LEMBAGA KETAHANAN ASIONAL
REPUBLIK INDONESIA

IMPLIKASI MILITER DAN EKONOMI TERHADAP CYBER WARFARE DAN LANGKAH-LANGKAH PERBAIKANNYA UNTUK MENGATASI DAMPAKNYA DI KEDUA BIDANG

Oleh :

SAIFULLAH KHAN

AIR COMMODORE / PAKISTAN

KERTAS KARYA ILMIAH PERSEORANGAN (TASKAP)
PROGRAM PENDIDIKAN REGULER ANGKATAN LXI
LEMHANNAS RI
TAHUN 2020

KATA PENGANTAR

Assalaamualaikum warahmatullah wabarakatuh, salam sejahtera bagi kita semua.

Puji dan syukur kepada satu-satunya Allah SWT. Kami sangat bersyukur atas berkat-Nya yang Dia curahkan ke atas kami dan pengampunan-Nya. Dia menciptakan manusia dengan kebijaksanaan dan kemampuan untuk menjelajahi rahasia alam yang tersembunyi. Dengan rahmat, bimbingan dan berkah-Nya, Karya Ilmiah Perorangan (TASKAP) dengan judul: "IMPLIKASI MILITER DAN EKONOMI TERHADAP CYBER WARFARE DAN LANGKAH-LANGKAH PERBAIKANNYA UNTUK MENGATASI DAMPAKNYA DI KEDUA BIDANG". Dapat diselesaikan dalam batas waktu dan ketentuan yang ditetapkan oleh Lemhanas RI. Judul TASKAP ini telah ditetapkan berdasarkan Surat Keputusan Gubernur Lembaga Ketahanan Nasional Republik Indonesia no. 81 Tahun 2020 tanggal 8 Juni 2020.

Saya beruntung memiliki Tuan Ending Fadjer sebagai penasihat saya, dan saya sangat berterima kasih atas dukungan dan bimbingannya selama proses penulisan peta tugas saya. Dia percaya pada saya dan selalu tersedia setiap kali saya menemui masalah atau memiliki pertanyaan tentang penelitian atau tulisan saya. Dia secara konsisten membiarkan makalah ini menjadi pekerjaan saya sendiri, tetapi mengarahkan saya ke arah yang benar dengan memotivasi saya untuk merencanakan tesis saya lebih awal dan memberikan produk yang sangat baik. Keahlian dan umpan baliknya tentang keamanan dunia maya telah menjadi cahaya penuntun selama pekerjaan penelitian saya.

Terakhir, izinkan saya untuk tidak lupa mengucapkan terima kasih yang tulus kepada istri saya Nyonya ABIDA IQBAL karena dia telah membebaskan

saya dari semua beban rumah tangga, ketika saya sibuk mempersiapkan tesis saya.

Penulis berharap makalah ini dapat bermanfaat sebagai sumber pemikiran bagi Lemhannas RI, serta bagi seluruh pemangku kepentingan.

Akhirnya semoga Allah SWT, Tuhan Yang Maha Esa senantiasa memberikan keberkahan dan hidayah kepada kita semua dalam menjalankan tugas dengan kejujuran dan pengabdian.

Sekian dan terima kasih, Wassalaamualaikum warahmatullah wabarakatuh,

Jakarta, 9 Oktober 2020

SAIFULLAH KHAN
AIR COMMODORE, PAKISTAN
Nomor Peserta: 070

PERNYATAAN KEASLIAN

1. Yang bertanda tangan di bawah ini:

   Nama : Saifullah Khan
   Pangkat : Air Commodore
   Jabatan : Sector Commander
   Instansi : Air Defence C^2 Center
   Alamat : Angkatan Udara Pakistan

   Sebagai peserta Program Pendidikan Reguler Angkatan (PPRA) LXI Tahun 2020 menyatakan dengan sebenarnya bahwa:

   a. Kertas Karya Ilmiah Perseorangan (Taskap) yang saya tulis adalah asli.

   b. Apabila ternyata sebagian atau seluruh tulisan Taskap ini terbukti tidak asli atau plagiasi, maka saya bersedia dinyatakan tidak lulus pendidikan Lemhanas RI.

2. Demikian pernyataan keaslian ini dibuat untuk dapat dipergunakan sebagaimana mestinya.

Jakarta, 9 Oktober 2020

SAIFULLAH KHAN

AIR COMMODORE, PAKISTAN

Nomor Peserta: 070

DAFTAR ISI

2. TABLE

TABEL

TABEL 1. Kasus utama Perang Dunia Maya

BAB I
PENDAHULUAN

1. Latar Belakang

Keadaan alami umat manusia adalah menjadi kompetitif, yang pasti mengarah pada konflik. Membahas kepastian perang, Albert Einstein berpendapat, “Selama ada negara berdaulat yang memiliki kekuatan besar, perang tidak bisa dihindari. Itu bukanlah upaya untuk mengatakan kapan itu akan datang, tetapi hanya itu yang pasti akan datang”[1]. Ketika kepentingan umat manusia diangkat ke udara, Jenderal Giulio Douhet mengamati, “Aeronautika, membuka bagi manusia bidang aksi baru, bidang di udara. Dengan demikian, perlu diciptakan medan perang baru; karena di mana pun dua orang bertemu, konflik tidak terhindarkan”[2]. Dalam karyanya yang besar, On War, Clausewitz, ahli teori dan praktisi militer abad ke-19 membahas perang pada tingkat yang lebih pribadi tetapi masih menemukan perang yang tak terhindarkan, “ Perang adalah tindakan hubungan manusia … Itu adalah bagian dari eksistensi sosial manusia”[3]. Perang yang tak terhindarkan tetap ada, apa pun bidang tindakannya.

Dua domain asli perang, darat dan laut, telah dilengkapi dengan dua domain tambahan, udara dan luar angkasa. Ketika era industri memberi jalan kepada era informasi, kuantitas dan kecepatan transfer informasi tumbuh, begitu pula penetrasi ke dalam masyarakat. Evolusi ini menghasilkan kekuatan fisik

yang dilengkapi dengan kekuatan tambahan - konten dan kode (informasi dan perangkat lunak komputer) - yang dapat memengaruhi ketiga elemen trinitas Clausewitz hampir secara instan dan bersamaan. Perubahan ini juga melegitimasi

---

1 Albert Einstein, Ideas and Opinions, New York: Crown Inc., 1954, page 118.

2 Giulio Douhet, The Command of the Air, 1921, trans. Dino Ferrari. (1942; new imprint Washington, DC: Office of Air Force History, 1983), page 3.

3 Carl von Clausewitz, On War, ed. and trans. Michael Howard and Peter Paret, Princeton, NJ: Princeton University Press, 1976, page 149.

media yang melaluinya informasi bergerak, dunia maya, sebagai domain peperangan kelima.

Munculnya komputer telah merevolusi filosofi kerja dan telah menunjukkan pergeseran paradigma dalam domain komersial maupun militer. Ini tidak hanya mengubah proses berpikir para pemikir dan ahli strategi militer, tetapi juga membawa perubahan mendasar dalam semua aspek kehidupan kita. Fenomena yang muncul-internet adalah produk sampingan dari evolusi jaringan komputer. Ini benar-benar telah mengubah dunia menjadi desa global, dengan semua bagian dunia terhubung ke jaringan yang besar.

Evolusi dunia maya dan jaringan dapat ditelusuri kembali ke APRANET[4] (Advanced Research Projects Agency Network), jaringan komputer militer pertama yang diprakarsai oleh Departemen Pertahanan AS pada akhir tahun enam puluhan. Pesan pertama di ARPANET dikirim oleh mahasiswa programmer UCLA Charley Kline, pada pukul 22:30 tanggal 29 Oktober 1969, dari Boelter Hall 3420. Pada tanggal 5 Desember 1969, seluruh jaringan dari empat komputer telah berhasil dibangun.

Perjalanan komputer jaringan dimulai dari empat node pada tahun 1969 menjadi jaringan empat puluh komputer pada tahun 1973. Untuk lebih memperluas jaringan ini ke dunia luar, sebuah situs seismik di Norwegia berhasil dihubungkan dengan APRANET melalui komunikasi satelit. Komputer di London juga Email pertama yang memanfaatkan jaringan ini dikirim pada tahun 1971, dan situs web pertama dibuat pada tahun 1991.dihubungkan dengan APRANET melalui tautan yang sama. Pada tahun 1975, PARANET dinyatakan beroperasi, dan Departemen Pertahanan mengambil alihnya.

Sejak itu, kemajuan dalam prosesor dan teknologi microchip, konektivitas telah diperbesar dari jaringan beberapa komputer menjadi milyaran perangkat yang

[4] PW Singer & Allan Friedman, Cyber Security and Cyber War, , Oxford University Press , New York

terhubung bersama. Selain itu, penggunaan internet telah beragam dan tidak lagi hanya domain militer. Saat ini, ada hampir 8.7 miliar perangkat yang terhubung di internet yang bertukar 40 triliun email setiap tahun. Padahal, jumlah website telah membengkak hingga 30 triliun. Diyakini bahwa, jumlah perangkat yang terhubung di internet akan membengkak menjadi 40 miliar pada tahun 2020[5]. Penggunaan internet telah meluas ke rumah sakit, jaringan listrik, bursa saham, sistem komunikasi dan transportasi.

Web komputer yang dihasilkan di tingkat global disebut sebagai ruang cyber. Ketersediaan informasi penting di ruang siber membuatnya rentan terhadap serangan siber. Oleh karena itu, perang siber telah menjadi peperangan paling penting di zaman sekarang. Ini perlu dipahami dengan baik agar operator pertempuran dunia maya, tentara, komandan, dan manajer di semua tingkatan memiliki pemahaman yang jelas tentang operasi, implikasi, dan tindakan balasannya.

2. Rumusan Masalah

Domain militer dan ekonomi keduanya memiliki relevansi yang besar dengan domain informasi. Dengan munculnya komputer berkecepatan tinggi yang mampu memproses prosesor kelas atas dan digitalisasi data, domain informasi telah merevolusi. Entitas informasi dalam militer dan ekonomi telah dihubungkan mallei media yang berbeda untuk memastikan pemrosesan yang cepat dan tepat dari informasi dan penyebaran yang diperlukan. Sisi lain dari kemajuan ini adalah bahwa kerentanan sistem ini telah meningkat berkali-kali lipat.

Orang luar dan pencuri elektronik dapat memiliki akses ke sistem ini dan dapat menggunakannya untuk keuntungan mereka atau mungkin merusaknya berdasarkan beberapa intensitas buruk. Sistem militer akan menjadi perhatian negara-negara musuh, sedangkan sistem komersial ditargetkan untuk memperoleh keuntungan

[5] Zaigham Mehmood, Data Science and Big Data Computing, Springer,UK, 2016

finansial, akses ke etnologi baru, eksploitasi dan gangguan, dll. Ini adalah ancaman terbesar yang dihadapi dunia di era kontemporer.

Domain cyber bahkan dapat mempengaruhi perubahan pemerintahan dan menyerang sistem keuangan. Sangat diyakini bahwa Rusia terlibat dalam rekayasa pemilihan AS untuk mendukung Donald Trump[6]. Pada tahun 2010, Amerika dan Israel mampu merusak sentrifugal nuklir Iran melalui serangan dunia maya.

Sejumlah besar serangan dunia maya sedang terjadi terhadap sistem keuangan yang lebih besar[7]. Peretas juga efektif dalam mengganggu atau menghancurkan sistem militer di masa lalu[8]. Penjahat dunia maya, individu atau teroris dunia maya yang disponsori negara bahkan dapat memulai perang nuklir antara musuh bebuyutan seperti India dan Pakistan. Ini akan menyebabkan malapetaka besar dan mengguncang perdamaian dunia. Spionase dunia maya adalah bidang lain yang telah menjadi ancaman besar bagi industri kelas atas.

Perang siber kini telah menjadi dimensi kelima dari peperangan. Kemajuan teknologi telah meningkatkan kerentanan sistem ini. Mengacu keoada rumusan masalah tersebut, maka pertanyaan kajian disusun sebagai berikut:

a. Apa dampak perang dunia maya terhadap sistem militer & komersial?
b. Bagaimana sistem ini ditargetkan?
c. Apa tujuan dan siapa semua yang terlibat dalam kegiatan ini?
d. Bagaimana kita dapat melawan ancaman melalui tindakan yang tepat di tingkat nasional dan organisasi?

[6] FBI, CIA and NSA joint report, Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution, 2017

[7] Candid Wueest, Internet Security Threat Report, Financial Threats Review, 2017

[8] Jeffery Carr, Inside Cyber Warfare, O’Reilly Media, Beijing, 2012

3. Maksud dan Tujuan Penelitian

a. Maksud.

Tujuan dari secara mendetail dan menyoroti pemain yang terlibat dalam perang dunia maya. Itu IRP ini adalah untuk mempelajari perang dunia maya juga akan mengedepankan motif di balik serangan ini. Upaya akan dilakukan untuk merekomendasikan beberapa tindakan balasan yang akan membantu dalam mengurangi efektivitas serangan Cyber.

b. Tujuan Penelitian.

1) Untuk memahami dan mendefinisikan terminologi Cyber Warfare.
2) Untuk menentukan target Cyber Warriors. Untuk menjelaskan berbagai strategi Perang Dunia Maya yang ofensif dan defensif.
3) Untuk mengukur dampak Perang Dunia Maya di domain militer dan ekonomi.
4) Untuk menyarankan beberapa rekomendasi untuk melawan penjahat Cyber di berbagai tingkatan.

4. Ruang Lingkup dan Sistematika

a. **Ruang Lingkup.** Ruang lingkup makalah ini adalah untuk mempelajari terbatas untuk memahami perang siber secara rinci dan menyoroti implikasinya pada domain militer dan ekonomi dan menyarankan tindakan penanggulangan yang layak.

b. **Sistematika.** Sebuah upaya telah dilakukan untuk pertama mengukur ancaman dan kemudian mengidentifikasi berbagai aspek perang dunia maya yang sedang dilakukan di era kontemporer. Makalah ini akan membahas aspek-aspek terkait dalam beberapa bab, sebagai berikut.

