nyata saat ini adalah perang siber baik dalam kapasitas hacker melawan Lembaga negara dalam hal ini menjadi tugas dan tanggung jawab Badan Siber dan Sandi Negara (BSSN) maupun perang siber yang menyerang perusahaan maupun individu. Ketahanan siber publik, *siber resilience,* merupakan bagian dari keamanan siber negara. Barometer terhadap keberhasilan melawan serangan siber yang menyerang sector privat dan korporasi seharus berbanding lurus dengan keberhasilan negara dalam mengatasi serangan siber kepada institusi negara. Utuk penting etika diplomasi pertahan dalam er siber. Negara kuat jika hanya mempertimbangkan kepentingannya semata,maka negara kecil akan tidak berdaya. Utuk itu negara berkepentingan dengan kapitalis, pemilik modal dan menguasi teknologi (Halkis, 2020)

Ancaman dalam bidang siber juga hanya bersifat melindungi data pribadi, korporasi dan insititusi militer dari serangan siber baik dari dalam maupun dari luar, namun juga ancaman siber adalah ketika negara tidak dapat melakukan tindakan preventif dengan mempersiapkan secara dini individu-individu yang tak hanya cakap dalam operasi melawan siber, namun perlunya individu yang mampu menciptakan inovasi-inovasi dalam membuat perangkat pertempuran siber. Perangkat tersebut dapat berupa pengembangan alutsista modern yang mandiri dan tangguh. Terutama dalam pembuatan software, teknologi *Artificial Inteligent* yang menggunakan bahasa (developing program) yang dibuat sendiri.

5. Kesimpulan

Kemajuan teknologi sebagai dampak revolusi industry 4.0 membawa dampak positif dan negative yang dirasakan oleh individu maupun korporasi. Selain mempermudah transaksi elektronik dan mempesingkat jarak dan waktu, perkembangan teknologi dalam bidang siber membawa ancaman tersendiri. Bagi individu ancaman pencurian data dan penipuan daring sering dirasakan akibat lemahnya lapis pengamanan siber yang seharusnya menjadi tanggung jawab pemerintah. Individu juga belum merasakan hadirnya problem solving yang legal kasus pencurian tersebut. Negara harus mempermudah layanan pengaduan dengan menggunakan teknologi yang ada yang dapat diunduh dengan mudah jika seseorang maupun perusahaan merasa dirugikan akibat serangan siber dengan segera melakukan upaya penelusuran digital.

Negara mempersiapkan dan mengenalkan teknologi *Artificial Inteligent* khususnya pada ranah pertahanan dengan langkah transfer of technologi, menyiapkan Pendidikan yang mendukung terciptanya teknologi berbasis *Artificial Inteligent* yang dapat diterapkan pada bidang-bidang militer seperti Intelijen, operasional, territorial, dan territorial mengingat pertempuran yang terjadi di masa yang akan dating merupakan pertempuran berbasis teknologi sehingga negara yang memiliki kemajuan teknologi dalam bidang militer secara teori akan lebih mudah memenangkan pertempuran.

6. Ucapan Terima Kasih

Penulis menyampaikan terima kasih kepada Letkol Sus Dr. Drs. Mhd Halkis, M. H selaku Sekretaris Prodi Diplomasi Pertahanan yang telah memberikan bimbingan dan arahan dan penulisan jurnal ini, serta rekan-rekan yang telah mendukung dan memberikan motivasi sehingga jurnal ini dapat diterbitkan

Daftar Pustaka

Cahiers Vilfredo Pareto, (2006) La révolution industrielle à l'échelle de l'histoire humaine de la biosphère

Frederich Ebert Stuftung, (2015) Les nouvelles technologies militaires numériques et les systèmes d'armes autonomes

Joseph S. Nye Jr, (2004). Power in the Global Information Age.

Jon Porter, (2020) Trump's campaign website hit with cryptocurrency scam.

Jean-Marc Vittori, (2019) Pourquoi la guerre du XXIe siècle sera technologique.

Halkis, Mhd, E*thics of Defense Diplomacy in Constellation Post National*, The International Journal of Business & Management. Volume 8, Issue 3, March 2020 , DOI: 10.24940/theijbm/2020/v8/i3/BM2003-061

Maharsi, Sri, 2000, Pengaruh Perkembangan Teknologi Informasi Terhadap Bidang Akuntansi Manajemen Jurnal Akuntansi & Keuangan Vol. 2, No. 2

Marsda TNI Asep Chaerudin, M.A.S.S., Strategi Keamanan Siber

Mark Skliton and Felix Hovsepian (2016), The 4th Revolution Industry

Michael Raska, (2020) Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns – Analysis.

Myriam Dunn Cavelty & Andreas Wenger, (2019) Cyber security meets security politics: Complex technology, fragmented politics, and networked science.

Jean-Marc Vittori, (2019) Pourquoi la guerre du XXIe siècle sera technologique.

Redaksi, (2019) https://jurnalsecurity.com/rubrik/cyber-security/

Thomas A. Johnson, 2015, Cyber-security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare

Wolfgang Ertel, (2016), An Introdutional to Artificial Inteligent,