ANALISIS MANAJEMEN RISIKO ANCAMAN KEJAHATAN SIBER *(CYBER CRIME)* DALAM PENINGKATAN *CYBER DEFENSE*

THE ANALYSIS OF CYBER CRIME THREAT RISK MANAGEMENT TO INCREASE CYBER DEFENSE

Ineu Rahmawati[1]

Alumni Universitas Pertahanan Indonesia
(rahmawati.ineu@gmail.com)

Abstrak – Kemajuan teknologi dan informasi menimbulkan ancaman baru di ruang siber yakni kejahatan siber. Kejahatan siber merupakan kejahatan yang lahir sebagai suatu dampak negatif dari perkembangan aplikasi pada internet. Dalam menganalisis dampak kejahatan siber terhadap pertahanan sebuah negara, diperlukan identifikasi manajemen risiko yang dapat mengetahui seberapa besar probabilitas dan konsekuensi yang ditimbulkan dari kejahatan siber. Risiko yang dihadapi dalam mengatasi ancaman kejahatan siber tidak kalah dengan perang konvensional. Hal ini menyebabkan risiko yang diidentifikasi harus bisa menghasilkan strategi pertahanan negara dalam menghadapi ancaman kejahatan siber.

Kata Kunci : kejahatan siber, manajemen risiko, strategi, pertahanan negara

Abstract – *Increasing technology and information caused new threat in cyberspace called cyber crime. Cyber crime is a crime that emerge as a negative impact of applications development on the internet. In analyzing the impact of cyber crime towards a state defense, it is necessary to identify risk management that can know how big the probability and consequences caused by cyber crime. The risks faced in overcoming the threat of cyber crimeis not inferior to conventional wars. This causes the identified risks has to be able to produce a state defense strategy in the face of cyber crime threat.*

Keywords: *cyber crime, risk management, strategy, state defense*

[1] Penulis merupakan alumni Manajemen Pertahanan Cohort 7, Universitas Pertahanan.

Pendahuluan

Perkembangan globalisasi dan teknologi informasi telah membawa perubahan besar dalam kehidupan manusia. Teknologi Informasi menjadikan hubungan komunikasi antar manusia dan antar bangsa semakin mudah dan cepat tanpa dipengaruhi oleh ruang dan waktu. Globalisasi adalah suatu proses perubahan dinamika lingkungan global sebagai kelanjutan dari situasi yang pernah ada sebelumnya yang ditandai dengan ciri kemajuan teknologi dan informasi, menimbulkan saling ketergantungan, pengaburan terhadap batas-batas negara (*borderless*).[2] Dampak dari perkembangan teknologi dan informasi mengubah haluan perang yang terjadi saat ini.

Era globalisasi mendorong sebagian negara tidak lagi menggunakan cara perang tradisionaldankonvensional. Akibatnya, kekuatan negara tidak lagi dilihat pada kekuatan persenjataan, tetapi juga pada segi budaya, perekonomian, politik, dan teknologi. Hal ini membuat persaingan dan peperangan menjadi semakin tidak terlihat batasannya. Peperangan dan konflik yang terjadi di suatu negara tidak hanya didominasi oleh kekuatan militer, tetapi kekuatan nirmiliter juga dilakukan oleh aktor non-negara (*non state actor*).

Bentuk peperangan yang tidak lagi menggunakan cara perang tradisional menimbulkan ancaman baru di ruang siber. Ancaman yang berevolusi menjadi serangan siber bukan sekadar konsep saja. Rentannya pertukaran informasi di ruang siber (*cyberspace*) didorong sebuah negara untuk membangun sistem keamanan yang dapat mengatasi ancaman tersebut. Peristiwa Estonia pada tahun 2007 dan Georgia pada tahun 2008 merupakan contoh serangan kejahatan siber (*cyber crime*) dengan pemanfaatan *Distributed Denial of Service* (DdoS), sehingga melumpuhkan aktivitas negara karena banyak sektor kritis yang diserang.[3] Serangan yang tercatat cukup mengkhawatirkan adalah serangan Stuxnet. Stuxnet adalah contoh *malware* yang sangat canggih dan berhasil melumpuhkan seperlima sistem kendali pengayaan nuklir dari pembangkit listrik tenaga nuklir milik Iran.[4]

Ancaman diruang siber (*cyberspace*) didominasi oleh aktor non-negara (*non state actor*) seperti individu *hacker,* kelompok *hacker,* kegiatan para *hacker*, *non-government organization* (NGO), terorisme, kelompok kejahatan terorganisir (*organized criminal groups*) dan sektor swasta (seperti *internet companies and carries*, *security companies*) juga dapat mengancam pertahanan dan kedaulatan negara.[5] Sasaran ancaman

[2] J.A. Scholte, *Globalization: A Critical Introduction*, (London: Palgrave, 2000).

[3] Nate Anderson, "Massive DDoS Attack Targets Estonia, Russia Accused", dalam http://arstchnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/, diakses pada 8 Juni 2017.

[4] Michael B. Kelly, "The Stuxnet Attack On Iran's Nuclear Plant Was Far More Dangerous Than Previously Thought", dalam http://www.businessinsidercim/stuxnet-was-far-more-dangerous-than-prevoius-thought-2013-11?IR=T&, diakses pada 8 Juni 2017.

[5] W. Pearlman & K.G. Cunningham, "Non State

kejahatan siber (*cyber crime)* pernah terjadi pada kasus penyadapan komunikasi pribadi Presiden Indonesia dan beberapa pejabat tinggi negara yang dilakukan Australia berdasarkan dokumen yang dibocorkan oleh Edward Snowden mantan kontraktor *National Security Agency* (NSA) dari Amerika.[6] Selain itu, salah satu situs resmi unit kerja Kementerian Pertahanan Republik Indonesia (Kemhan RI) dibobol oleh *hacker,* yakni *website* milik Direktorat Jenderal Potensi Pertahanan (Ditjen Pothan) yang mengalami perubahan laman yang disebut *defacing*[7]*.* Situs tersebut dibobol oleh CVT (*Cyber Vampire Team*) dengan menuliskan laman situs "*Oops Myanmar Hacker was here*". Kemudian menuliskan kalimat dalam bahasa Inggris, yaitu:

> *Hello Indonesia Government, you should be proud with uneducated Indo script kiddies. Coz they believe (defacing/ Ddosing) to other country website is the best solution for them. If you would sympathize the white programmers/ developers of your country and how they are feeling. You can catch such script kiddies. Coz CVT are ready to provide those kiddies information.*[8]

Ancaman global, kemajuan teknologi dan informasi tidak hanya ditujukan untuk menyerang instansi pemerintah dan militer. Namun dapat pula mengancam seluruh aspek kehidupan manusia, seperti ekonomi, politik, budaya, dan keamanan suatu negara. Baru-baru ini, serangan siber juga terjadi pada *website* industri telekomunikasi milik pemerintah. Ancaman kejahatan siber (*cybercrime)* dapat terjadi karena adanya kepentingan dari berbagai individu atau kelompok tertentu. Ancaman inidalam aspek kehidupan masyarakat menimbulkan berbagai ancaman fisik baik nyata ataupun tidak nyata dengan menggunakan kode-kode komputer *(software)* untuk melakukan pencurian informasi dan data yang dapat mengancam suatu negara.

Peningkatan terhadap ancaman kejahatan siber (*cyber crime*)yang dilakukan baik oleh negara ataupun aktor non-negara (*non state actor*) berdampak terhadap terjadinya *cyber warfare* atau gangguan *cyber* (*cyber violence).* Ketergantungan negara terhadap jaringan komunikasi membawa tantangan dan ancaman tersendiri. Oleh sebab itu, dibutuhkan analisis manajemen risiko dalam menghadapi serangan kejahatan siber (*cyber crime)* dengan tujuan menjaga pertahanan dan kedaulatan NKRI dalam mewujudkan tujuan nasional. Manajemen risiko dapat artikan sebagai serangkaian prosedur dan metodologi yang digunakan untuk mengidentifikasi, mengukur, memantau dan mengendalikan risiko yang timbul dari kegiatan organisasi.[9]

Actors, Fragmentation, and Conflict Processes", *Journal of Conflict Resolution*, Vol.2 No. 56, 2012.

[6] "Snowden: Ponsel SBY Disadap Australia", dalamhttp://news.liputan6.com/read/748895/snowden-ponsel-sby-disadap-australia, diakses pada 8 Juni 2017.

[7] Erwin Kurnia N.M., "Kesiapan Sumber Daya Manusia Teknologi Informasi (SDM-TI) Kementerian Pertahanan untuk Mengantisipasi Cyber Warfare", Tesis Universitas Pertahanan, 2015.

[8] "Situs Dirjen Kementerian Pertahanan RI Di-Hack", dalam https://news.detik.com/berita/2243078/situs-dirjen-kementerian-pertahanan-ri-di-hack?9911012, diakses pada 12 Mei 2017.

[9] Rini Lestari, " Manajemen Risiko Terhadap

Manajemen risiko yang dibuat dalam bidang informasi dan komunikasi yang berhubungan dengan kehidupan banyak warga negara ataupun yang bersifat rahasia, merupakan hal yang dilakukan untuk mengurangi tingkat kerawanan penyalahgunaan informasi dan data di ruang siber *(cyberspace)*.

Risiko yang terjadi dalam menghadapi ancaman kejahatan siber (*cyber crime)* berasal dari dalam maupun luar negara dengan memanfaatkan kondisi sosial, politik, budaya, ideologi, dan perkembangan teknologi. Banyak cara yang dilakukan oleh berbagai macam pihak untuk mendapatkan informasi yang ada dalam Sistem Informasi Pertahanan Negara (Sisfohanneg). Beberapa aksi penyerangan bahkan telah dilakukan, misalnya aksi peretasan dengan melakukan *defacing* terhadap situs Dirjen Pothan Kemhan. Bocornya informasi terkait pertahanan negara yang terdapat didalam Sisfohanneg dapat mengancam kedaulatan negara, khususnya kedaulatan informasi. Konsep manajemen risiko dalam pertahanan merupakan unsur penting untuk menganalisis seberapa besar ancaman berdampak kepada pertahanan negara.

Dalam konteks menghadapi ancaman serangan kejahatan siber (*cyber* crime), tidak dapat diselesaikan dengan hanya menggunakan kekuatan senjata. Namun membutuhkan integrasi seluruh kekuatan nasional dibawah komando dan kendali (Kodal) Kementerian Pertahanan (Kemhan).[10] Risiko yang dihadapi dalam mengatasi ancaman kejahatan siber (*cyber crime)* tidak kalah dengan perang konvensional. Penggunaan teknologi *cyber* berdampak luas karena bisa mencakup berbagai aspek kehidupan bermasyarakat dan bernegara, diantaranya bidang ideologi, politik, ekonomi, sosial budaya, dan keamanan. Kejahatan siber (*cyber crime)* semakin meningkat yang dimanfaatkan pihak-pihak tertentu baik secara individu atau kelompok maupun negara dengan tujuan tertentu untuk dapat melemahkan lawannya. Kondisi ini perlu diwaspadai karena tidak menutup kemungkinan suatu negara dapat dilumpuhkan dan dihancurkan dengan perang teknologi atau melalui *cyber*.[11]

Sebagai bangsa yang berdaulat dan beradab tentu perlu upaya untuk mempertahanan keutuhan suatu negara dengan membangun pertahanan negara yang kuat demi tercapainya tujuan kepentingan nasional. Berbagai kondisi diatas menggambarkan betapa pentingnya identifikasi manajemen risiko dalam menghadapi ancaman kejahatan siber (*cyber crime*) dalam pengeloaan pembangunan pertahanan negara.

Definisi Kejahatan Siber (*Cyber Crime*)

Teknologi merupakan kegiatan yang dilahirkan oleh manusia dengan

Kinerja Organisasi", *Jurnal Riset Akuntansi dan Bisnis*, Vol.13, No.2, 2013.