1) Pada Bab I dibahas tentang latar belakang masalah dan gagasan pengembangan konsep CW dalam kerjasama bilateral menuju multilateral dan

menyoroti masalah yang dihadapi, maksud dan tujuan penulisan serta metodologi penelitian yang digunakan.

2) Pada Bab II dilakukan tinjauan pustaka, dengan gambaran dan cakupan CW dalam konteks yang lebih luas serta hubungan antara Cyber Warfare dan Cyber Space. Bab ini juga akan membahas beberapa aspek terkait terkait kesalahpahaman tentang persepsi CW.

3) Bab III menjelaskan para pelaku perang dunia maya dan berfokus pada tujuan utama mereka. Ini juga membahas strategi cyber ofensif dan defensif secara komprehensif. Ini juga cukup menggambarkan implikasi militer dan ekonomi dari perang dunia maya dengan mengutip berbagai insiden yang terjadi di seluruh dunia baik dalam domain militer maupun ekonomi. Analisis insiden ini cukup menyoroti pentingnya Perang Dunia Maya.

4) Bab IV terutama membahas tentang langkah-langkah dan langkahlangkah yang direkomendasikan yang akan diadopsi untuk mengatasi implikasi militer dan ekonomi dari perang dunia maya di berbagai tingkatan untuk melawan ancaman ini.

Pengetahuan tentang ancaman ini merupakan langkah terpenting untuk mengurangi dampaknya. Mendidik massa, LEA, dan mengontrol akses ke peralatan TIK adalah langkah utama dalam melawan prajurit cyber yang efektif. Meskipun saya orang non-teknis, saya tetap bersemangat untuk melakukan penelitian ini, karena saya melihat masa depan domain ini sangat menantang dan menjanjikan. Bangsa yang mahir dalam bidang ini akan menguasai dunia baik dalam bidang militer maupun ekonomi.

5. Metode dan Pendekatan

a. Metode

Penelitian komprehensif dimaksudkan untuk dilakukan pada berbagai aspek perang dunia maya. Penelitian ini didasarkan pada review materi dan data sekunder. Karya penelitian dan buku yang ditulis oleh berbagai sarjana akan dikonsultasikan untuk mengembangkan dan pemahaman yang mendalam, menjadikannya sebagai dasar dan membangun pendapat saya sendiri.

b. Pendekatan

Penulisan TASKAP menggunakan pendekatan perspektif bela negara sebagai bagian yang tidak terpisahkan dari kepentingan nasional. Analisis dilakukan dengan menggunakan pendekatan multidisiplin yang terdiri dari teori sistem teknologi tak berawak, teori pertahanan dan teori kepentingan nasional.

6. Pengertian

a. Definisi Dunia Maya

Doktrin USAF - Operasi Ruang Siber 3-12 mendefinisikan Ruang Siber sebagai:

> "Sebuah domain global dalam lingkungan informasi yang terdiri dari jaringan teknologi informasi yang saling bergantung nfrastruktur, termasuk Internet, jaringan telekomunikasi, sistem komputer, serta prosesor dan pengontrol tertanam"[9].

[9] "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". Practioners Jason Andress & Steve Winterfeld, Cyber warfare: Technique, Tactics for Security, Elsevier, Newyork, 2014

Dengan kata yang lebih sederhana, itu adalah lingkungan yang diciptakan oleh pertemuan jaringan kerja sama komputer, sistem TI, dan infrastruktur telekomunikasi yang biasa disebut sebagai World Wide Web. Ini juga dapat didefinisikan sebagai:

"Kombinasi infrastruktur yang menghubungkan jutaan jaringan, router, sakelar, ponsel pintar, perangkat portable dan komputer perangkat mesh untuk berkomunikasi satu sama lain"[10].

b. Definisi Perang Cyber

Ada perdebatan yang sedang berlangsung tentang bagaimana perang dunia maya harus didefinisikan dan tidak ada definisi absolut yang disetujui secara luas[11]. Sementara mayoritas sarjana, militer dan pemerintah menggunakan definisi yang merujuk pada aktor yang dispons ori negara dan negara, Definisi lain dapat mencakup aktor non-negara, seperti kelompok teroris, perusahaan, ekstremis politik atau ideologis kelompok, peretas, dan organisasi kriminal transnasional tergantung pada konteks pekerjaan[12].

Contoh definisi yang dikemukakan oleh para ahli di bidangnya adalah sebagai berikut.

'Cyberwarfare' digunakan dalam konteks yang luas untuk menunjukkan penggunaan kekuatan teknologi antarnegara bagian dalam jaringan komputer tempat informasi disimpan, dibagikan, atau dikomunikasikan secara online[13].

---

[10] "A combination of infrastructures which connects millions of networks, routers, switches, smart phones, portable devices and computers making a mesh devices communicating with each other".

[11] Green, James A., Cyber warfare: a multidisciplinary analysis, London. 7 November 2016.

[12] Arquilla, John, "Can information warfare ever be just?" Ethics and Information Technology, page 203 212.

[13] "Cyberwarfare' is used in a broad context to denote interstate use of technological force within computer networks in which information is stored, shared or communicated online". Cyber warfare : a multidisciplinary analysis. Green, James A., 1981-. London. 7 November 2016

Paulo Shakarian dan kawan-kawan mengemukakan definisi berikut yang diambil dari berbagai karya termasuk definisi Clausewitz tentang perang:

"Cyberwarfare adalah perluasan kebijakan melalui tindakan yang dilakukan di dunia maya oleh aktor negara (atau oleh aktor non-negara dengan arahan atau dukungan signifikan negara) yang merupakan ancaman serius bagi keamanan negara lain, atau tindakan serupa yang diambil sebagai tanggapan terhadap ancaman serius bagi keamanan negara"[14].

Peperangan secara umum diyakini mengacu pada pelaksanaan permusuhan militer dalam situasi konflik bersenjata antara negara saingan atau aktor non-negara. Peperangan adalah sarana untuk memperlancar peperangan dalam suatu medium. Seperti peperangan lainnya, perang yang dilakukan di Cyberspace disebut peperangan Cyber. Penggunaan jaringan, komputasi, dan senjata siber baik dalam domain komersial maupun militer dapat dianggap sebagai Perang Siber.

Departemen Pertahanan Amerika Serikat (DoD) mencakup bagian militer Dalam definisi, yang berbunyi:

“Tindakan yang dilakukan untuk mencapai keunggulan informasi guna mendukung bangsa strategi militer dengan mempengaruhi informasi dan informasi musuh sistem berbasis sambil memanfaatkan dan mempertahankan sistem informasi sendiri”[15].

---

[14] "Cyberwarfare is an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security"
Shakarian, Paulo, Introduction to cyber-warfare: a multidisciplinary approach. Shakarian, Jana., Ruef, Andrew. Amsterdam [Netherlands]: Morgan Kaufmann Publishers.

[15] USAF Doctrine-Cyber Space Operations 3-12,2006

Setelah membiasakan diri dengan sifat dunia maya, penting juga untuk mengidentifikasi apa itu infrastruktur kritis? Apa yang semua termasuk dalam domain infrastruktur kritis yang jika terpengaruh akan menimbulkan efek bencana pada pembuatan perang dan kemampuan mendukung perang suatu negara.

c. Definisi Infrastruktur Kritis

USA sebagai negara terdepan dalam kemajuan teknologi selalu dianggap sebagai acuan untuk mendefinisikan konsep dan istilah baru. Untuk menentukan infrastruktur kritis, sekali lagi referensi telah diambil dari USAF Doctrine –Cyber space Operation 3-12. Ini didefinisikan sebagai:

"Sistem dan aset, baik fisik maupun virtual, sangat vital bagi Amerika Serikat bahwa ketidakmampuan atau kehancuran system Tersebut dan aset akan memiliki dampak yang melemahkan keamanan, nasional keamanan ekonomi, kesehatan atau keselamatan publik nasional, atau apapun kombinasi dari hal-hal itu"[16].

Sebutkan di sini bahwa Departemen Keamanan Dalam Negeri (DHS), AS, telah mengidentifikasi beberapa infrastruktur penting yang harus dilindungi dari serangan dunia Definisi yang sama dapat diterapkan di negara mana pun di dunia. Perlu juga di maya dalam situasi damai maupun perang. Ini adalah sebagai berikut:

1) Pertanian dan Pangan
2) Perbankan dan Keuangan
3) Industri Kimia
4) Fasilitas Komersial

[16] Ibid

5) Komunikasi
6) Manufaktur Kritis
7) Bendungan & Air
8) Pangkalan Industri Pertahanan
9) ayanan Darurat
10) Sumber Energi
11) Fasilitas Pemerintah
12) Perawatan Kesehatan dan Kesehatan Masyarakat
13) Teknologi Informasi
14) Reaktor Nuklir
15) Bahan dan Limbah
16) Pos dan Pengiriman
17) Sistem Transportasi

BAB II
TINJAUAN PUSTAKA

7. Umum

Sejak diperkenalkannya komputer dalam domain militer dan komersial, kerentanannya terhadap serangan dunia maya telah meningkat. Penggabungan teknologi informasi dalam domain ini telah meningkatkan banyak potensi mereka, tetapi penjaga fisik telah diganti dengan penjaga virtual. Penjaga fisik dengan senjata yang melindungi perlengkapan dan material fisik lebih efektif dan sulit untuk dinegosiasikan. Tetapi penjaga virtual dapat dinegosiasikan dengan sangat mudah. Kadang-kadang para penjaga ini bahkan tidak mengetahui bahwa sistem yang mereka lindungi telah disusupi. Upaya telah dilakukan ke arah ini sampai batas tertentu.

Di masa lalu, telah terjadi serangan dunia maya terhadap entitas pemerintah serta militer. Stephen Herzog telah menjelaskan secara rinci bagaimana lembaga pemerintah Estonia disfungsional oleh serangan siber yang dilakukan oleh Rusia[17]. Estonia menjadi negara yang baru muncul dan sumber daya yang terbatas tidak diperlengkapi untuk melawan serangan ini. Berbagai lembaga pemerintah terhenti. Keseriusan serangan terhadap Estonia menghasilkan tanggapan internasional yang cepat. Estonia memiliki sedikit persiapan pertahanan dunia maya formal di luar kerangka kerjanya untuk melawan tindakan terorisme tradisional, dan Tim Tanggap Darurat Komputer (CERT) pemerintah memerlukan bantuan Finlandia, Jerman, Israel, dan Slovenia untuk memulihkan operasi jaringan normal[18].

Dorthy E Denning menyoroti bahwa peretas telah menyerang sistem yang dijalankan oleh pemerintah dan pengusaha bisnis. Tidak ada area yang dijalankan oleh

[17] Herzog, Stephen. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, Journal of Strategic Security 4, no. 2, 2011
[18] Ibid

otak buatan yang terlindungi dari penyerang ini. Rumah sakit, bank, industri, dan jaringan komunikasi semuanya dapat diserang, dieksploitasi, dan dimanipulasi. Mereka dapat merusak sistem sinyal lalu lintas dan kereta api. Mereka memiliki kemampuan untuk menanamkan bom elektronik ke dalam sistem yang dapat menimbulkan malapetaka dan menyebabkan kerusakan skala besar[19].

M. Gercke dalam bukunya Understanding Cyber Crime: a Guide for Developing Countries menuturkan bahwa pada tahun 2003, software jahat menyebabkan 17 milyar dollar bagi perekonomian dunia. Perkiraan konservatif adalah bahwa kejahatan dunia maya menghasilkan sekitar 100 miliar Dolar setiap tahun di AS. Ini telah melampaui uang yang dihasilkan melalui obat-obatan terlarang dan bisnis ilegal. Sebagian besar pengusaha dan industri Amerika menganggap kejahatan dunia maya sebagai ancaman yang lebih kuat daripada pencurian fisik[20]. Interkonektivitas entitas telah membuat pekerjaan mencuri lebih mudah. Seorang peretas hanya membutuhkan keahlian dalam peretasan, komputer, dan koneksi internet.

Paul Rosenzweigh dalam bukunya Cyber Warfare menarasikan kisah serangan dunia maya yang dilakukan terhadap fasilitas Nuklir Iran. Stuxnet adalah nama virus yang menargetkan sistem Supervisory Control dan Data Acquisition. Ini menyerang perangkat lunak khusus SCADA yang bertanggung jawab untuk mengendalikan sentrifugal. Stuxnet memasuki sistem Iran melalui beberapa interaksi antara sistem SCADA dan program eksternal berbasis Windows.

Diasumsikan bahwa seorang ilmuwan Iran menggunakan USB yang terinfeksi di salah satu komputer yang terkait dengan program nuklir Iran. Beberapa percaya bahwa itu adalah pekerjaan orang dalam yang dengan sengaja memasang USB yang terinfeksi ke dalam sistem. Stuxnet melewati sistem keamanan yang dipasang untuk

[19] Dorthy E Denning , Information Warfare and Security, ACM Press, California, 1999
[20] M. Gercke ,Understanding Cyber Crime: a Guide for Developing Countries, ITU-D ICT Applications and Cybersecurity Division, Geneva, 2011

menjalankan sentrifugal pada kecepatan yang konstan dan aman. Iran belum secara terbuka menerima tingkat kerusakan yang diterima sistemnya. Namun diyakini, bahwa minimal 1.000 sentrifugal di fasilitas Natanz telah hancur atau rusak[21].

Mencuri atau memperoleh rahasia nasional musuh dulunya merupakan permintaan besar bagi mata-mata, tetapi di dunia cyber, spionase dunia maya dapat dengan mudah dilakukan terhadap negara bangsa musuh. Diyakini bahwa terabyte data telah dicuri oleh peretas tak dikenal dari Pentagon yang secara serius membahayakan keamanan negara AS. Serupa dengan itu, pemberontak siber akan menyerang entitas siber musuh untuk merusak, memblokir, atau menghancurkannya[22].

Komandan Sayap MK Sharma dalam bukunya, "Cyber Warfare, The Power of the Unseen" menceritakan malapetaka yang diciptakan oleh Rusia di Georgia. Infrastruktur kritis diserang oleh penyerang dunia maya Rusia yang memengaruhi media pemerintah, sistem transportasi keuangan yang menyebabkan kekacauan dan kebingungan. Semua jaringan komunikasi runtuh dan tanggapan yang sangat dibutuhkan dari militer Georgia tidak dapat dihasilkan[23].

Laporan Ancaman Keamanan Internet (ISTR) yang dibuat oleh Symantec menjelaskan penipuan keuangan dan pencurian yang dilakukan oleh pencuri Cyber. Grup Dyre (Infostealer.Dyre) biasanya menargetkan wirausahawan besar dan merampas ribuan dolar mereka. Target dipilih sendiri dan terinfeksi dengan email phishing. Kelompok lain (Trojan.Redaman) yang aktif di Rusia dan menargetkan sistem perbankan jarak jauh. Grup Buhtrap juga telah terlibat dalam faud perbankan sebesar 25 juta dolar di Rusia dan Ukraina. Demikian pula, pada tahun 2006, seorang

---

[21] Paul Rosenzweigh, Cyber warfare: How Conflicts in Cyber Space are Challenging America and Changing the World , Praeger, USA, 2013

[22] M. Gercke ,Understanding Cyber Crime: A Guide for Developing Countries, ITU-D ICT Applications and Cybersecurity Division, Geneva, 2011

[23] Wing Commander MK Sharma, Cyber Warfare, The Power of the Unseen, KW Publications, New Delhi, 2011

pencuri dunia maya mencuri sekitar US $ 81 juta dari bank sentral Bangladesh. Itu adalah salah satu perampokan bank paling berani dari jenisnya. Para peretas ini masuk ke komputer bank dan memperoleh semua kode akses untuk mentransfer dana.

Spionase industri dan pencurian hak kekayaan intelektual adalah aspek lain dari pencurian dunia maya. Negara berkembang telah terlibat dalam kegiatan ini untuk mendapatkan akses ke teknologi canggih. Laporan Symantec mengungkapkan bahwa peretas komputer yang menggunakan server berbasis di AS yang dimiliki oleh seorang pemuda China (dijuluki 'Covert Grove') menyerang 29 perusahaan yang terlibat dalam penelitian, pengembangan, dan pembuatan bahan kimia dan bahan canggih. Tujuan utama serangan ini adalah untuk mengumpulkan kekayaan intelektual seperti dokumen desain, formula, dan proses manufaktur. " Serangan itu berlanjut selama hampir dua bulan. Dia berhasil mencuri informasi berharga yang akan digunakan dalam produksi lokal[24].

Dalam bukunya Dark Territory: The Secret History of Cyber War (2016), Fred Kaplan menarik dari percakapan dengan para pemimpin pemerintah Amerika terkemuka, termasuk mantan direktur National Security Agency, untuk menyampaikan pandangan di balik layar pada formulasi kebijakan atas berlangsung beberapa dekade. Kaplan menulis: "Jika Amerika, atau Komando

Siber AS, ingin melakukan perang dunia maya, ia akan melakukannya dari dalam rumah kaca". Apa pun yang bisa kita lakukan, menurutnya, musuh bisa meniru atau belajar untuk berbuat lebih baik. (Serangan dunia maya 12 Mei menggunakan teknologi yang berasal dari Amerika Serikat.) Buku ini menelusuri kemajuan Amerika Serikat dalam keamanan siber, dan Kaplan menyimpulkan bahwa meskipun cukup

[24] Industrial Espionnage Cyber Style- Financial Times

banyak upaya telah dilakukan untuk mengembangkan kejahatan siber, lebih sedikit yang berfokus pada melindungi negara dari serangan potensial[25].

Dalam bukunya Cyber War: The Next Threat to National Security and What to Do About It Richard A. Clarke, mantan penasihat kontraterorisme Presiden George W. Bush yang mengkritik presiden karena mengabaikan peringatan pra9/11 tentang Al yang menjulang. Ancaman Qaeda, berpendapat bahwa lebih banyak sumber daya harus diinvestasikan untuk menangkal serangan dunia maya. Meskipun pemerintah telah menyiapkan perlindungan untuk informasi intelijen dan militer, sektor swasta tetap rentan. Clarke dan rekan penulisnya menguraikan seperti apa sebenarnya serangan dunia maya di Amerika Serikat - kereta api akan dinonaktifkan, sistem keuangan dan jaringan listrik rusak, catatan medis terhapus. Clarke dan Knake menyusun rencana yang menurut mereka akan memberi Amerika Serikat kesempatan untuk bertempur[26].

Buku ini mengambil pandangan holistik tentang dunia cyber dan bagaimana hal itu berkaitan dengan Amerika Serikat terkait kapabilitas, kerentanan, kebijakan, dan strategi potensial. Kami, sebagai mahasiswa dan instruktur mata kuliah Networks for Cyber Operations, menggunakan buku ini sebagai salah satu teks kami di semester Musim Semi 2016. Penulis Richard

Clarke menggunakan pengalamannya menangani senjata nuklir, dan perannya sebagai Special Advisor pada President for Cyber Security menjelaskan bagaimana situasi dunia telah berubah membuat serangan cyber menjadi ancaman yang signifikan bagi Amerika Serikat. Clarke dan Knake melakukan pekerjaan yang sangat baik dalam berbicara kepada khalayak umum (dari pemula dunia maya hingga prajurit dan peretas cyber yang berpengalaman). Para penulis memperkenalkan subjek dengan menggambarkan serangan siber Israel di Suriah sebelum pemboman fasilitas

---

[25] Fred Kaplan, Dark Territory: The Secret History of Cyber War, New York, America, 2016

[26] Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat To National Security And What To Do About It, Harper Collins, 2010

nuklir pada tahun 2007. Buku ini menjauhi aspek teknis dari serangan siber, tetapi memberikan informasi latar belakang terperinci tentang Internet dan bagaimana digitalisasi telah menciptakan medan perang baru.

Meskipun Neuromancer ditulis pada tahun 1984 jauh sebelum munculnya World Wide Web, karya penting William Gibson memprediksi peran Cyber Space di masa depan. Dia memberikan ide tentang "representasi grafis dari data yang diambil dari bank setiap komputer dalam sistem manusia". Protagonis Gibson, Case, adalah seorang peretas komputer yang dapat menyambungkan mesinnya untuk merasakan transmisi elektronik secara dekat - dengan kata lain, masukkan "matriks," istilah lain yang dibuat oleh Gibson. Setelah Case kedapatan mencuri oleh mantan majikannya, mereka merusak sistem saraf pusatnya, memutuskan aksesnya ke dunia maya. Ketika dia ditawari bantuan untuk memperbaiki sistem sarafnya dengan imbalan layanan peretasannya dalam misi jahat, Case langsung mengambil kesempatan itu. Dan mulailah novel ini berlangsung cepat. Buku kanonik mengeksplorasi implikasi dari kecerdasan buatan yang semakin kuat[27].

Penulis buku Cyber Warfare - Truth, Tactics, and Strategies, Dr. Chase Cunningham memegang gelar Ph.D. dan M.S. dalam ilmu komputer dari Colorado Technical University dan menikmati pengalaman lebih dari 20 tahun dalam operasi cyber forensic dan cyber analic, dan telah menghabiskan waktu di pusat kerja di NSA, CIA, FBI, dan lembaga pemerintah lainnya.

Dalam Cyber Warfare - Truth, Tactics, and Strategies, dia menjelaskan kepada pembaca untuk memahami skala ancaman dunia maya saat ini, sejarah dan bagaimana mereka mengimbangi evolusi teknologi informasi dan komunikasi, karena mereka menjadi bagian penting dari kehidupan sehari-hari.

[27] William Gibson, Neuromancer, Hachette UK, 2016

Dia berpendapat bahwa banyak pertempuran di masa depan akan dilakukan dengan senjata cyber, mempersempit kesenjangan sumber daya dan kemampuan yang telah lama ada antara negara kaya dan miskin. Semuanya sekarang dapat secara efektif menjatuhkan musuh mereka[28].

Penulis juga menjelaskan kekurangan dari jaringan yang telah kami bangun, mengapa keamanan siber adalah pengejaran yang tidak pernah berakhir dan secara khusus mengapa keamanan berbasis perimeter tidak lagi menjadi pilihan yang baik di era kerja jarak jauh. Dia menekankan pentingnya strategi dalam perang dunia maya. Sama seperti peperangan di ruang fisik, perubahan taktik juga penting. Seseorang harus beradaptasi dengan keadaan baru yang ditimbulkan oleh musuh dunia maya.

Untuk membantu pembaca lebih memahami masalah ini, ia menghubungkan taktik dan teknik serangan dunia maya dengan contoh kehidupan nyata (militer) dari Perang Irak. Penulis juga mengilustrasikan alat dan teknologi yang dapat berguna untuk meningkatkan postur keamanan organisasi dan membantu merespons dengan cepat dan efektif terhadap potensi ancaman dunia maya.

8. Kerangka Hukum sebagai Payung untuk Cyber Warfare

Hampir tidak mungkin untuk membaca berita tanpa menemukan berita utama yang mengatalogkan pelanggaran dunia maya terbaru atau penyalahgunaan data. Kekayaan intelektual dicuri dari perusahaan dengan kecepatan yang mengkhawatirkan. Aktor asing ikut campur dalam pemilihan melalui akun media sosial palsu, bersama dengan cara lain yang lebih jahat - termasuk akses diam-diam dari email kampanye internal. Penjahat menggunakan celah gelap internet untuk menjual narkoba, senjata, dan bahkan orang. Dan kelompok teroris menggunakan media digital untuk merekrut dan menginspirasi calon pengikut di seluruh dunia.

[28] Dr. Chase Cunningham, Cyber Warfare – Truth, Tactics, and strategies, Packt Publishing UK, 2020

Jumlah perusahaan dan pemerintah yang menjadi korban peretasan digital hampir terlalu banyak untuk dihitung - Ashley Madison, Bank of Montreal, CIBC, eBay, Equifax, dan JP Morgan Chase menawarkan contoh yang siap pakai. Volume peristiwa ini mengungkapkan paradoks ekonomi digital dan keamanan siber. Di satu sisi, teknologi telah menghasilkan kenyamanan, efisiensi, dan penciptaan kekayaan - dan karenanya, perusahaan mendorong untuk menghubungkan segala sesuatu yang dapat dihubungkan. Di sisi lain, dorongan besar untuk mendigitalkan masyarakat ini berarti membangun kerentanan yang melekat ke dalam inti model ekonomi. Ini semua terjadi di atas sistem aturan global yang sangat terfragmentasi dan terbelakang.

Karena perang dunia maya baru muncul dalam beberapa tahun terakhir, berbagai negara memiliki definisi yang berbeda untuk istilah yang serupa, bahkan jika mereka memiliki definisi sama sekali.[29] Bahkan di dalam suatu negara, karena konsep perang siber ini sangat baru, lembaga pemerintah berbeda dalam hal definisi mereka tentang istilah tertentu. Misalnya, Departemen Pertahanan Amerika Serikat mendefinisikan dunia maya:

"Domain global dalam lingkungan informasi yang terdiri dari jaringan infrastruktur teknologi informasi yang saling bergantung, termasuk Internet, jaringan telekomunikasi, sistem komputer, dan prosesor dan pengontrol tertanam." [30]

Namun Laporan Layanan Riset Kongres 2001 mendefinisikan dunia maya:

"keterhubungan total manusia melalui komputer dan telekomunikasi tanpa memperhatikan geografi fisik."[31]

[29] Hathaway, supra note 36, page 818, 823-825.
[30] Schaap, supra note 12, page 125.
[31] Ibid. page 126.

Selain itu, Strategi Militer Nasional untuk Operasi Ruang Siber memiliki definisi lain dari ruang maya:

“Domain ditandai dengan penggunaan komputer dan perangkat elektronik lainnya untuk menyimpan, memodifikasi, dan bertukar data melalui sistem jaringan dan infrastruktur fisik terkait”[32].

Perlu dicatat bahwa keragaman definisi ini mengarah pada pendefinisian ruang siber, bukan peperangan siber, subjek yang jauh lebih kontroversial yang harus menemukan terminologi umum jika suatu perjanjian atau kerangka hukum internasional lainnya akan dibangun.[33] Clarke, siber yang disebutkan di atas Pakar keamanan, mendefinisikan serangan dunia maya:

"Tindakan suatu negara-bangsa untuk menembus komputer atau jaringan negara lain dengan tujuan menyebabkan kerusakan atau gangguan" [34].

Beberapa sarjana mengkritik definisi ini karena tidak membedakan antara kejahatan dunia maya, serangan dunia maya, atau perang dunia maya dan juga tidak menyebut aktor non-negara (yang sering menjadi pelaku serangan dunia maya).[35] Kepala Staf Gabungan juga telah mengemukakan Definisi militer untuk serangan dunia maya, yang menyatakan serangan dunia maya adalah:

"Tindakan bermusuhan menggunakan komputer atau jaringan terkait atau ... sistem, aset, atau fungsi”[36].

---

[32] Schaap, supra note 12, page 126.

[33] Hathaway, supra note 36, page823.

[34] Id. page 823 (citing Richard A. Clarke & Robert K Knake, Cyber War: The Next Threat to National Security and What to Do About It, 2010.

[35] Hathaway, supra note 36, page 823-24.

[36] Ibid. Page 824.

Perbedaan antara negara-negara dalam mendefinisikan serangan bersenjata memainkan peran kunci dalam kesulitan membangun kerangka hukum.[37] Kerjasama Shanghai adalah perjanjian yang ditandatangani oleh Rusia, Cina, dan negara-negara Asia Tengah lainnya yang mendefinisikan perang dunia maya lebih ekspansif daripada Amerika Serikat karena yang termasuk dalam konteks perang dunia maya adalah "perang informasi", yang berarti:

"Pencucian otak psikologis massal untuk mengguncang masyarakat dan negara, serta memaksa negara untuk mengambil keputusan demi kepentingan pihak lawan"[38].

Negara-negara demokrasi Barat prihatin dengan dimasukkannya perang informasi ini dalam definisi perang dunia maya Kerjasama Shanghai karena katakata stabilitas politik dapat digunakan untuk membenarkan penyensoran pidato politik pembangkang online.[39] Menariknya, Rusia telah menyatakan bahwa mereka akan mempertimbangkan peperangan informasi apa pun terhadapnya atau militernya sebagai fase militer dari suatu konflik.[40]

Definisi lain yang telah disusun oleh sekelompok sarjana untuk memecahkan beberapa masalah penerapan hukum yang akan dibahas di bawah ini menggambarkan serangan dunia maya sebagai:

"Tindakan apa pun yang dilakukan untuk merusak fungsi jaringan komputer untuk tujuan keamanan politik atau nasional"[41].