[10] *Ibid.*

[11] Sugeng Brantas, "Defence Cyber dalam Konteks Pandangan Bangsa Indonesia tentang Perang dan Damai", Jurnal Pertahanan, Vol.2, No.2, 2014, hlm.55.

merencanakan dan menciptakan benda-benda material yang bernilai praktis, seperti mobil, pesawat, televisi adalah hasil dari pengembangan teknologi. Dilihat dari fungsi dan pentingnya teknologi, semua kalangan masyarakat dan instasi pemerintah sangat tergantung terhadap teknologi baik yang digunakan untuk hal postif maupun negatif. Kata *cyber* dan teknologi diuraikan dari asal kata *technique*, dari kata Yunani Technikos yang berarti kesenian atau keterampilan dalam dan logos adalah limo atau asas-asas utama pada *cyber* (*software).*[12] Meningkatnya pemanfaatan pada ruang siber (*cyberspace)* di seluruh lini kehidupan masyarakat pada era globalisasi saat ini secara parallel, akan menghubungkan pada pemanfaatan suatu jaringan teknologi internet pada obyek atau sektor tertentu sesuai dengan tujuan dari pengawakannya.

Ruang siber (*cyberspace*) adalah ruang dimana komunitas saling terhubung menggunakan jaringan (misalnya intenet) untuk melakukan berbagai kegiatan sehari-hari.[13] *Cyber* diartikan sebagai istilah lain, yaitu *cyberspace* yang diambil dari data *cybermetics*. Pada mulanya istilah *cyberspace* tidak ditujukan untuk menggambarkan interaksi yang terjadi melalui jaringan komputer. John Perry Barlow pada tahun 1990 mengaplikasikan istilah siber (*cyber)* yang dihubungkan pada jaringan internet. Dalam perkembangannya, *cyber* dapat membawa dampak positif dan negatif yang bisa menimbulkan suatu kejahatan dalam perkembangan dunia *cyber*. Kejahatan yang lahir sebagai suatu dampak negatif dari perkembangan aplikasi pada internet ini disebut dengan kejahatan siber (*cyber crime*) yang mencakup semua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif aplikasi internet.

Menurut pendapat Mcdonnell dan Sayers, ancaman siber terdiri atas tiga jenis,[14] yaitu:

a. Ancaman perangkat keras (*hardware threat*)
   Ancaman ini merupakan ancaman yang disebabkan oleh pemasangan perangkat tertentu yang berfungsi untuk melakukan kegiatan tertentu didalam suatu sistem, sehingga peralatan tersebut merupakan gangguan terhadap sistem jaringan dan perangkat keras lainnya.
b. Ancaman perangkat lunak (*software threat)*
   Ancaman ini merupakan ancaman yang disebabkan masuknya perangkat lunak tertentu yangberfungsi untuk melakukan kegiatan pencurian, perusakan, dan manipulasi informasi.
c. Ancaman data/informasi (*data/ information threat)*
   Ancaman ini merupakan ancaman yang diakibatkan oleh penyebaran data/informasi tertentu yang bertujuan untuk kepentingan tertentu.

[12] *Ibid.*

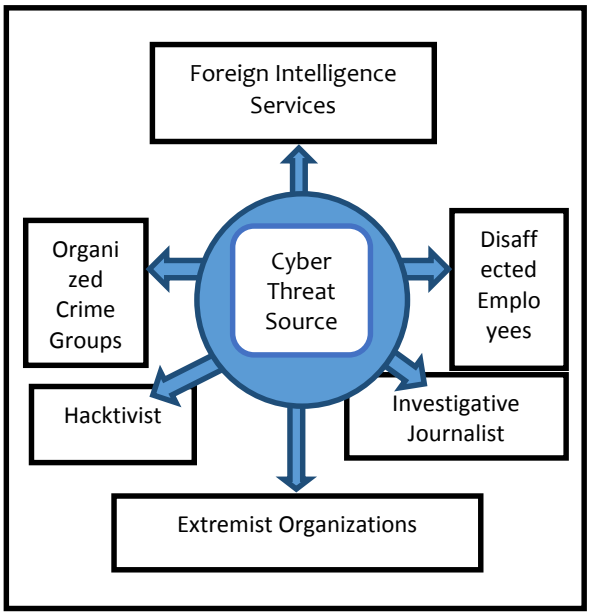
[13] Kementerian Pertahanan Indonesia, *Pedoman Pertahanan Siber*, (Jakarta: Kemhan RI, 2014), hlm.5.

[14] *Ibid.*

Dalam kajian Strategis Keamanan Siber Nasional, mendefinisikan ancaman kejahatan siber (*cyber crime*) sebagai setiap kondisi dan situasi serta kemampuan yang dinilai dapat melakukan tindakan atau gangguan atau serangan yang mampu merusak atau segala sesuatu yang merugikan sehingga mengancam kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersedian (*availability*) sistem dan informasi.[15] Ancaman siber dapat terjadi karena adanya kepentingan dari berbagai individu atau kelompok tertentu dalam aspek kehidupan masyarakat dapat menimbulkan berbagai ancaman fisik, baik nyata ataupun yang tidak nyata dengan menggunakan kode-kode komputer (*software*) untuk melakukan pencurian informasi (*information theft*), kerusakan sistem (*system destruction*), manipulasi informasi (*information corruption*) atau perangkat keras (*hardware*) untuk melakukan gangguan terhadap sistem (*network instruction*) ataupun penyebaran data dan informasi tertentu untuk melakukan kegiatan propaganda.[16]

Sumber-sumber ancaman siber dapat berasal dari berbagai sumber, seperti intelijen asing (*foreign intelligence service*), kekecewaan (*disaffected employees*), investigasi jurnalis (*investigatives journalist*), organisasi ekstremis (*extremist organization*), aktivitas para *hacker* (*hacktivist*), dan kelompok kejahatan terorganisir (*organized crime groups*).