---

[37] Kirsch, supra note 7, page 641.

[38] Hathaway, supra note 36, page 825 (quoting Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, Dec. 2, 2008, Annex 1, at 209 [hereinafter SCO Agreement]).

[39] Ibid.

[40] Schaap, supra note 12, page 124.

[41] Hathaway, supra note 36, page 826.

Hukum konflik bersenjata mengatur tindakan militer antar negara selama masa konflik bersenjata yang sedang berlangsung. Kunci analisisnya adalah kapan serangan dunia maya akan dianggap sebagai serangan bersenjata menurut Pasal 51? Seseorang harus melakukan analisis tentang apa arti kekuatan untuk menempatkan perang dunia maya dalam kerangka kerja ini.

Pasal 2 (4) Piagam PBB melarang ancaman atau penggunaan kekerasan terhadap negara lain. Pendekatan adalah pendekatan berbasis target, yang melihat ke target serangan dunia maya untuk memutuskan apakah serangan bersenjata terjadi. Salah satu cara untuk melihat apakah kekuatan dan, melalui itu, serangan bersenjata telah terjadi terhadap negara korban adalah pendekatan berbasis efek.

Pendekatan ini melihat efek langsung serangan dunia maya terhadap statuskorban, tetapi masalah yang dilihat beberapa orang dalam pendekatan ini adalah bahwa serangan dunia maya biasanya tidak secara langsung menyebabkan kerusakan. Serangan dunia maya dapat menyebabkan bahaya melalui cara tidak langsung, seperti seseorang meninggal akibat saluran telepon terputus ke pusat panggilan darurat karena serangan penolakan layanan yang .didistribusikan.

Oleh karena itu, ia mendukung kemajuan tatanan kelembagaan internasional yang lebih stabil. Sistem berbasis aturan internasional di dunia maya masih dalam tahap awal, dan pendekatan konsensus diperlukan untuk memastikan bahwa semua negara berkontribusi dalam menyusun arsitektur tata kelola.

9. Kerangka Teoretis

a. Teori Peperangan

Perang harus dipahami sebagai konflik bersenjata yang aktual, disengaja, dan meluas antara komunitas politik, dan oleh karena itu didefinisikan sebagai bentuk

kekerasan atau intervensi politik. Warfare - mengacu pada aktivitas dan karakteristik umum dari jenis perang, atau perang secara umum. Tindakan yang dilakukan oleh satu kelompok terhadap kelompok lain untuk mencapai tujuannya atau untuk mencapai keunggulan. Perang siber juga berkaitan dengan pencapaian tujuan dalam domain dunia maya.

b. Teori keunggulan informasi

Keunggulan informasi adalah keuntungan operasional yang diperoleh dari kemampuan untuk mengumpulkan, memproses, dan menyebarkan arus informasi yang tidak terputus sementara mengeksploitasi atau menyangkal kemampuan musuh untuk melakukan hal yang sama. Komandan memanfaatkan keunggulan informasi untuk menyelesaikan misi. Dalam ranah cyber, kelompok penentang juga mengeksploitasi informasi untuk mendapatkan keuntungan dari kelompok lain

c. Strategi Serangan dan Pertahanan

Dalam strategi ofensif, sebuah kelompok mengambil tindakan berurutan untuk mengambil keuntungan dari lawan dan mencapai tujuan yang ditetapkan. Sebaliknya, strategi defensif digunakan untuk menyangkal superioritas kelompok lawan dan menjaga kepentingannya. Kedua strategi ini sama-sama berlaku untuk domain cyber. Faktanya, kelompok yang bersaing tetap mencari informasi satu sama lain untuk menyusun rencana balasan mereka untuk mempertahankan kemampuan ofensif dan defensif mereka.

10. Data dan fakta

Dengan perkembangan teknologi informasi (TI), dunia maya menjadi medan pertempuran lain setelah darat, laut, udara, dan luar angkasa. Internet telah menjadi bagian integral dan penting dari suatu negara, masyarakat, dan kehidupan sehari-hari individu. Namun, bersama dengan kemudahan yang dihadirkan oleh Internet, hal itu juga menimbulkan peningkatan jumlah potensi risiko dan tantangan. Misalnya, jumlah serangan dunia maya pada tahun 2011 meningkat 36% dibandingkan dengan tahun

2010, dan jumlah perangkat lunak berbahaya meningkat 41% selama periode yang sama. Sejumlah contoh telah muncul selama 25 tahun terakhir yang menunjukkan keterlibatan satu negara dalam serangan dunia maya terhadap negara lain.

Buku putih [48] yang ditulis tentang pertahanan nasional di China dan di seluruh dunia, yang diterbitkan pada tahun 2013, menunjukkan, “Perubahan dalam bentuk perang dari mekanisasi ke informasi semakin cepat. Kekuatan besar sedang mengembangkan teknologi militer yang baru dan lebih canggih dengan penuh semangat untuk memastikan bahwa mereka dapat mempertahankan keunggulan strategis dalam persaingan internasional di bidang-bidang seperti luar angkasa dan dunia maya. " Dimensi lain dari perang dunia maya adalah mengobarkan Konflik Intensitas Rendah oleh satu negara terhadap negara lain melalui berbagai cara. Rincian beberapa insiden yang terjadi dalam dua dekade terakhir ditabulasikan seperti di bawah:-

Kasus Serangan Cyber Utama

Entitas yang Bermusuhan	Entitas Sasaran	Jangka Waktu	Deskripsi Kegiatan Singkat
AS, Israel	Iran	2008-2011	**Pertandingan Olimpiade:** AS dan Israel cukup merusak pembangkit listrik tenaga nuklir Iran (mesin sentrifugal melalui virus STUXNET)
Rusia	Ukraina	2015-2016	**Serangan Jaringan Listrik Ukraina:** Peretas Rusia menembus sistem distribusi listrik dan mematikan sistem yang menyebabkan pemadaman listrik di seluruh negeri.
Republik Faderal Yogoslavia	Kosovo dan NATO	1999	Selama perang Kosovo, para peretas Yogslavia, Rusia dan China (setelah serangan udara NATO atas kedutaan China) melumpuhkan situs-situs NATO untuk

			menunjukkan ketidaksenangan mereka atas keterlibatan NATO.
Rusia	Georgia	2008	Akibat penembakan drone Georgia oleh jet tempur Rusia, ketegangan meningkat antara dua negara. Selanjutnya, peretas Rusia mengganggu semua layanan internet Georgia.
Iran	Arab Saudi	2012-2016	**Shamoon**: Peretas Iran Sistem jaringan perusahaan minyak milik negara Saudi, ARAMCO, dan memengaruhi 30000 stasiun kerja.
KoreaUtara	AS	2014-2015	Peretas Korea Utara menyerang perusahaan film AS (gambar sony) karena menunjukkan kekesalan mereka atas film kontroversial "The Interview"
Rusia	Estonia	2007-2008	Karena keputusan pemerintah Estonia menghapus monumen era Soviet, peretas etnis Rusia melumpuhkan semua sistem perbankan, penyiaran, dan pemerintah nasional.

11. Cyber Warfare - Konteks Strategis

Konteks strategis yang berubah membentuk strategi, struktur, dan kepemimpinan perang dunia maya. Pertanyaan kunci yang diajukannya adalah: Mengingat perubahan yang terjadi dalam tatanan dunia, apa artinya ini bagi perang dunia maya? Secara khusus, ia mencoba untuk fokus pada masalah penting tetapi tidak selalu mendesak terkait dengan ketersediaan yang lebih luas dari teknologi perang dunia maya.

Ada konsentrasi yang berlebihan pada jenis masalah ini dengan mengorbankan analisis strategis yang lebih luas tentang bagaimana perubahan dalam seluruh konteks keamanan internasional berdampak pada dunia maya. Kebanyakan kebijakan dunia maya telah berkembang untuk berfokus pada masalah jangka pendek. Struktur telah dibangun untuk mengelola tuntutan mendesak ini dan ini telah mengorbankan perhatian yang ditujukan pada masalah-masalah penting yang tidak perlu mendesak perhatian segera pemimpin.

a. Peran konteks Strategis

Konteks strategis menggambarkan tren yang relatif bertahan di lingkungan eksternal yang menjadi latar belakang untuk setiap latihan strategi. Daftar berikut adalah contoh konteks strategis:

1) Meningkatkan multipolaritas, dengan banyak pusat daya.
2) Beberapa persaingan kekuatan utama dalam domain politik, militer dan ekonomi.
3) Hilangnya monopoli kekuatan besar atas senjata nuklir (Israel, Korea Utara, Pakistan, mungkin Iran).
4) Modernisasi kekuatan strategis kekuatan utama.
5) Ketersediaan teknologi baru yang luas melalui pasar dan terutama perusahaan multinasional.
6) Beberapa mengikis internasionalisme liberal (demokrasi, Brexit, pemilu AS 2016, UE di Eropa Timur).
7) Kegagalan AS untuk mengubah Timur Tengah dengan kombinasi kekuatan lunak dan keras.
8) Terorisme lanjutan.

Ada beberapa alasan untuk fokus pada konteks strategis saat menganalisis perkembangan di dunia maya. Pertama, konteks ini akan semakin mempengaruhi dan membentuk keamanan nasional dan tatanan dunia. Hal ini relatif kurang benar selama

era pasca-Perang Dingin pada 1990-an dan 2000-an, ketika kebijakan, debat, rencana, dll. AS memiliki dampak besar yang tidak proporsional pada keamanan internasional. Sebagai puncak kekuatan Amerika, konteks stategik menjadi semakin penting.

Alasan lain pentingnya konteks adalah bahwa beberapa gagasan tentang seperti apa dunia akan terlihat penting untuk perencanaan kebijakan. Seseorang tidak bisa begitu saja melihat dunia masa lalu dan membayangkan bahwa itu akan terus berlanjut tanpa batas ke masa depan.

BAB III
PEMBAHASAN

12. Umum

Teknologi informasi dan komunikasi telah berkembang selama dua dekade terakhir dan sekarang terintegrasi ke dalam hampir setiap aspek kehidupan kita. Masyarakat saat ini jauh lebih digital dan ekonomi serta kehidupan sehari-hari kita lebih kaya karenanya. Transformasi yang ditimbulkan oleh digitalisasi ini menciptakan ketergantungan baru. Ekonomi kita, administrasi pemerintah, dan penyediaan layanan penting sekarang bergantung pada integritas dunia maya dan pada infrastruktur, sistem, dan data yang mendukungnya. Hilangnya kepercayaan pada integritas itu akan membahayakan manfaat revolusi teknologi ini.

Sebagian besar perangkat keras dan perangkat lunak yang awalnya dikembangkan untuk memfasilitasi lingkungan digital yang saling berhubungan ini telah memprioritaskan efisiensi, biaya, dan kenyamanan pengguna, tetapi keamanan tidak selalu dirancang sejak awal. Aktor jahat - negara musuh, organisasi kriminal atau teroris dan individu - dapat memanfaatkan celah antara kenyamanan dan keamanan.

Dalam domain sipil, perluasan Internet di luar komputer dan telepon seluler ke sistem cyber-fisik atau 'pintar' lainnya memperluas ancaman eksploitasi jarak jauh ke seluruh host teknologi baru. Sistem dan teknologi yang menopang kehidupan kita sehari-hari - seperti jaringan listrik, sistem kendali lalu lintas udara, satelit, teknologi medis, pabrik industri, dan lampu lalu lintas - terhubung ke Internet dan, oleh karena itu, berpotensi rentan terhadap gangguan

Berkenaan dengan domain militer, keunggulan informasi dianggap sebagai persyaratan utama pertempuran modern. Nilai informasi tidak boleh terlalu ditekankan karena relevansinya sudah dirasakan sejak awal peperangan. Sun Tzu dalam buku

klasiknya "The Art of War" telah menekankan pentingnya pengendalian informasi dan manajemen persepsi dengan menipu musuh dan menuntunnya untuk salah menghitung kekuatan dan kemampuan kita. Pertempuran modern tidak hanya dapat dilakukan dengan senjata mematikan tetapi mesin eksploitasi informasi yang kuat diperlukan untuk mempengaruhi kemampuan perang musuh. Ini akan meningkatkan peluang keberhasilan pasukan sahabat melalui melawan musuh.

Perang dunia maya menjadi cabang cabang dari Perang informasi dianggap sebagai media kelima di mana pertempuran di masa depan akan terjadi. Semua negara maju seperti AS, Prancis, Inggris, dan Jerman telah membentuk tentara Cyber khusus mereka. Medan pertempuran untuk perang dunia maya sangat luas. Penyerang tidak harus menjadi bagian dari medan pertempuran terdekat, dia hanya membutuhkan koneksi internet dan keterampilan yang diperlukan untuk memengaruhi mesin yang ditargetkan. Korban serangan dunia maya dapat berupa instalasi militer maupun entitas komersial. Bahkan negara terkecil pun bisa efektif dalam perang dunia maya melawan negara-negara berteknologi maju.

Ancaman dunia maya berdampak pada seluruh masyarakat kita, jadi sangat penting bahwa setiap orang memiliki peran dalam respons nasional kita. Meskipun pemerintah memiliki peran kepemimpinan yang lebih besar namun kontribusi sektor swasta, akademisi dan individu juga dibutuhkan yang memiliki kapasitas untuk berinovasi lebih cepat dari sektor pemerintah. Ini juga memungkinkan untuk mendapatkan pemikiran muda terbaik ke dalam keamanan dunia maya. Selain itu, Pemerintah perlu merumuskan strategi Cyber, dimana; memiliki rencana pengembangan dunia maya untuk 5-10 tahun ke depan yang melibatkan semua pemangku kepentingan. Rencana ini akan menyediakan platform dasar untuk membangun kemampuan dunia maya dan juga harus memenuhi variabel yang tidak terduga.

13. Aktor yang Terlibat dalam Perang Dunia Maya

Para peneliti dan cendekiawan telah mengidentifikasi secara luas empat kategori aktor yang telah menjadi pelaku perang dunia maya dalam berbagai bentuk pada beberapa kesempatan. Aktor-aktor tersebut adalah: a. Negara Bangsa.

b. Penjahat.

c. Kelompok Bermotivasi Masalah.

d. Organisasi teroris.

14. Tujuan Cyber Warriors

Tidak ada operasi militer yang dilancarkan tanpa menetapkan maksud dan tujuan yang ingin dicapai. Sama halnya dengan perang dunia maya, tujuan harus sangat jelas saat meluncurkan serangan dunia maya terhadap target apa pun baik yang bersifat militer atau komersial. Tujuan utamanya adalah untuk mencapai keunggulan informasi dan memanfaatkan informasi untuk keuntungan sendiri. Berikut adalah beberapa tujuan utama perang dunia maya:

a. *Spionase Cyber. Spionase, menurut Merriam-Webster, adalah:*

"praktek memata-matai atau menggunakan mata-mata untuk mendapatkan informasi tentang rencana dan kegiatan terutama dari pemerintah asing atau perusahaan pesaing." Jika kita menyamakan definisi ini dalam domain cyber, peretas dapat dianggap sebagai matamata yang mengumpulkan informasi di seluruh dunia untuk keuntungan ekonomi, politik, atau militer.

Warroior cyber yang sengaja direkrut dan sangat dihargai ini memiliki pengetahuan teknis untuk menutup apa pun dari infrastruktur pemerintah hingga sistem keuangan atau sumber daya utilitas. Mereka telah memengaruhi hasil pemilihan politik, menciptakan kekacauan di acara internasional, dan membantu perusahaan berhasil atau gagal. Banyak dari penyerang ini menggunakan ancaman persisten maju

(APT) sebagai modus operandi mereka untuk secara diam-diam memasuki jaringan atau sistem dan tetap tidak terdeteksi selama bertahun-tahun. Jadi, perang siber dapat didefinisikan sebagai:

"Bentuk serangan siber yang mencuri data rahasia, sensitif, atau kekayaan intelektual untuk mendapatkan keuntungan atas perusahaan pesaing atau entitas pemerintah"[42].

Oleh karena itu, informasi tentang aktivitas musuh selalu menjadi aset besar bagi komandan militer lawan terutama selama perang. Di masa lalu, metode pengu mpulan intelijen konvensional digunakan. Namun, dalam pertempuran modern, teknologi berbasis komputer digunakan dalam jumlah yang cukup besar. Data ini dapat dengan mudah diekstraksi oleh agen musuh dari terminal itu sendiri atau melalui serangan dunia maya[43].

c. **Pencurian Hak Kekayaan Intelektual.**

Serangan dunia maya juga digunakan untuk mencuri hak kekayaan intelektual. Telah dilaporkan bahwa beberapa penyerang dunia maya yang disponsori oleh beberapa negara bagian atau pengusaha telah terlibat dalam pencurian desain dan formula penemuan baru. Sebagian besar kegiatan ini disponsori oleh perusahaan pesaing dan perusahaan yang bersaing di bidang yang sama. Penyerang dunia maya diluncurkan untuk mengekstraksi informasi berharga dari organisasi yang ditargetkan.

Laporan Symantec mengungkapkan bahwa peretas komputer yang menggunakan server berbasis di AS milik seorang pemuda China (dijuluki 'Covert Grove') menyerang 29 perusahaan yang terlibat dalam penelitian, pengembangan, dan pembuatan bahan kimia dan bahan canggih. Tujuan utama serangan ini adalah untuk mengumpulkan kekayaan intelektual seperti dokumen desain, formula, dan proses

[42] What is Cyber Espionage and how can you prevent it? Cyberchasse.com/cyber-espionage/

[43] Hediej Nasheri, Economics Espionage, Cambridge University Press UK, 2005

manufaktur. Serangan itu berlanjut selama hampir dua bulan. Dia berhasil mencuri informasi berharga yang akan digunakan dalam produksi lokal.

Salah satu kelompok penyerang terkenal di China adalah TEMP.Periscope, atau Leviathan. Grup ini baru-baru ini meningkatkan serangan mereka dan menargetkan perusahaan AS di bidang teknik dan maritim yang terhubung dengan Laut China Selatan dan beberapa rute perdagangan tersibuk di dunia. Kelompok pelaku ancaman Tiongkok lainnya, APT10, disalahkan atas kampanye yang mungkin dimulai pada tahun 2009. Sebagai salah satu ancaman keamanan siber berkelanjutan terlama dalam sejarah, APT10 baru-baru ini menyerang perusahaan melalui penyedia layanan terkelola di berbagai industri di beberapa negara, seperti serta beberapa perusahaan Jepang, menyebabkan jumlah kerusakan yang tidak diketahui melalui pencurian data dalam jumlah besar.

d. **Serangan Cyber untuk Keuntungan Finansial.**

Serangan malware juga dapat digunakan untuk memperoleh data informasi pribadi orang-orang untuk mengakses bank, kartu kredit, dan kartu ATM mereka. Jaringan kejahatan dunia maya internasional menggunakan malware yang dikenal sebagai Zeus untuk menangkap data perbankan online dari perusahaan, kota, dan gereja menengah. Sebelum FBI dan lembaga penegak hukum lainnya menggagalkan operasi tersebut pada 2010, jaringan tersebut berhasil mencuri 70 juta dolar[44].

Korea Utara dilaporkan memiliki pasukan lebih dari 6.000 peretas yang mengumpulkan uang untuk membayar program nuklir negara itu. Serangan baru-baru ini yang dikaitkan dengan Korea Utara adalah APT37, yang menargetkan Korea Selatan, Jepang, Vietnam, dan Timur Tengah. Serangan itu konon dipimpin oleh kelompok peretas terkenal bernama Lazarus, yang telah aktif selama lima tahun terakhir ini. Grup tersebut telah dikutip atas serangan seperti Sony Pictures pada tahun

[44] PW Singer and Allen Friedman,Cyber Security and Cyberwar, Oxford University Press, 2014, UK

2014, yang meraup puluhan juta dolar, dan mungkin bertanggung jawab atas pencurian siber senilai $ 81 juta dari sebuah bank Bangladesh pada tahun 2016.

e. **Serangan untuk Menolak Layanan.**

Serangan Denial-of-Service (serangan DoS) atau serangan Distributed Denial-of-Service (serangan DDoS) adalah upaya untuk membuat mesin atau sumber daya jaringan tidak tersedia bagi pengguna yang dituju. Pelaku serangan DoS biasanya menargetkan situs atau layanan yang dihosting di server web profil tinggi seperti bank, gateway pembayaran kartu kredit, dan bahkan server nama root. Serangan DoS mungkin tidak terbatas pada metode berbasis komputer, karena serangan fisik strategis terhadap infrastruktur bisa sama menghancurkannya. Misalnya, memotong kabel komunikasi bawah laut dapat sangat melumpuhkan beberapa kawasan dan negara sehubungan dengan kemampuan peperangan informasi mereka. Serangan semacam itu telah dilakukan oleh Yahoo, e Bay, CNN dan Amazon.com. Serangan penolakan layanan terdistribusi (DDoS) menggunakan sistem komputer yang dikompromikan untuk mengatur banjir permintaan pada sistem target, menyebabkannya untuk menutup dan menolak layanan ke pengguna lain. Ini berpotensi digunakan untuk spionase ekonomi atau industri dengan tujuan sabotase. Metode ini diduga digunakan oleh dinas rahasia Rusia, selama dua minggu dalam serangan siber di Estonia pada Mei 2007, sebagai tanggapan atas penghapusan tugu peringatan perang era Soviet.

f. **Penghancuran Instalasi Vital.**

Beberapa malware tertentu memiliki kemampuan untuk membuat sistem tidak beroperasi untuk jangka waktu yang lebih lama atau secara permanen. Ini melibatkan penargetan sarana atau prasarana yang diandalkan orang. Memang, tindakan seperti itu menyebabkan kepanikan dan gangguan massal. Beberapa target umum termasuk jaringan listrik, sistem air, sistem keuangan, dll. Salah satu contoh penting adalah Stuxnet. Stuxnet adalah worm komputer berbahaya yang digunakan oleh militer Amerika sebagai bagian dari operasi yang berjudul Operation Olympic Game. Worm tersebut menyusup ke komputer pabrik dan dimaksudkan untuk menyabotase fasilitas

pengayaan uranium Iran. Karenanya, New York Times melaporkan bahwa Suxnet adalah "Serangan pertama terhadap infrastruktur industri penting yang menjadi fondasi ekonomi modern."

e. **Membalas Dendam.**

Serangan dunia maya dapat dimotivasi oleh perasaan dan sentimen yang keras terhadap suatu kelompok atau seseorang atau suatu negara bangsa. Setelah pemboman kedutaan besar China di Beograd oleh pejuang angkatan udara AS, para peretas China menyerang banyak situs AS untuk membalas ketidaksenangan mereka terhadap AS[45].

f. **Motivasi Terkait Masalah.**

Banyak tindakan perang dunia maya berasal dari agenda bermotif politik. Memang, sering kali tindakan aktivis disalahartikan sebagai perang dunia maya. Peretasan sebenarnya datang dari kelompok protes kecil, bukan dari aktor negara bangsa. Hacktivist akan sering berpartisipasi dalam metode gangguan klasik. Beberapa contoh termasuk DoS atau sabotase untuk menarik perhatian mereka atau menyebarkan ideologi mereka.

Grup seperti Anonim, Pasukan Kadal, dan Ahli Penipuan telah membantu membentuk serangkaian stereotip dan penerimaan campuran di antara warga sipil. Hacktivist sering menggunakan situs seperti Wikileaks untuk memposting informasi secara anonim yang mendukung ide dan keyakinan mereka, sering kali diterima secara beragam. Beberapa masalah politik seperti Kashmir dan Palestina adalah beberapa contoh yang akan memberikan pembenaran kepada penyerang dunia maya untuk menyerang situs web pemerintah India dan Israel. Kabarnya, Hizbullah juga menargetkan situs-situs Israel untuk membalas kekesalan mereka atas kebijakan mereka.

---

[45] Ellen Messmer, Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says,CNN.com, USA, May 12, 1999

g. **Peretasan Kesenangan.**

Beberapa ahli perangkat lunak yang baru lahir mungkin mengadopsi peretasan komputer untuk memuaskan ego mereka dan keinginan mereka untuk menunjukkan di antara penerapan keterampilan peretasan komunitas mereka dengan masuk ke komputer pribadi seseorang[46].

15. Strategi Cyber Ofensif

Untuk memahami operasi cyber secara umum dan sifat ofensif dari kemampuan ini, pemahaman tentang beberapa konsep dasar yang terkait dengan cyber warfare perlu dikembangkan. Penyerang siber akan mencari kerentanan sistem dan titik lemah untuk menciptakan efek spionase atau serangan siber yang diinginkan. Memanfaatkan kerentanan ini, prajurit dunia maya "mengakses" sistem yang diinginkan dan menyuntikkan sistem ini dengan muatan atau senjata yang dirancang khusus untuk menciptakan "efek" yang diinginkan.

Seorang peretas yang sukses akan dapat memperoleh akses ke data yang diinginkan dan akan berusaha mempengaruhi integritas atau ketersediaannya. “Kerahasiaan” data berarti menjaga data dari tangan mereka yang tidak berwenang untuk melihat atau mengaksesnya, “integritas” data mengacu pada pencegahan modifikasi / perubahan yang tidak sah pada data atau fungsi sistem.

“Ketersediaan” data berarti dapat diakses kapan pun diperlukan. Prinsip dasar ini mengatur sistem ITC dan keamanan data. Strategi balasan defensif akan menggunakan teknik ini untuk melindungi dari serangan dunia maya.

b. Strategi Dasar

[46] Dorthy E Denning , Information Warfare and Security, ACM Press, 1999

Memperoleh kenalan yang memadai tentang kerentanan, akses, muatan, dan efek terkait komputer. Pemahaman menyeluruh tentang beberapa strategi serangan siber dasar dapat dikembangkan yang akan membantu dalam merancang strategi siber defensif. Strategi ini dibahas dalam paragraf berikut:

1) **Tolak Akses.** Ini dicapai dengan menyerang perangkat keras atau sistem yang berisi data untuk menolak akses ke ini.

2) **Gangguan atau Kehancuran.** Gangguan dapat disebabkan oleh sistem yang mengumpulkan dan menyimpan data atau bagian dari sistem yang menyebarkannya. Padahal, hal tersebut dapat disebabkan oleh kerusakan fisik media penyimpanan atau rusaknya data sehingga menjadi tidak dapat dipulihkan pada waktu yang dibutuhkan agar berguna.

3) **Mencuri Data.** Jenis strategi ini diadopsi terhadap beberapa rahasia pribadi atau nasional yang sensitif seperti rencana atau rancangan militer.

4) **Manipulasi Data dan Sistem.** Dalam strategi manipulatif, penyerang dapat menambah, menghapus atau mengubah data atau perilaku pada sistem yang ditargetkan untuk memanfaatkan situasi baru. Seseorang yang melakukan penipuan atau sabotase dunia maya pasti sering menggunakan cara ini.

b. Implikasi Militer Dari Cyber Warfare

Munculnya komputer mengubah pasar sistem pertahanan. Produsen sistem militer menghabiskan jutaan dolar dalam penelitian untuk memasukkan prosesor komputer ke dalam sistem ini. Tujuan utama peralihan dari teknologi konvensional ke sistem berbasis komputer adalah teknologi baru yang menghasilkan sistem biaya rendah dengan kapasitas penanganan data yang besar. Selain itu, kemampuan pemrosesan kecepatan tinggi meningkatkan kapasitas penanganan data dengan kecepatan yang jauh lebih cepat. Meskipun, penggabungan komputer dalam peralatan

pertahanan telah memungkinkan mereka untuk menangani operasi tersebut lebih besar daripada yang sebelumnya.

Namun, kerentanan sistem ini telah meningkat. Hari ini mereka lebih rentan terhadap serangan dibandingkan dengan yang sederhana. Virus kecil atau kuda Troya dapat sangat mempengaruhi kemanjuran sistem ini. Penargetan lunak peralatan pertahanan sekarang menjadi pilihan yang lebih disukai melawan kerusakan keras. Pemahaman yang menyeluruh dan mendalam perlu dikembangkan terkait implikasi perang dunia maya ini. Pada paragraf-paragraf berikutnya, implikasi perang siber pada sistem militer akan dibahas secara detail.