Gambar 1. Sumber-sumber Ancaman



Sumber: Dr. Federick Wamala, CISSP
Sumber: International Telecommunication Unit(ITU) National Cybersecurity Strategy Guide, 2012

Risiko kejahatan siber (*cyber crime*) berpotensi terhadap kehilangan sistem informasi data, kegiatan militer dan gangguan lainnya yang menggunakan jaringan komputer dan internet. Dalam melihat sumber-sumber ancaman di atas, pemerintah melalui Kementerian Pertahanan (Kemhan) perlu mempersiapkan diri dalam menghadapi ancaman siber ini. Kemhan perlu mempersipakan Sumber Daya Manusia yang handal dalam menguasai teknologi, sistem infrastruktur yang handal, dan didukung oleh perundang-undangan atau kebijakan dalam melaksanakan operasi *cyber warfare.*

[15] Iwan, dkk, *Kajian Strategi Keamanan Cyber Nasional: Dalam Rangka Meningkatkan Ketahanan Nasional di Bidang Keamanan Cyber,* (Jakarta: Tesis Universitas Pertahanan Indonesia, 2012).
[16] *Ibid.*

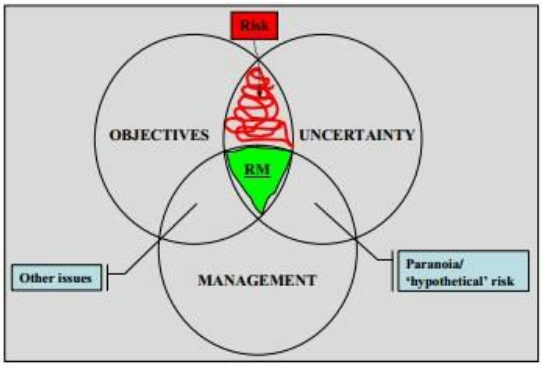
Pembahasan

Indonesia termasuk kedalam lima negara terbesar yang menggunakan media sosial dan dianggap sebagai potensi positif (kekuatan) atau potensi negatif (kerentanan/kelemahan) jika dikaitkan dengan potensi perang siber. Penggunaan media sosial di kalangan masyarakat bisa berpotensi mengancam kedaulatan negara. Namun disisi lain, media sosial juga bisa menjadi sumber pengetahuan tentang dunia teknologi informasi, komunikasi dan digital, sehingga masyarakat bisa melek dunia digital. Aktivitas masyarakat Indonesia yang menggunakan teknologi digital pada akhirnya akan menjadi potensi dalam perang siber. Penggunaan teknologi informasi akan mudah disadap atau diretas oleh para *hacker* maupun *cracker* dari negara asing, sehingga akan menciptakan kerawanan khususnya informasi intelijen yang menggunakan dunia maya sebagai sarana transmisi. Teknologi penyadapan yang maju secara cepat untuk meretas berbagai pengguna media sosial yang justru akan sangat membahayanakan dalam era perang siber.

Manajemen risiko didefinisikan sebagai "*process of understanding and managing the risk that organization is inevitability subject to attempting to achieve its corporate objectives*".[17] Manajemen risiko juga didefinisikan sebagai "*the essence of risk management lies in maximizing the areas where we have some control over the outcome while minimizing the areas where we have absolutely no control over the outcome, and the linkage between effect and cause is hidden from us*".[18]

Merujuk pada dua definisi di atas, manajemen risiko merupakan proses yang berkesinambungan, dilakukan selama kegiatan pengelolaan pertahanan dalam menghadapi ancaman kejahatan siber (*cyber crime*). Manajemen risiko merupakan manajemen (*management*) yang merencanakan rencana lanjutan dalam menghadapi risiko (*risk*) dan ketidakpastian (*uncertainty*) agar bisa memaksimalkan pencapaian tujuan (*objective*).

Gambar 2. Managemen Risiko (*Risk Management*)



Sumber: Steve Gibson, www.cranfield.ac.uk

Elemen dari manajemen risiko menurut *Institute of Risk Management* antara lain *Risk Assessment*, merupakan proses mengidentifikasi, mendeskripsikan dan mengestimasi; *Risk Evaluation*, pengambilan keputusan tentang risiko yang signifikan yang harus diberi

[17] P.M. Collier, S. Agyei dan Ampomah, *CIMA's Official Learning System: Management Accounting – Risk and Control Strategy, First Edition*, (Oxford: Elsevier, Ltd, 2006).

[18] Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk*, (Canada: John Wiley&Sons Inc, 1998)

perlakuan tergantung *risk appetite; risk treatment, risk appetite* dilakukan respons atau perlakuan yang merupakan proses pemilihan dan pengimplementasian. Adapun beberapa tahap dalam proses manajemen risiko yang dapat diimplementasikan dalam menghadapi ancaman kejahatan siber (*cyber crime*) dijelaskan sebagai berikut: [19]

a. *Identify*

Dalam tahap ini, identifikasi risiko kejahatan siber sebaiknya dilakukan secara berkala terhadap pemicu adanya kejahatan siber. Dalam proses ini, seluruh aspek yang berpotensi menimbulkan kerugian diidentifikasi dengan seksama. Seluruh risiko yang teridentifikasi selanjutnya diukur. Ukuran risiko pada ancaman ini mengacu pada dua ukuran, yaitu Probabilitas dan Dampak Probabilitas.

b. *Assess*

Dalam tahap ini, *assess* atau penilaian pada dasarnya menilai tingkat risiko yang ditimbulkan dari kejahatan siber yang berdampak pada seluruh aspek kehidupan terutama pertahanan negara. Penilaian terhadap kejahatan siber tidak dapat diukur secara langsung namun bisa menggunakan tabel matriks dalam pengukuran risiko yang ditimbulkan akibat kejahatan siber.

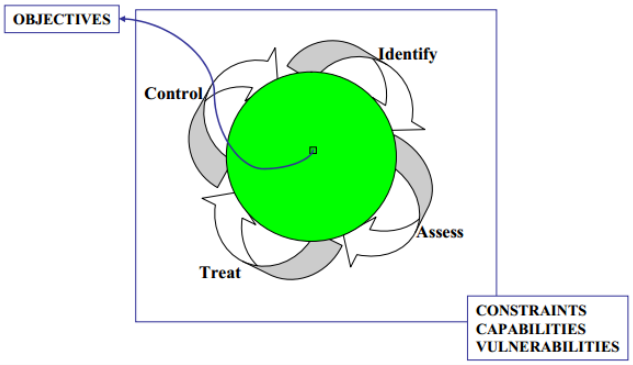
c. *Treat*

Setelah melakukan identifikasi dan pengukuran risiko, selanjutnya digunakan sebagai dasar untuk menentukan perlakuan dan respons terhadap risiko, apakah risiko akan diterima, dialihkan, diminimalisir atau dihindari. Dalam kasus ini, perlu dilakukan minimalisir terhadap pencurian informasi dan data yang sering terjadi baik secara individu maupun lembaga.

d. *Control*

Pemantauan dan penyesuaian perlu terus dilakukan untuk menilai keberhasilan manajemen risiko. Dalam proses pemantauan, sebaiknya terdapat mekanisme peringatan dini bagi pihak pengendali keamanan seperti Kementerian Pertahanan Republik Indonesia, sehingga pihak pengendali dapat melakukan tindakan-tindakan yang dianggap perlu agar bisa mengantisipasi adanya kejahatan siber.