1) **Pencurian informasi penting.** Informasi sensitif yang disimpan di hard disk komputer yang terhubung dengan internet dapat dikompromikan kapan saja oleh pejuang cyber dan peretas. Ancaman lain terhadap informasi ini mungkin berasal dari ancaman orang dalam. Operator orang dalam dengan akses ke peralatan sensitif mungkin bekerja untuk musuh; dia dapat mengekstrak data yang diperlukan dengan mudah untuk menyerahkannya kepada agen musuh.

2) **Penghancuran Sistem Pertahanan.** Sebagian besar peralatan militer diawasi oleh sistem SCADA (Supervisory Control and Data Acquisition) untuk menjaganya dari kerusakan, merekomendasikan pemeliharaan jadwal, membatasi operasinya di luar batasan yang ditentukan, dan mengoordinasikan fungsi sistem kerja yang berbeda.

Sistem ini dipasang di hampir semua sistem modern seperti radar, generator, pesawat terbang, pembangkit listrik, dan tank. Penyerang cyber musuh akan mencoba masuk ke sistem SCADA dari entitas yang ditargetkan dan mengganggu logika operasional SCADA atau membuat SCADA tidak berfungsi. Sistem kompleks modern tidak dapat beroperasi tanpa sistem pengawasan.

Contoh terbaik dalam hal ini adalah sistem FADEC[47] yang dipasang di mesin pesawat. FADEC adalah sistem yang terdiri dari komputer digital, yang disebut pengontrol mesin elektronik (EEC) atau unit kontrol mesin (ECU), dan aksesori terkaitnya yang mengontrol semua aspek kinerja mesin pesawat. Ini memastikan bahwa mesin beroperasi pada tingkat optimal dan mengganggu saat operator melampaui batas berbahaya.

Kontrol mesin digital otoritas penuh sejati tidak memiliki bentuk pengesampingan manual yang tersedia, menempatkan otoritas penuh atas parameter pengoperasian mesin di tangan komputer. Mematikan atau tidak tersedianya FADEC pada mesin dapat menyebabkan kehancurannya. Contoh terbaru adalah penghancuran sentrifugal nuklir Iran dengan virus "Stuxnet".

3) **Memperlambat Loop OODA.** Pusat manajemen pertempuran modern semuanya berbasis komputer. Tentakel dan sensor lapangan dihubungkan dengan pusat-pusat ini untuk penyediaan informasi medan pertempuran penting tentang aktivitas musuh. Melalui aliran cepat sentrisitas bersih informasi di antara anggukan dipastikan untuk pengambilan keputusan tanggapan yang cepat dan pembuangan cepat ancaman oleh penembak. Untuk menjelaskan lebih lanjut, radar dan sensor lain yang dihubungkan dengan eselon atas akan mentransfer informasi penting tentang aktivitas musuh melalui jaringan komunikasi.

Manajer pertempuran yang duduk di pusat-pusat ini akan memiliki gambaran gabungan. Selalu ada kemungkinan bahwa sistem ini mungkin terinfeksi malware atau Trojan horse dengan beberapa stik USB yang terinfeksi. Pada beberapa titik kritis, virus ini dapat menyerang prosesor di pusat manajemen pertempuran membuat mereka tidak mampu atau terdegradasi ke tingkat di mana respons yang diperlukan tertunda. Respon yang tertunda dianggap tidak ada respon, sehingga musuh dapat memberikan kerusakan tanpa terluka oleh musuh.

[47] Federal Aviation Agency, FADEC, https://go.usa.gov/xn89k

4) **Kekacauan dan Kebingungan.** Dalam situasi perang dan kontigensi operasional, pusat komando dan kendali menjadi pusat saraf karena pusat-pusat ini umumnya diawaki oleh pejabat tinggi. Serangan dunia maya terhadap pusat semacam itu dapat membuat mereka tidak efektif. Akibatnya, kebingungan dan kekacauan akan terjadi jika musuh dapat menargetkan pusat komando dan kendali kita; yang sangat tidak diinginkan terutama pada saat-saat kritis. Kebingungan dan ketidaktegasan pada level ini pasti akan mempengaruhi moral dan kemampuan bertarung dari eselon bawah.Keuntungan dari strategi ini adalah sebagian besar waktu berjalan tanpa disadari.

5) **Pengaruh pada Sistem Komunikasi.** Radio komunikasi modern yang tersedia di pasar semuanya berbasis perangkat lunak. Radio ini dapat dengan mudah dikonfigurasi oleh pengguna sesuai kebutuhan mereka dengan kode enkripsi. Selain itu, radio ini juga digunakan untuk konektivitas data link antara pemain udara dan darat. Radio semacam itu juga akan menjadi salah satu target para pejuang dunia maya.

Kesalahan kecil perangkat lunak yang dimasukkan ke terminal ini, dapat memengaruhi kinerja seluruh tim pembuat perang. Jenis serangan ini jika digabungkan dengan serangan elektronik (Communication Jamming) akan menghasilkan bencana bagi kelompok militer yang menjadi sasaran. Selain itu, perlu juga disebutkan pada titik ini bahwa pengganda kekuatan seperti platform AWACS terhubung dengan pusat bumi melalui radio.

Radio yang terinfeksi virus juga akan mengeluarkannya dari kemanjurannya akan sangat berkurang. Pertukaran telepon dan sistem pengiriman surat juga dapat terpengaruh oleh serangan dunia maya.

6) **Pengaruh pada Armada Pesawat Tempur.** Pesawat tempur generasi ketiga dan keempat dilengkapi dengan avionik terbaru dan radar AI. Fungsi sistem ini dipantau dan dikelola melalui perangkat lunak dan prosesor yang kompleks. Filosofi

pemeliharaan dan operasional platform ini didasarkan pada perangkat lunak komputer yang dirancang khusus untuk mereka. Pilot dan insinyur berinteraksi dengan platform ini melalui perangkat lunak yang disesuaikan. Instruksi penting seperti rute penerbangan, instruksi senjata dan amunisi dan perencanaan dimasukkan ke dalam pesawat tempur melalui USB dan disk.

Demikian pula, jadwal perawatan dan pemeriksaan juga dikelola melalui perawatan komputer dan laptop. Pejuang cyber yang ahli akan mengeksploitasi perangkat input ini untuk merusak logika perangkat lunak platform ini. Mesin modern tanpa peralatan yang berfungsi ini adalah platform besi yang tidak berguna.

7) **Mematikan Jaringan Listrik Militer.** Cara termudah untuk menurunkan kekuatan militer musuh adalah dengan menargetkan pembangkit listrik mereka. Kekurangan pasokan listrik komersial akan dipenuhi dari pembangkit listrik. Hal ini akan menjadi beban tambahan pada bahan bakar, pelumas, dan dukungan logistik tambahan terutama untuk daerah yang berjauhan. Pelaksanaan operasi berkelanjutan pada generator juga akan meningkatkan keausannya terutama selama cuaca buruk.

8) **Menghasilkan False Signaling di Intranet.** Komunikasi internal dalam organisasi militer dilakukan melalui jaringan loop tertutup yang disebut intranet. Meskipun jaringan semacam ini dan tidak berkomunikasi dengan orang luar, namun, sangat mungkin bahwa beberapa penyusup dapat masuk ke jaringan ini dan menyebarkan berita palsu dan menghasilkan instruksi yang salah untuk formasi yang lebih rendah. Dia juga dapat mengirimkan status peralatan operasional yang tidak akurat ke komando yang lebih tinggi yang dapat mempengaruhi pengambilan keputusan kritis. Basis data yang berbeda mengenai peralatan operasi, kesehatan dan logistik dapat diubah untuk mempengaruhi pengambilan keputusan.

d. Implikasi Ekonomi dari Cyber Warfare

Perang siber akan mempengaruhi entitas ekonomi dengan besaran yang sama dengan yang menjadi sasaran elemen militer. Tidak seperti sistem militer di mana entitas dilindungi dengan baik secara fisik dan tidak tersedia akses internet, organisasi komersial adalah mangsa empuk bagi peretas, pencuri dunia maya, dan penjahat dunia maya. Organisasiorganisasi ini harus menghadapi jutaan malware dan trojan horse setiap tahun yang dibuat untuk digunakan untuk tujuan tertentu. Cyber warriors akan menargetkan jaringan listrik, sistem transpirasi, sistem komunikasi, bank, bursa saham, industri, dan fasilitas R&D. Implikasi perang dunia maya dalam bidang ekonomi dibahas secara rinci:

1) **Spionase Cyber.** Negara-negara maju seperti Amerika Serikat, Jepang dan Perancis telah menjadi korban spionase dunia maya. Sebelum munculnya komputer, spionase dilakukan oleh operator intelijen manusia yang biasa mencuri rahasia dagang dan desain paten dari organisasi terkemuka dan kompetitif.

Alasan spionase cyber adalah akses ke teknologi dengan cara yang mudah. Penelitian dan pengembangan membutuhkan investasi modal yang besar dari negara bagian dan organisasi. Namun, jika teknologinya bisa diakses tanpa mengeluarkan banyak biaya, maka ideologi pencurian harus diupayakan. Internet semakin memungkinkan para pemburu dunia maya untuk mencuri informasi komersial yang sensitif, teknologi yang sangat rahasia seperti senjata luar angkasa dan militer.

Ada dua jenis spionase, satu Spionase Industri dan yang lainnya adalah pencurian Hak Kekayaan Intelektual. Pencurian hak kekayaan intelektual dan Pelanggaran termasuk penyalinan ilegal, distribusi atau penjualan perangkat lunak, permainan, film, musik dan kekayaan intelektual lainnya. Selain itu, jenis spionase ini dapat dilakukan oleh negara-negara yang ingin memperoleh informasi mengenai beberapa teknologi canggih. Sedangkan spionase industri dilakukan oleh beberapa organisasi individu yang mungkin mencuri beberapa desain teknologi baru dari pesaingnya.

Pada tahun 2007, FBI melaporkan bahwa ada 108 negara dengan organisasi penyerang dunia maya khusus yang mencari rahasia industri. Basis data telah menjadi target yang disukai para penjahat dunia maya dan negara-bangsa. Kantor Kabinet Inggris melaporkan pencurian kekayaan intelektual dan biaya spionase industri sebesar £ 16,8 miliar pada tahun 2012.

Laporan Investigasi Pelanggaran Data (DBIR) Verizon 2012 melaporkan 855 insiden pelanggaran keamanan di jaringan industri dan perusahaan, dengan total 174 juta catatan yang disusupi di seluruh AS, Inggris, Belanda, Irlandia, dan Australia. Dari 855 insiden yang diinvestigasi oleh DBIR ini, 92% tidak ditemukan hingga pihak luar mengungkapkannya[48].

2) **Pencurian ID Pribadi.** Penjahat dunia maya profesional akan mengadopsi berbagai cara dan sarana untuk mencuri informasi pribadi seperti alamat email, kata sandi, nomor kartu kredit, dan kata sandi. Saat ini terlalu banyak orang yang memiliki akses ke informasi tentang identitas orang lain. Konsumen tidak berdaya terhadap ini dan berbagai teknik digunakan untuk mengekstrak informasi pribadi.

Mencuri nama pengguna dan sandi seseorang seperti mencuri kunci mobil seseorang, membuka mobil dengan kunci yang dicuri tidak akan menghasilkan alarm apa pun bagi keamanan. Belanja online adalah cara lain yang menunjukkan informasi pribadi orang-orang di web. The Times of India melaporkan bahwa Hacker, yang menyebut diri mereka Evil Shadow Team dan dilaporkan berbasis di China menyerang www.microsoftstore.co.in mencuri ID login dan password orang-orang yang telah menggunakan situs tersebut untuk berbelanja.

Menurut laporan, ID dan kata sandi disimpan dalam file teks biasa tanpa enkripsi apa pun. Evil Shadow kemudian memposting pesan di situs Microsoft, mengatakan "sistem

[48] M. E. Kabay, Industrial Espionage,Phd thesis, 2008

yang tidak aman akan dibaptis". Perbankan dan transaksi online adalah cara lain untuk mengekspos klien bank kepada pencuri dunia maya yang akan mengeksploitasi lubang loop di sistem untuk memeras uang.

3) **Penipuan melalui ID yang Dicuri.** Pencuri dunia maya menggunakan ID yang dicuri untuk melakukan kejahatan keuangan seperti transfer dana ilegal dari akun korban. Dalam beberapa kasus, ID yang dicuri ini telah digunakan untuk melakukan belanja online. Meskipun, bank memastikan perlindungan yang memadai terhadap transaksi yang melanggar hukum tetapi terkadang tindakan pencegahan keamanan ini dilanggar oleh ahli pencuri dunia maya. Pedagang mewah "Neiman Marcus" Sabtu mengonfirmasi bahwa pencuri mencuri beberapa informasi kartu pembayaran pelanggannya dan membuat tagihan tidak sah selama musim liburan, menjadi pengecer kedua dalam beberapa pekan terakhir yang mengumumkan telah menjadi korban serangan keamanan siber.

4) **Mematikan Jaringan Listrik.** Jaringan Listrik adalah sistem vital suatu negara. Pasokan listrik berkelanjutan dipastikan melalui manajemen jaringan yang efisien melalui SCADA. Menyerang sistem ini, akan membuat negara menjadi gelap dan sejumlah sistem dan fasilitas terkait akan berhenti berfungsi.

Pemadaman listrik ini akan memengaruhi fungsi komputer, kereta api, rumah sakit, dan layanan telekomunikasi serta infrastruktur vital lainnya. Ini mewakili target istimewa untuk serangan dunia maya, dan pertahanan mereka merupakan hal mendasar dalam setiap strategi dunia maya. Dalam skenario masa depan apa pun, peperangan konvensional akan ditingkatkan dengan menyerang target ini.

5) **Memanipulasi Sistem Rumah Sakit.** Di sebagian besar negara, rumah sakit dikelola melalui sistem manajemen rumah sakit yang baik. Basis data dan peralatan yang berbeda dihubungkan pada jaringan untuk memudahkan akses dan fungsi. Penyerang dunia maya juga dapat menargetkan sistem manajemen rumah sakit untuk meningkatkan tingkat kesulitan bagi pemerintah selama kemungkinan apa pun. Ini

akan sangat menurunkan semangat orang ketika mereka melihat bahwa pasien tidak dirawat di rumah sakit seperti yang diharapkan.

6) **Sistem Pengendalian Fasilitas Kritis.** Sistem Supervisory Control And Data Acquisition (SCADA) umumnya bertanggung jawab untuk menjalankan mesin dan peralatan modern. SCADA memungkinkan mesin dan pabrik ini untuk dikelola dan dijalankan secara mandiri dan dari jarak jauh. Penyerang dunia maya dapat memasuki sistem ini dan mengganggu logika operasional SCADA terkait.

Penyerang dapat membahayakan sistem manajemen pabrik kimia di situs nuklir, mengubah proses produksi, dan mengekspos area yang luas pada risiko kehancuran.

Pada tahun 2007, situs nuklir Iran menjadi sasaran malware bernama Stuxnet. Malware ini bertanggung jawab untuk mengontrol fungsi operasi sentrifugal pemantauan SCADA. Logika yang salah dimasukkan ke dalam sistem yang mengakibatkan kerusakan hampir 1000 sentrifugal.

7) **Sistem Distribusi dan Pembersihan Air.** Distribusi dan pembersihan air sekali lagi dikelola oleh sistem otomatis yang memastikan jumlah bahan kimia yang diperlukan untuk dicampur untuk pembersihan dan distribusi tepat waktu. Gangguan pasokan dapat menyebabkan area yang luas tanpa air. Selain itu, perubahan rasio pencampuran bahan kimia dengan air dapat membuatnya tidak layak untuk dikonsumsi manusia.

8) **Memanipulasi Sistem Transportasi.** Sistem sinyal lalu lintas jalan raya dan sistem transportasi kereta api diatur oleh sistem otomatis. Penyerang dunia maya dapat membuat malapetaka dengan mengganggu sistem manajemen ini. Menampilkan sinyal hijau ke segala arah di jalan yang ramai tentunya akan mengakibatkan kecelakaan dan malapetaka.

Pemblokiran Perbankan dan Sistem keuangan. Sistem keuangan merupakan aset penting bagi suatu negara dan bloknya dapat menyebabkan masalah serius, seperti terhambatnya kegiatan ekonomi sasaran. Meskipun tidak dapat menyebabkan hilangnya nyawa manusia secara langsung, serangan dunia maya dapat menyebabkan keruntuhan finansial suatu negara. Skenarionya mengkhawatirkan; Jika kita berpikir bahwa keuangan global saat ini sangat bergantung pada ekonomi masing-masing negara, serangan dunia maya terhadap suatu negara dapat menyebabkan konsekuensi yang serius dan tidak dapat diprediksi ke seluruh sistem ekonomi.

16. Analisis

a. Munculnya komputer telah merevolusi filosofi kerja dan telah menunjukkan pergeseran paradigma dalam domain komersial maupun militer.

b. Komputer tidak hanya mengubah proses berpikir para pemikir dan ahli strategi militer, tetapi juga membawa perubahan mendasar dalam semua aspek kehidupan kita.

c. yang muncul- internet adalah produk sampingan dari evolusi jaringan komputer telah benar-benar mengubah dunia menjadi desa global, dengan semua bagian dunia terhubung ke jaringan besar.

d. Saat ini, ada hampir 8,7 miliar perangkat yang terhubung di internet yang bertukar 40 triliun email setiap tahun

e. Penggunaan internet telah meluas ke rumah sakit, jaringan listrik, bursa saham, sistem komunikasi dan transportasi

f. Web komputer yang dihasilkan di tingkat global disebut sebagai ruang cyber.

g. Karena jaringan komputer dan internet dirancang dengan tujuan utama untuk memberikan kemudahan akses informasi, hemat biaya dan efisiensi bagi banyak orang, ia kekurangan fitur keamanan yang diperlukan untuk mencegah masuknya pengguna yang tidak diinginkan.

h. Ketersediaan informasi vital dan sangat besar di ruang cyber telah membuatnya rentan terhadap serangan dunia maya oleh aktor non-negara dan berbasis negara.

i. Peperangan siber telah muncul sebagai peperangan paling penting di masa kini dan dinyatakan sebagai ranah peperangan kelima.

j. Sebagian besar negara maju yang bersaing dalam domain politik, ekonomi, dan militer telah menggunakan cara siber untuk mengalahkan satu sama lain.

k. AS, Prancis, Jerman, dan Inggris telah membentuk pasukan Cyber untuk menciptakan operasi berbasis efek.

l. Dua dekade terakhir telah menyaksikan banyak insiden perilaku operasi perang dunia maya oleh aktor negara dan non-negara baik di domain militer dan ekonomi di seluruh dunia.

m. Kurangnya konsensus mengenai standarisasi berbagai terminologi dan cakupannya terkait dengan perang siber antar berbagai negara menjadi kendala dalam perumusan kerangka hukumnya.

n. Serangan dunia maya dalam peran DoS terutama di wilayah yang masyarakat umum dan massa terpengaruh akan menghasilkan efek psikologis ketidakpercayaan terhadap kepemimpinan mereka.

o. Di tingkat nasional, pemerintah bersinkronisasi dengan swasta dan pemangku kepentingan lainnya dapat membuat strategi keamanan siber. Pusat komando keamanan siber nasional dirasa perlu untuk bertindak sebagai penghubung di antara berbagai pemangku kepentingan.

p. Di tingkat internasional, negara-negara koalisi dapat menggagalkan ancaman melalui kerja sama yang erat dan upaya bersama dengan berbagi informasi dan keahlian.

BAB IV
PENUTUP

17. Simpulan

Pengguna internet sekarang berjumlah milyaran dan lebih dari empat milyar komputer, server, router, switch dan modem terhubung. Penggunaan internet yang meningkat telah memberikan lebih banyak kesempatan kepada penjahat untuk memanfaatkan situasi ini. Bidang siber yang selalu berubah dan terus berkembang menuntut pembaruan terus-menerus pada teknologi dan keterampilan siber yang lebih baik. Oleh karena itu, masalah ini tidak lagi hanya untuk departemen TI tetapi untuk seluruh organisasi. Keterampilan dunia maya perlu menjangkau setiap profesi.

Ancaman dunia maya adalah ancaman yang tidak bisa dihilangkan sama sekali. Teknologi digital bekerja karena terbuka, dan keterbukaan itu membawa risiko. Apa yang dapat kami lakukan adalah mengurangi ancaman ke tingkat yang memastikan kami tetap berada di garis depan revolusi digital.

Pemerintah sendiri tidak dapat menyediakan semua aspek keamanan dunia maya negara. Strategi yang tertanam dan berkelanjutan diperlukan di mana warga, industri, dan mitra lain dalam masyarakat dan pemerintah, memainkan peran penuh mereka dalam mengamankan jaringan, layanan, dan data kami.

Lebih penting lagi, selama bertahun-tahun sistem militer juga menjadi sasaran para pejuang dunia maya. Malware kecil yang dimasukkan ke dalam sistem C4I dapat menyebabkannya tidak dapat beroperasi pada titik kritis operasi. Ancaman dianggap sangat mematikan dan efektif dengan melibatkan lebih sedikit sumber daya dan upaya. Namun, kemanjuran dan sifat mematikannya dapat dikurangi dan disusutkan dengan menerapkan tindakan balasan yang komprehensif pada pembentukan militer serta entitas ekonomi.

Komunitas internasional harus bekerja sama untuk menyusun prosedur, hukum, aturan dan keluar dunia maya dengan mekanisme untuk memerangi ancaman dunia maya secara efektif dalam semua manifestasinya. Negaranegara yang dicurigai mensponsori spionase dan serangan dunia maya harus bekerja sama dengan komunitas dunia untuk mengekang ancaman ini. Tantangan terbesar bagi perdamaian dunia adalah mengontrol penggunaan internet oleh teroris dan penjahat. Ini adalah tanggung jawab semua negara untuk bekerja sama dan berkoordinasi untuk menangkap pencuri dunia maya dan teroris. Forum khusus di tingkat PBB dapat menjadi pilihan yang baik dalam menangani masalah yang berkaitan dengan kejahatan dunia maya.

18. Rekomendasi

Berdasarkan studi penelitian saya, saya ingin merekomendasikan beberapa tindakan yang mungkin dapat membantu dalam melawan efek serangan dunia maya baik di bidang militer maupun ekonomi. Langkah ini perlu dilaksanakan dan diambil di tingkat nasional dan organisasi untuk melawan atau mengurangi efektivitasnya.

a. Level Nasional

1) **Perumusan Strategi Pengembangan Cyber.** Pemerintah sendiri tidak dapat menyediakan semua aspek keamanan dunia maya negara. Strategi yang tertanam dan berkelanjutan diperlukan di mana warga, industri, dan mitra lain dalam masyarakat dan pemerintah, memainkan peran penuh mereka dalam mengamankan jaringan, layanan, dan data kami. Strategi harus bertujuan untuk mencapai sektor keamanan siber yang dinamis dan basis keterampilan pendukung yang dapat mengimbangi dan maju dari ancaman yang berubah. Strategi ini juga harus menawarkan visi yang koheren dan menarik untuk dibagikan dengan sektor publik dan swasta, masyarakat sipil, akademisi, dan populasi yang lebih luas. Itu juga harus melayani tujuan berikut:

2) **Meningkatkan Keterampilan Cyber.** Kami kurang memiliki keterampilan dan pengetahuan untuk memenuhi kebutuhan keamanan dunia maya kami di sektor publik dan swasta. Dalam bisnis, banyak anggota staf tidak sadar akan keamanan dunia maya dan tidak memahami tanggung jawab mereka dalam hal ini, sebagian karena kurangnya pelatihan formal. Publik juga kurang sadar dunia maya. Kami juga perlu mengembangkan keterampilan dan kemampuan khusus yang akan memungkinkan kami untuk mengimbangi teknologi yang berkembang pesat dan mengelola risiko dunia maya terkait. Kesenjangan keterampilan ini mewakili kerentanan nasional yang harus diselesaikan.

3) **Gradasi sistem Legacy ke atas.** Banyak organisasi terus menggunakan sistem lama yang rentan hingga peningkatan TI berikutnya. Perangkat lunak pada sistem ini sering kali mengandalkan versi lama yang belum ditambal. Versi lama ini sering mengalami kerentanan yang dicari penyerang dan memiliki alat untuk dieksploitasi. Masalah lainnya adalah penggunaan perangkat lunak yang tidak didukung oleh beberapa organisasi, yang tidak memiliki rezim penambalan.

4) **Kebijakan Cyber.** Kebijakan siber harus menjadi dokumen pedoman tentang hal-hal yang berkaitan dengan perlindungan sistem siber. Selain itu, harus dengan jelas menjelaskan tanggung jawab dan otoritas elemen yang berbeda dan memberikan jalan ke depan untuk ancaman yang dibayangkan. Kebijakan ini juga harus membantu menyempurnakan kebijakan keamanan nasional sambil menangani ancaman dunia maya terhadap militer serta sistem komersial.

5) **Pusat Keamanan Siber Nasional.** Ini harus menjadi platform tingkat nasional yang secara khusus menjaga ancaman dunia maya. Platform ini harus bertanggung jawab untuk memandu pemerintah yang duduk pada kebijakan dan rekomendasi tentang masalah yang berkaitan dengan ancaman dunia maya. Fasilitas pemantauan harus tersedia di organisasi bergengsi ini untuk memburu lalu lintas ilegal di jaringan. Komando ini harus diawaki oleh personel militer dan sipil yang sangat terampil dan berkualitas. NCSC akan menyediakan hal berikut:

a) Sumber nasihat terpadu untuk intelijen ancaman keamanan siber Pemerintah dan jaminan informasi;
b) Wajah publik yang kuat dari tindakan Pemerintah terhadap ancaman dunia maya - bekerja sama dengan industri, akademisi, dan mitra internasional untuk menjaga negara terlindungi dari serangan dunia maya.
c) Penyiapan harus memiliki sistem firewall terbaru, tangguh, dan canggih yang dapat mencegah serangan cyber secara efisien.

6) **Deteksi Intrusi.** Pada tingkat negara bagian beberapa sistem deteksi intrusi dapat dikembangkan untuk melacak dan menangkap pencuri dunia maya.

7) **Kekuatan perang cyber (Serangan & Defensif).** Di bawah bimbingan komando dunia maya, kekuatan siber ofensif dan defensif yang berdedikasi harus dibentuk. Kekuatan pertahanan harus dipercayakan untuk melindungi sistem cyber sendiri, sedangkan elemen ofensif harus memiliki keahlian dalam menargetkan sistem sipil dan militer musuh.

8) **Perumusan Hukum untuk Kejahatan Cyber.** Di sebagian besar negara, undang-undang khusus untuk kejahatan dunia maya tidak ada, oleh karena itu pemerintah yang bersangkutan harus merumuskan undang-undang yang mengatur pengoperasian perang dunia maya.

9) **Mendidik Massa dan Badan Penegakan Hukum:** Pengetahuan massa secara umum dan penegakan hukum pada khususnya sangat buruk. Kesadaran di antara kedua komunitas dapat ditingkatkan dengan seminar, ceramah dan kursus pelatihan. Pengembang perangkat lunak muda juga dapat dididik untuk tidak mengadopsi kesenangan peretasan hanya untuk membuktikan keberanian mereka. Sebagian besar siswa muda tidak memahami bahwa peretasan berarti mengganggu privasi tubuh dan sama dengan pencurian. Institusi pendidikan

harus menjadikannya bagian dari kurikulum mereka untuk melakukan pembinaan siswanya dalam hal ini.

b. Tingkat Organisasi

1) Keamanan fisik peralatan TIK harus dijamin untuk melindunginya dari kerusakan fisik jika terjadi serangan sabotase.

2) Masuknya personel yang tidak sah harus diperiksa untuk mengurangi kemungkinan penyuntikan virus oleh agen musuh di peralatan TIK.

3) Semua sistem komputer dan aksesorinya, hard disk, USB dan disket harus dilindungi dengan perlindungan kata sandi yang kuat untuk menghilangkan kemungkinan gangguan sistem dan data.