Gambar 3. Proses Manajemen Risiko



Sumber: Steve Gibson, www.cranfield.ac.uk

[19] *Ibid.*

Matriks Risiko (*Risk Matrix*)

Potensi ancaman kejahatan siber (*cyber crime*) mengarak kepada *cyber warfare.* Adapun potensi ancaman yang kejahatan siber (*cyber crime*) di Indonesia sebagai berikut.

1. *Hacking*

   Kasus peretasan atau hacking beberapa kali terjadi di Indonesia. Penyebabnya beragam mulai dari sekadar iseng mengetas keamanan hingga penolakan wacana pemerintah. Contoh kasus pada pilpres 2014 lalu sempat tersebar kabar jika situs Komisi Pemilihan Umum (KPU) telas diretas oleh *hacker*. Indikasinya yaitu situs KPU sempat tidak bisa diakses.[20]

   Tidak hanya di sektor pemerintah, akan tetapi pihak swasta pun sering mengalami *hacking* oleh *hacker*. Baru-baru ini Perusahaan Telkomsel dihack oleh hacker. Dalam laman tersebut, sang peretas itu memprotes harga paket data Telkomsel yang dianggap terlalu mahal. Deskripsinya pun berisi kata-kata kasar yang mengeluhkan soal itu.[21]

2. *Cracking*

   Kasus cracking terjadi di Indonesia dengan cara "*carder*" yang hanya mengintip kartu kredit kemudia *cracker* mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan pribadi. *Cracker* yang berpengalaman membuat script atau program sendiri untuk melakukan *cracking*, yang menjadi incaran sasaran, yaitu database kartu kredit, database *account bank*, database informasi pelanggan, dan pembelian barang dengan kartu kredit palsu[22].

3. *Cyber Sabotage*

   Cyber Sabotage dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, sistem jaringan computer yang terhubung dengan internet. *Cyber sabotage* merupakan mudus yang paling ditakuti oleh hampir industri besar di dunia. Setidaknya modus-modus 'cantik' yang dimainkan bervariasi mulai dari pos jaringan berbahaya dan fitnah sosial, sepanjang jalan sampai ke informasi konsumen, *hacking*, dan bocornya sistem dari perusahan seperti nomor kartu atau rahasia industry.[23]

4. *Spyware*

   Spyware adalah program yang dapat merekam secara rahasia

[20] Trentech, "Kasus Hackting Terbesar di Indonesia", dalam https://www.trentech.id/5-kasus-hacking-terbesar-di-indonesia/, diakses pada 10 Juli 2017.

[21] Tekno Kompas, "Situs Telkomsel Diretas Berisi Keluhan Internet Mahal", dalam http://tekno.kompas.com/read/2017/04/28/08042477/situs.telkomsel.diretas.berisi.keluhan.internet.mahal, diakses pada 10 Juli 2017.

[22] Dista Amalia Arifah, "kasus Cybercrime Indonesia", *Jurnal Bisnis dan Ekonomi (JBE)*, Vol.18, No.2, September 2011.

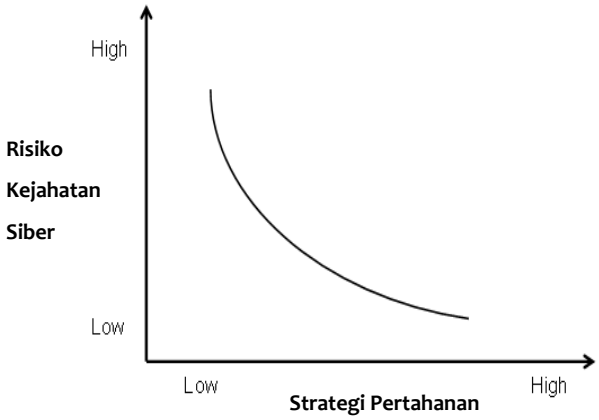
[23] "Meminimalisir Kejahatan Cyber Crime dan Cyver Sabotage di Indonesia, dalam http://news.detik.com/kolom/2610228/meminimalisir-kejahatan-cyber-crime-dan-cyber-sabotage-di-indonesia, diakses pada 10 Juli 2017.

segala aktivitas online user, seperti merekam *cookies* atau *registry*. Data yang sudah terekam akan dikirim atau dijual kepada perusahaan atau perorangan yang akan mengirim iklan atau menyebarkan virus.[24] Kasus *malware* terjadi pada masyarakat Indonesia pengguna bank *online.* Pelaku menyebarkan malware untuk memperdaya korbannya. *Malware* disebarkan ke ponsel nasabah melalui iklan-iklan *software* internet banking palsu yang kerap muncul di sejumlah laman internet.

Ketika nasabah mengunduh *software* palsu itu, *malware* akan secara otomatis masuk ke ponsel dan memanipulasi tampilan laman internet banking seolah-olah laman tersebut benar berasal pelaku menyebar *malware* untuk memperdaya korbannya. *Malware* internet banking seolah-olah laman tersebut benar-benar berasal dari bank.

Kunci dalam memahami risiko mencakup kedalam dua unsur, yaitu probabilitas (*probability*) dan konsekuensi (*consequence*). Hal ini dilakukan karena risiko juga sesuatu yang tidak bisa dihindari. Oleh karena itu, pemahaman terhadap manajemen risiko sangat penting dilakukan dalam penentuan sebuah strategi. Adapun *Risk Matrix* yang ditimbulkan dari kejahatan siber (*cyber crime*) bila ditinjau dari segi probabilitas dan konsekuensi sebagai berikut.

Gambar 4. Matriks Risiko (*Risk Matrix*)



Sumber: Diolah oleh Penulis

Dalam matriks risiko dapat dilihat bahwa semakin tinggi risiko kejahatan siber (*cyber crime*) maka strategi pertahanan yang dibuat harus ditingkatkan.

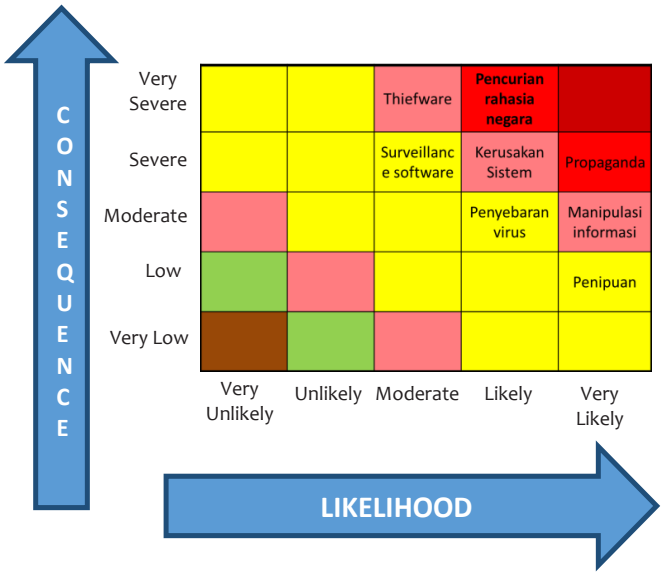
Manajemen risiko merupakan elemen fundamental dari sebuah strategi. Dari manajemen risikolah kita dapat membuat perhitungan sebuah anggaran biaya yang diperlukan. Dalam penanggulangan kejahatan siber (*cyber crime*), tidak sedikit biaya yang dikeluarkan dalam pengamanan kerahasian informasi dan data sebuah negara. Oleh karena itu, manajemen risiko yang dibuat dapat membuat sebuah strategi yang lebih terjangkau dalam menghadapi ancaman kejahatan siber (*cyber crime*).

Risiko adalah metrik integratif untuk mengevaluasi alternatif dan memprioritaskan sumber daya. Dalam pengambilan keputusan dalam manajemen risiko, risiko yang menjadi prioritas tertinggi harus didanai terlebih dahulu dibandingkan prioritas lebih

[24] *Ibid.*

rendah. Hal penting yang dilakukan dalam manajemen risiko adalah pembuatan grafis yang mengambarkan risiko dalam hal probabilitas dan konsekuensinya. Risiko adalah kombinasi dari kemungkinan (*likelihood*) dan konsekuensi (*consequence*). Hal ini menjawab pertanyaan seberapa mungkin probabilitas yang terjadi dan seberapa buruk konsekuensi yang terjadi. Berikut contoh grafis dari ancaman kejahatan siber.

Gambar 5. Grafis Risiko



Sumber: Diolah oleh Penulis

Risiko pada ancaman *cyber* kian hari kian meningkat. Pusdatin Kementerian Pertahanan RI mengatakan bahwa perang dingin *cyberwar* sedang berjalan dalam konteks global. Cepat atau lambat negara Indonesia akan terlibat didalamnya dimana *cyberwar* ini bisa dilakukan oleh *nation-state actor*.

Cyberwar terjadi dilihat dari suatu keadaan dimana sebuah negara melakukan penetrasi terhadap komputer ataupun *server* negara lainnya. Keadaan seperti ini tentu berkaitan langsung dengan kedaulatan negara dan kepentingan nasional Indonesia. Oleh karena itu, Indonesia harus mempersiapkan sistem pertahanan negara yang baik. Jika tidak ditanggapi dengan baik, risiko terbesar yang akan dialami adalah pencurian data rahasia negara dan perubahan geopolitik serta geostrategis Indonesia dengan negara-negara lain.

Pertahanan Negara dalam Menghadapi Kejahatan Siber (*Cyber Crime*)

Pada aspek militer,*cyber* digunakan sebagai alat untuk melakukan serangan terhadap kekuatan lawan atau mengetahui kelemahan lawan dan merusak jaringan pertahanan. Dalam mencapai suatu kekuatan, *cyber* bergantung pada strategi suatu negara dan kebijakan untuk mengembangkan *cyber security*.

Pembentukan *cyberarmy* merupakan bagian dari pembangunan Pusat Pertahanan Siber *(cyber defense)* yang meliputi pertahanan sistem komunikasi dan informasi Kementerian Pertahanan. *Cyberarmy* terdiri dari kalangan militer yaitu TNI AD, TNI AU, dan TNI AL serta kalangan sipil yang ikut dalam pertahanan negara di bidang Teknologi dan Informasi. *Cyberarmy* dibutuhkan sebagai pertahanan negara yang bisa menangkis segala serangan di dunia maya yang setiap saat bisa mengganggu

keutuhan NKRI.[25] *Cyberarmy* juga dituntut untuk memiliki kemampuan menyerang yang dapat mengimbangi kemajuan teknologi dan informasi negara lain.

Dalam pertahanan negara baik militer maupun nirmiliter sangat penting memiliki suatu sistem baru sebagai generasi modern dan perang masa depan, dalam bidang pertahanan teknologi dan informasi. Selain pertahanan negara yang kuat, juga dibutuhkan dukungan hukum yang saling memengaruhi dan saling berhubungan dalam menghadapi ancaman *cyber crime*. Hukum diperlukan untuk menciptakan ketertiban dan keadilan dalam masyarakat.

Teknologi, hukum dan masyarakat saat ini menjadi satu kesatuan yang tidak bisa dipisahkan. Seiring dengan kemajuan teknolgi, masyarakat dituntut untuk terus berkembang dan tidak jarang mengakibatkan munculnya kejahatan-kejahatan baru dalam teknologi. Oleh karena itu, hukum menjadi bagian terpenting untuk mengatasi kriminalitas yang dapat merusak pertahanan negara.

Kejahatan siber (*cyber crime*) di Indonesia marak terjadi baik dilakukan oleh individu atau kelompok. Semua tindak kriminal yang berhubungan dengan siber sangat beragam jenisnya, mulai dari hak cipta, pembajakan, penyalahgunaan akses bahkan hingga pencemaran nama baik perorangan maupun institusi. Namun hal ini sangat kontras dengan hukum yang mengatur kejahatan siber yang masih sangat minim batasan-batasan yang bisa dijadikan acuan untuk menjerat pelaku dalam melakukan tindak kriminal. Ketimpangan ini menjadikan hukum yang kurang kuat. Penegakan hukum di Indonesia tentang penyalahgunaan komputer dipengaruhi oleh beberapa faktor yaitu Undang-Undang, mentalitas para aparat, perilaku masyarakat, sarana serta kebudayaan.