4) Sistem harus dilindungi dengan perangkat lunak antivirus yang asli, bagus, dan diperbarui.

5) Perlindungan firewall harus diaktifkan di semua sistem.

6) Slot dan perangkat input dan output adalah penyebab utama sistem TIK menjadi sasaran penyerang dunia maya. Akses perangkat input / output harus diblokir.

7) Ancaman orang dalam dalam organisasi akan menjadi sumber utama spionase dunia maya atau serangan dunia maya terutama dalam sistem militer. Semua personel yang bekerja di area sensitif perlu mendapat izin keamanan dan pengawasan yang sangat ketat harus dilakukan. Konsep manajer keamanan cyber harus diterapkan di bidang militer dan komersial untuk menjaga area spesifik ini.

8) Perangkat lunak bajakan dapat dengan mudah menjadi sasaran malware dan virus. Ini adalah wajib bahwa hanya perangkat lunak asli yang diinstal pada sistem kritis.

c. Sistem Militer

1) **Sistem Siaga.** Sistem militer yang merendahkan akan memiliki efek yang menghancurkan pada respon kekuatan secara keseluruhan terhadap tindakan musuh. Prosedur siaga, peralatan, dan sistem komunikasi wajib ada untuk melengkapi operasi militer. Dalam kasus lingkungan yang rusak, operasi harus segera dialihkan dari sistem yang terinfeksi ke sistem siaga untuk kelancaran operasi.

2) **Memisahkan Jaringan Militer dari Internet.** Peralatan TIK militer tidak boleh terhubung dengan internet. Jaringan militer dapat dilakukan pada jalur khusus yang membuat jaringan loop tertutup tanpa akses ke pihak luar. Menyerang jaringan loop tertutup adalah proposisi yang sulit bagi penyerang dunia maya.

3) **Perlengkapan dan Aksesori Spesifikasi Militer.** Perlengkapan dan aksesori spesifikasi militer harus digunakan untuk sistem C4I militer. Peralatan ini harus dibeli dari vendor terkenal dan sebelum digunakan untuk militer, perangkat keras ini harus diperiksa untuk Backdoors dan Chippings.

4) **Perlindungan Tingkat Bidang dari Fisik Nod.** Net Centric Warfare akan menuntut banyak terminal komunikasi lapangan untuk kelancaran aliran data antar elemen. Penyerang dunia maya dapat menargetkan sistem ini untuk menginfeksi seluruh sistem dengan virus dan malware. Personil yang melakukan tugas di lokasi lapangan harus dididik tentang serangan tersebut.

5) **Perangkat Lunak Enkripsi yang Dikembangkan Sendiri.** Perangkat lunak enkripsi tanpa kode sumber terdiri dari perangkat lunak dan dapat didekripsi kapan saja oleh prajurit cyber. Perangkat lunak enkripsi asli harus dikembangkan yang harus digunakan pada sistem kritis.

6) **Dokumentasi Setiap Kegiatan.** Setiap aktivitas yang dilakukan saat menggunakan peralatan TIK harus didokumentasikan dengan baik oleh orang yang bertanggung jawab. Jika beberapa software up gradation atau maintenance telah dilakukan, maka harus login dengan detail yang lengkap. Catatan akan membantu kami dalam memastikan dan menangkap pelaku jika sistem mulai berperilaku buruk.

7) **Pembuangan Hard Disk Lama dan Perangkat Portabel dengan Benar.** Hard disk lama dengan data rahasia harus dihancurkan dengan membakar.

8) **Dokumen Rahasia hanya dalam bentuk Hard Copy.** Data lunak dapat dengan mudah diakses oleh siapa pun jika tidak dilindungi dengan baik. Namun, jika tidak dicuri, itu dapat dihapus atau diubah oleh penyerang dunia maya. Data rahasia harus disimpan dalam bentuk hard copy dan diamankan dengan baik.

d. **Entitas Ekonomi / Komersial**

1) SCADA yang Lebih Kuat dan Kuat. Firewall generasi selanjutnya harus dipasang untuk menciptakan keamanan di sekitar SCADA. Selain itu, firewall ini juga akan mengisolasi proses dari seluruh jaringan dan membuat hub keamanan. Prosedur akses ke SCADA online dapat dibuat rumit dengan mengintegrasikan prosedur otentikasi yang ketat dan izin pengguna terbatas. Jika ada ancaman serangan yang akan segera terjadi, akses internet mungkin ditolak ke sistem ini untuk tujuan keamanan.

2) Bank dan sistem keuangan harus menyewa jasa insinyur perangkat lunak ahli. Mereka harus dapat memberikan solusi yang baik terhadap pencurian cyber.

3) Pencurian keuangan online dapat sangat dikurangi dengan integrasi sistem identifikasi Biometrics. Semua transaksi harus dikenakan identifikasi biometrik. Konsumen saat melakukan transaksi online harus diminta untuk sidik jari dan Identifikasi Retina dan Iris. Prosedur ini dapat mengurangi pencurian cyber secara luas.

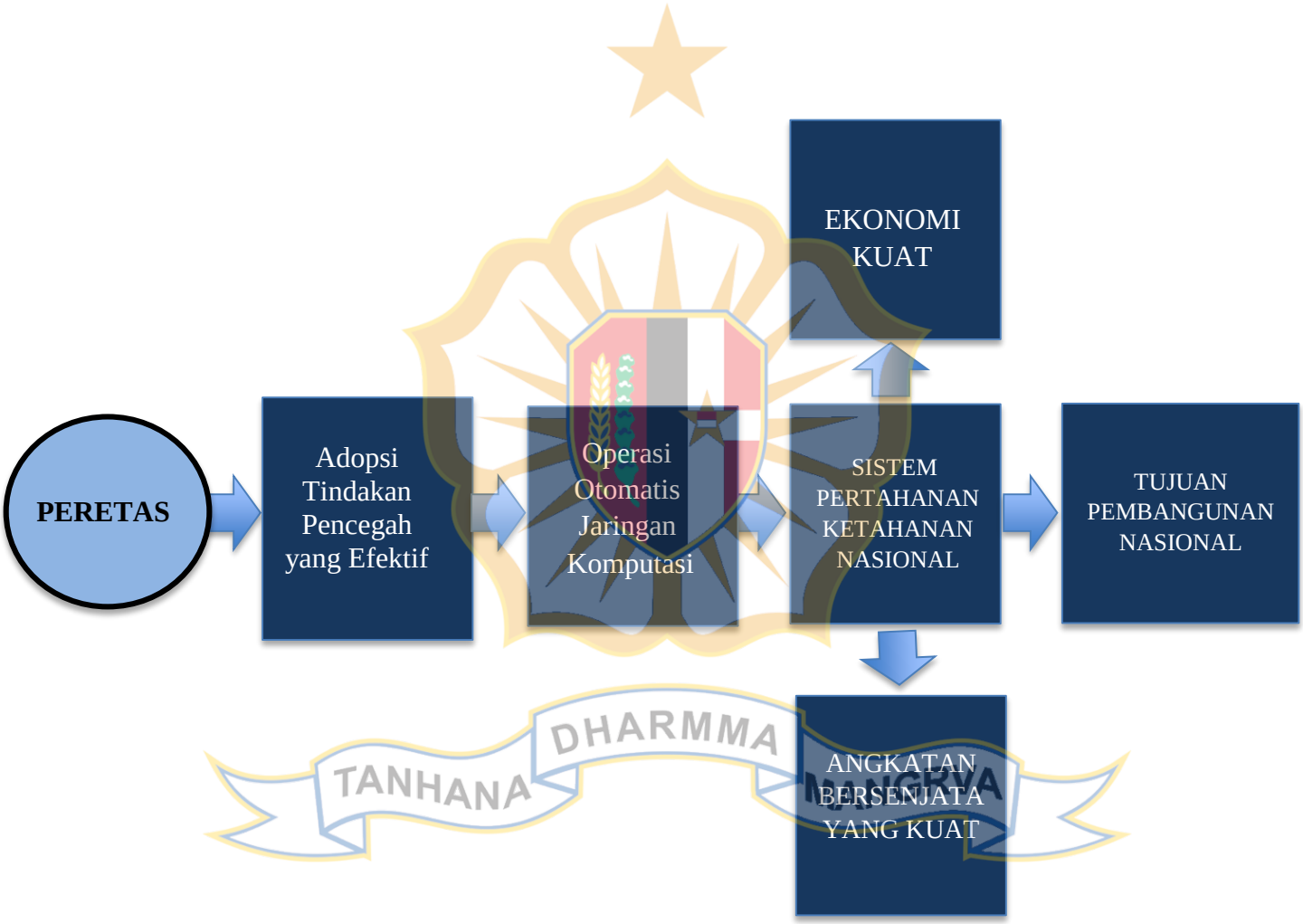
4) Audit keamanan sistem harus dilakukan secara konsisten oleh seorang ahli untuk mengatasi setiap pelanggaran keamanan cyber.

DAFTAR PUSTAKA

- Albert Einstein, Ideas and Opinions,1954.
- Arquilla, John, "Can information warfare ever be just?" Ethics and Information Technology,
- Candid Wueest, Internet Security Threat Report, Financial Threats Review, 2017
- Carl von Clausewitz, On War, ed. and trans. Michael Howard and Peter Paret, Princeton, NJ: Princeton University Press, 1976
- Dorthy E Denning , Information Warfare and Security, 1999
- Dr. Chase Cunningham, Cyber Warfare – Truth, Tactics, and strategies, 2020
- FBI, CIA and NSA joint report, Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution, 2017
- Federal Aviation Agency, FADEC, https://go.usa.gov/xn89k
- Fred Kaplan, Dark Territory: The Secret History of Cyber War, New York, America, 2016
- Giulio Douhet, The Command of the Air, 1921, trans. Dino Ferrari. (1942; new imprint Washington, DC: Office of Air Force History, 1983)
- Green, James A., Cyber warfare: a multidisciplinary analysis, November 2016.
- Hathaway, supra note 36, page 825 (quoting Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, Dec. 2, 2008, Annex 1, at 209 [hereinafter SCO Agreement]).
- Hediej Nasheri, Economics Espionage, 2005
- Herzog, Stephen. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, Journal of Strategic Security 4, no. 2, 2011
- Industrial Espionnage Cyber Style- Financial Times
- Jeffery Carr, Inside Cyber Warfare, 2012

- M. E. Kabay, Industrial Espionage, Phd thesis, 2008
- M. Gercke ,Understanding Cyber Crime: A Guide for Developing Countries, ITU-D ICT Applications and Cybersecurity Division, 2011
- Paul Rosenzweigh, Cyber warfare: How Conflicts in Cyber Space are Challenging America and Changing the World, 2013
- Practioners Jason Andress & Steve Winterfeld, Cyber warfare: Technique, Tactics for Security, 2014
- PW Singer and Allen Friedman, Cyber Security and Cyberwar, 2014
- Richard A. Clarke & Robert K Knake, Cyber War: The Next Threat to National Security and What to Do About It, 2010
- Shakarian, Paulo, Introduction to cyber-warfare: a multidisciplinary approach.
- USAF Doctrine-Cyber Space Operations 3-12,2006
- What is Cyber Espionage and how can you prevent it? Cyberchasse.com/cyber-espionage/
- William Gibson, Neuromancer, Hachette UK, 2016
- Wing Commander MK Sharma, Cyber Warfare, The Power of the Unseen, 2011
- Zaigham Mehmood, Data Science and Big Data Computing, 2016

ALUR PIKIR


PERETAS
Adopsi Tindakan Pencegah yang Efektif
Operasi Otomatis Jaringan Komputasi
EKONOMI KUAT
SISTEM PERTAHANAN KETAHANAN NASIONAL
TUJUAN PEMBANGUNAN NASIONAL
ANGKATAN BERSENJATA YANG KUAT

TABEL

TABEL 1. Kasus serangan cyber utama

Entitas yang Bermusuhan	**Entitas Sasaran**	**jangka waktu**	**Deskripsi Kegiatan Singkat**
AS, Israel	Iran	2008-2011	Pertandingan Olimpiade: AS dan Israel cukup merusak pembangkit listrik tenaga nuklir Iran (mesin sentrifugal melalui virus STUXNET)
Rusia	Ukraina	2015-2016	Serangan Jaringan Listrik Ukraina: Peretas Rusia menembus sistem distribusi listrik dan mematikan sistem yang menyebabkan pemadaman listrik di seluruh negeri.
Republik Faderal Yogoslavia	Kosovo dan NATO	1999	Selama perang Kosovo, para peretas Yogslavia, Rusia dan China (setelah serangan udara NATO atas kedutaan China) melumpuhkan situs-situs NATO untuk menunjukkan ketidaksenangan mereka atas keterlibatan NATO.

Rusia	Georgia	2008	Akibat penembakan drone Georgia oleh jet tempur Rusia, ketegangan meningkat antara dua negara. Selanjutnya, peretas Rusia mengganggu
			semua layanan internet Georgia.
Iran	Arab Saudi	2012-2016	Shamoon: Peretas Iran Sistem jaringan perusahaan minyak milik negara Saudi, ARAMCO, dan memengaruhi 30000 stasiun kerja.
KoreaUtara	AS	2014-2015	Peretas Korea Utara menyerang perusahaan film AS (gambar sony) karena menunjukkan kekesalan mereka atas film kontroversial "The Interview"
Rusia	Estonia	2007-2008	Karena keputusan pemerintah Estonia menghapus monumen era Soviet, peretas etnis Rusia melumpuhkan semua sistem perbankan, penyiaran, dan pemerintah nasional.

DAFTAR RIWAYAT HIDUP

Nama	:	Saifullah Khan
Pangat	:	Air Commodore
Nomor Angkatan Darat	:	PA 10490
Jabatan Terakhir	:	Commanding Officer C^2 Center
Instansi	:	Air Defence Wing
Alamat Resmi	:	Angkatan Udara, Pakistan
Alamat Rumah	:	B42, Askari X, Lahore
Negara	:	Pakistan
Telepon	:	+92 321 4665733
Surel	:	saifullahkhan10490@gmail.com

Jakarta, 7 Oktober 2020

DHARMMA TANHANA MANGRVA

SAIFULLAH KHAN

AIR COMMODORE

PAKISTAN