Kementerian Komunikasi dan Informasi RI mencatat ada 21 Undang-Undang dan 25 RUU yang akan terkena dampak dari Undang-Undang yang mengatur kejahatan siber(*cybercrime*).[26] Harmonisasi eksternal berupa penyesuaian perumusan pasal-pasal *cybercrime* dengan ketentuan serupa dari negara lain, terutama dengan *Draft Convention on Cyber Crime* dan pengaturan *cybercrime* dari negara lain. Dunia teknologi internet telah memberikan revolusi dan inovasi terhadap manusia dalam melakukan komunikasi. Oleh karena itu, diperlukan harmonisasi antara hukum dan teknologi. Harmonisasi ini telah dilaksanakan dengan baik dalam RUU, PTI, RUU IETE, RUU ITE, RUU TPTI maupun RUU KUHP.[27]

Persoalan *cyber crime* ini diperlukan standarisasi dan harmonisasi dalam tiga area tertentu, yaitu *legislation, criminal enforcement*, dan *judicial review* dalam upaya penegakan hukum dan peradilannya.[28]

[25] *Ibid.*

[26] *Ibid.*

[27] *Ibid.*

[28] Edmon Makari, "Informasi Hukum untuk Sistem Ketahanan Nasional Terhadap Penyelenggaraan Sistem dan Komunikasi Elektronik Global", *Jurnal Ketahanan Nasional,* 2014, hlm. 77.

Undang-Undang ITE merupakan undang-undang yang secara khusus mengatur tindak pidana siber baik hukum pidana maupun hukum acara pidana. Hukum yang baru lahir tersebut adalah *cyberlaw*. *Cyberlaw* sendiri digunakan untuk penegakan hukum terkait dengan pemanfaatan teknologi informasi dalam mengantisipasi perilaku masyarakat pada teknologi informasi, sebagai batasan untuk melakukan kejahatan (*Law of Information Technology*) dan hukum dunia maya.

Perencanaan SDM TI untuk Menghadapi Ancaman Kejahatan Siber (*Cyber Crime*)

Persiapan yang harus dimiliki Indonesia dalam menghadapi kejahatan siber (*cyber crime*) adalah sumber daya manusia dan fasilitas produksi pengamanan negara. Sumber daya manusia berbasis kompetensi diharapkan mampu menciptakan cara berpikir positif terhadap dinamika perubahan lingkungan global sehingga menambah kepedulian terhadap perkembangan teknologi dan informasi yang menimbulkan berbagai dampak dalam kehidupan masyarakat, terutama berkaitan dengan ancaman siber.

Dalam rangka antisipasi kejahatan siber, (*cyber crime*) diperlukan ahli teknologi yang dapat menunjang sistem pertahanan negara yang canggih dan modern. Oleh karena itu, diperlukan sebuah kerja sama dengan industri pertahanan Indonesia yang bisa membuat program sistem informasi dan komunikasi yang bisa bersaing dengan negara lain. Peningkatan peran militer dalam mengembangkan sistem pertahanan siber di Indonesia tidak bisa dipungkiri. *Cyber military defense* menyiapkan operasional dan sumber daya untuk meningkatkan *national cyber security.*[29]

Pengembangan sistem pertahanan siber di Indonesia dipengaruhi oleh dua faktor. Faktor pertama adalah regulasi dan yang kedua adalah keberadaan pusat komando siber. Pemerintah perlu membuat sebuah regulasi yang baik dan tepat terkait pengembangan *national cyber security*. Sebagai bahan perbandingan, regulasi yang dibuat oleh pemerintah Amerika yaitu *USA cyber attack convention, draft cyber warfare international law manual* dan *council of Europe convention on cyber crime* 2001.[30]

Hal penting lainnya dalah membangun pusat komando keamanan pertahanan siber. Pemerintah Indonesia akan mengimplementasikan *cyber operation command* yang bertujuan untuk menjadi pusat komando pertahanan siber di Indonesia. Ketika pusat komando tersebut sudah bisa dijalankan, ada harapan besar bagi bangsa Indonesia yang sudah siap mengantisipasi *non-traditional threat*, yakni kejahatan siber (*cyber crime*) yang semakin hari semakin besar dampaknya bagi kedaulatan NKRI. Hal ini merupakan langkah besar yang perlu dilanjutkan agar berjalan optimal. Kebutuhan regulasi yang tepat dan

[29] *Ibid.*
[30] *Ibid.*

kerjasama dengan semua pihak baik pemerintah maupun swasta bisa menjadi kunci dalam menghadapi tantangan dunia siber yang semakin kompleks.[31]

Proses perencanaan SDM TI merupakan bagian dan fungsi pembinaan personel di lingkungan Kementerian Pertahanan dan jajarannya.[32] Fungsi ini dilaksanakan oleh Biro Kepegawaian, sesuai Permenhan Nomor 16 Tahun 2010, pasal 41, ayat 2 bahwa Pengadaan PNS Kemhan, Mabes TNI dan Angkatan serta pengembangan pegawai Kemehan. Proses perencanaan SDM TI didasarkan atas kriteria tertentu, seperti latar belakang pendidikan, administrasi, fisik, kesehatan, maupun psikologi SDM, harus menjadi bahan pertimbangan. Proses pengadaan PNS di lingkungan Kemhan memiliki beberapa tahapan dimulai dari proses pengadaan, pendidikan, penggunaan, perawatan dan pemisahan.

Upaya perwujudan SDM berbasis kompetensi, merupakan modal utama dalam menghadapi berbagai perubahan lingkungan strategis dan kemajuan teknologi saat ini. Perencanaan SDM TI lebih memperhatikan kualitas daripada kuantitas untuk memenuhi kebutuhan personel. Pemahaman akan latar belakang pendidikan SDM TI baik pendidikan formal maupun informal sangat membantu organisasi dalam menghasilkan SDM TI yang berkualitas. Oleh karena itu, persiapan SDM TI memerlukan kemampuan terhadap sistem pertahanan negara, sistem jaringan, aplikasi, dan kebijakan berkaitan dengan siber.

Kesimpulan

1. Ancaman kejahatan siber *(cyber crime)* dalam bentuk pencurian informasi dan data yang bersifat rahasia ditujukan untuk menyerang individu, instansi pemerintah dan militer yang mengancam pertahanan suatu negara. Pemerintah melalui lembaga Kementerian Pertahanan perlu mempersiapkan diri dalam menghadapi ancaman siber ini. Kemhan perlu mempersipakan Sumber Daya Manusia yang handal dalam menguasai teknologi, sistem infrastruktur yang handal, dan didukung oleh perundang-undangan atau kebijakan dalam melaksanakan operasi *cyber warfare.*
2. Manajemen risiko yang dibuat dalam bidang informasi dan komunikasi yang berhubungan dengan kehidupan banyak warga negara ataupun yang bersifat rahasia merupakan hal yang dilakukan untuk mengurangi tingkat kerawanan penyalahgunaan informasi dan data di ruang siber *(cyberspace).* Manajemen risiko merupakan elemen fundamental dari sebuah strategi. Risiko adalah kombinasi dari kemungkinan (*likelihood*) dan konsekuensi (*consequence*). Hal ini menjawab pertanyaan seberapa mungkin probabilitas yang terjadi

[31] Mohammad Syahruddin, *Propaganda Malaysia terhadap Pertahanan Negara Indonesia melalui Cyber pada Kasus Blok Ambalat*, (Jakarta: Tesis Universitas Pertahanan, 2015).
[32] *Ibid.*

dan seberapa buruk konsekuensi yang terjadi. Oleh karena itu, manajemen risiko penting dibuat untuk mempersiapkan sistem pertahanan negara yang baik.

3. Dalam mencapai suatu kekuatan siber bergantung pada strategi suatu negara dan kebijakan untuk mengembangkan *cyber security.* Selain pertahanan negara yang kuat, juga dibutuhkan dukungan hukum yang saling mempengaruhi dan saling berhubungan dalam menghadapi ancaman *cyber crime*. Kebutuhan regulasi yang tepat dan kerjasama dengan semua pihak baik pemerintah maupun swasta bisa menjadi kunci dalam menghadapi tantangan dunia siber yang semakin kompleks.

Daftar Pustaka

Buku

Bernstein, Peter L. 1998. Against the Gods: The Remarkable Story of Risk. Canada: John Wiley&Sons Inc.

Bessis, J. 2002. *Risk Management in Banking*. Willey: Chicester.

Collier, P.M. Agyei S, dan Ampomah. 2006. *CIMA's Official Learning System: Management Accounting – Risk and Control Strategy, First Edition*. Oxford: Elsevier Ltd.

J.A. Scholte, 2000. *Globalization: A Critical Introduction*. London: Palgrave.

Kementerian Pertahanan Indonesia. 2014. *Pedoman Pertahanan Siber*.Jakarta: Kemnhan RI.

Scholte, J.A. 2000. *Globalization: A Critical Introduction*. London: Palgrave.

Jurnal

Arifah, Dista Amalia. 2011. "Kasus Cybercrime Indonesia". *Jurnal Bisnis dan Ekonomi (JBE)*. Vol.18. No.2.

Andersen, T.J. 2008. "The Performance Relationship of Effective Risk Management: Exploring The Firm-Specific investment Retaionale". Long Range Planning. Vol. 41. No.2.

Brantas, Sugeng. 2014. "Defence Cyber dalam Konteks Pandangan Bangsa Indonesia tentang Perang dan Damai". *Jurnal Pertahanan.* Vol.2. No.2.

Lestari, Rini. 2013. "Pengaruh Manajemen Risiko Terhadap Kinerja Organisasi. Jurnal Riset Akuntansi dan Bisnis". Vol. 13. No.2.

Makari, Edmon. 2014."Informasi Hukum untuk Sistem Ketahanan Nasional terhadap Penyelenggaraan Sistem dan Komunikasi Elektronik Global". Jurnal Ketahanan Nasional. Vol.2. No.2.

Pearlman, W. and Cunningham, K.G. 2012. "Non State Actors, Fragmentation, and Conflict Processes". *Journal of Conflict Resolution*. Vol.2. No.56.

Tesis

Iwan, dkk. 2012. *Kajian Strategi Keamanan Cyber Nasional: Dalam Rangka Meningkatkan Ketahanan Nasional di Bidang Keamanan Cyber.* Jakarta: Tesis Universitas Pertahanan Indonesia.

Kurnia N.M., Erwin. 2015. *Kesiapan Sumber Daya Manusia Teknologi Informasi (SDM-TI) Kementerian Pertahanan untuk Mengantisipasi Cyber Warefare*. Jakarta: Universitas Pertahanan Indonesia.

Syahruddin, Mohammad. 2015. *Propaganda Malaysia terhadap Pertahanan Negara Indonesia melalui Cyber pada Kasus Blok Ambalat*. Jakarta: Universitas Pertahanan Indonesia.

Website

Anderson, Nate, "Massive DDoS Attack Targets Estonia, Russia Accused",

dalam http://arstchnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/, diakses pada 8 Juni 2017.

Kelly, Michael B, "The Stuxnet Attack On Iran's Nuclear Plant Was Far More Dangerous Than Previously Thought", dalam http://www.businessinsidercim/stuxnet-was-far-more-dangerous-than-prevoius-thought-2013-11?IR=T&, diakses pada 8 Juni 2017.

Nate, Anderson, Massive DDoS Attack Targets Estonia, Russia Accused, dalam http://arstchnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/, diakses pada 8 Juni 2017.

Situs Dirjen Kementerian Pertahanan RI Di-Hack, dalam https://news.detik.com/berita/2243078/situs-dirjen-kementerian-pertahanan-ri-di-hack?9911012, diakses pada 12 Mei 2017.

Snowden: Ponsel SBY Disadap Australia", dalam

http://news.liputan6.com/read/748895/snowden-ponsel-sby-disadap-australia, diaksespada 8 Juni 2017.

Tekno Kompas, " Situs Telkomsel Diretas Berisi Keluhan Internet Mahal", dalam http://tekno.kompas.com/read/2017/04/28/08042477/situs.telkomsel.diretas.berisi.keluhan.internet.mahal, diakses pada 10 Juli 2017

Trentech. "Kasus Hackting Terbesar di Indonesia", dalam https://www.trentech.id/5-kasus-hacking-terbesar-di-indonesia/, diakses pada 10 Juli 2017.