ANALISIS PENGGUNAAN MEDIA SIBER TERHADAP KEAMANAN NASIONAL: SUATU STUDI DI MALAYSIA

ANALYSIS OF CYBER MEDIA TO NATIONAL SECURITY: CASE STUDY IN MALAYSIA

Amarmuazam Usmani bin Othman [1]

Universitas Pertahanan

(muazam@yahoo.com)

Abstrak -- Pengguna internet adalah tinggi di negara-negara di dunia. Persentase pengunaan internet yang tinggi akan menyebabkan rakyat mendapatkan informasi yang tidak dapat dipastikan benar atau tidak. Arab spring adalah contoh di negara-negara Timur Tengah di mana penggunaan media sosial dapat menjatuhkan pemerintah yang ada. Pihak-pihak yang ada agenda tertentu sering mengguna media siber untuk melancarkan serangan siber. Media siber dapat dijadikan alat untuk melakukan serangan kepada pemerintah dalam bentuk perang urat saraf. Media siber bersifat terbuka dan pengunaannya yang meluas sukar bagi pemerintah memantau dan mengawalnya. Selain sebagai media untuk melakukan perang urat saraf, media siber juga dapat menyebabkan terjadinya salah faham di antara pihak-pihak yang bertikai. Ini karena penafsiran secara terbuka dan mampu membawa kepada pertikaian jika tidak ditangani dengan baik. Sikap pengguna media siber yang tidak ada kesadaran terhadap keselamatan dengan mudah mengunggah informasi-informasi rahasia seperti surat-surat dinas, aset pertahanan dan lain-lain ke internet telah membuka rahasia negara kepada umum. Di samping itu, serangan siber atas sistem pemerintahan dan ekonomi juga boleh meruntuhkan negara, seperti apa yang berlaku di Estonia dan Georgia. Serangan sistem pemerintahan oleh Rusia telah merusakkan ekonomi dan politik negara tersebut. Penggunaan media siber yang tidak dikawal mampu memusnahkan keamanan, kesejahteraan dan ekonomi negara. Sekiranya ini berlaku, negara akan kehilangan investor dan ekonomi negara akan merosot. Kemerosotan ekonomi akan memusnahkan asas negara dan negara akan menjadi huru hara. Dengan hampir semua lingkungan kehidupan bersandarkan kepada teknologi informasi, kerawanan keamanan siber akan memberi bencana yang besar kepada negara. Baik dari segi ekonomi, politik, keamanan, dan lain-lain. Maka sangatlah penting untuk diketahui bagaimana peran penggunaan media siber dalam rangka keamanan negara.

Kata Kunci: Siber, Media Sosial, Keamanan Nasional, Perang Informasi, Spionase.

Abstract *-- Internet is becoming necessity for the nation and the user percentage is increasing year by year. High percentage of internet user will cause many people to get unreliable information. Arab spring is an example in Middle Eastern countries where the use of social media can topple existing governments. Parties on a hidden agenda often use cyber media to launch cyber-attacks to their victims. Cyber media can be used as a tool to attack the government in the form of psychological*

[1] Amarmuazam Usmani bin Othman, MEng adalah mahasiswa program study magister terapan Strategi Pertahanan Matra Darat Ch-4, Fakultas Strategi Pertahanan, Universitas Pertahanan Indonesia.

warfare. Cyberspace is open to everyone to use and its difficult for the government to monitor and control it. Cyber media can also lead to misunderstandings among conflicting parties if the issue not handled properly. The cyber-media user's non-awareness towards security by uploading confidential information such as official letters, defense assets and so on has opened nation's secrets to the public. In addition, cyber attacks on government's administration and economy may also undermine the country, as in the cases of Russia cyber attack to Estonia and Georgia. The use cyber media without proper law and regulations can destroy the nation's security, welfare and economy. If this happen, the country would lose investors and the country's economy would be affected. The economic downturn will destroy the stability of the nation and the country will become fail state. With almost every part of our life relying on information technology, cyber security vulnerability will bring great disaster to the country in terms of economy, politics, security etc. Therefore, it is important to know how the cyber media role in the framework of nation's security.
***Keyword**: Cyber, Social Media, National Security, Cyber War, Espionage*

Pendahuluan

Teknologi informasi dan komunikasi tidak dapat dipisahkan dengan kehidupan manusia pada saat ini. Hampir semua negara di dunia menyediakan internet kepada warganya. Persentase pengunaan internet yang tinggi akan menyebabkan rakyat mendapatkan informasi yang tidak dapat dipastikan benar atau salah. Informasi yang salah dan fitnah bisa melemahkan negara dan pemerintahan. Ini akan menyebabkan berlakunya konflik dan selanjutnya rakyat hilang kepercayaan kepada pemerintah karena informasi yang salah sengaja disebarkan dengan tujuan untuk menghilangkan kepercayaan kepada pemerintah. Arab spring adalah contoh di negara Mesir dan Libya di mana penggunaan media sosial dapat menjatuhkan pemerintah yang ada. Pihak-pihak yang ada agenda tertentu sering mengguna media siber untuk melancarkan serangan siber. Oleh karena media televisi dan radio bisa dimonitor dan ditentukan oleh pemerintah, pihak-pihak yang berkepentingan menggunakan media siber bagi membuat propaganda karena media siber sulit untuk dimonitor dan ditentukan kandungan berita.

Media siber dijadikan alat untuk melakukan serangan kepada pemerintah dalam bentuk perang urat saraf. Media siber bersifat terbuka dan pengunaannya yang meluas sukar bagi pemerintah memantau dan mengawalnya.

Media siber dapat menyebabkan terjadinya salah faham di antara pihak-pihak yang bertikai. Ini karena penafsiran secara terbuka dan mampu membawa kepada pertikaian jika tidak ditangani dengan baik. Kegemaran berkongsi berita dan video di media sosial yang mengandung unsur provokasi dan perpecahan akan menggugat stabilitas

negara. Kemudian komen-komen berunsur provokasi menyusul selepas menonton video tersebut menyemarakkan lagi api perpecahan dan kebencian. Maka perlu dilakukan kontrol dan monitor agar ulasan dan video yang bisa memprovokasi tidak disebarkan dengan sewenang-wenangnya. Hal ini seperti yang berlaku di dalam kasus Ahok (Gubernur DKI Jakarta). Maka berlakulah demonstarsi besar-besaran karena provokator-provokator telah menyemarakkan api kebencian. Ini tidak baik untuk kesatuan negara dan bangsa serta mampu memecah belahkan negara.

Sikap pengguna media siber yang tidak ada kesadaran terhadap keselamatan dengan mudah mengunggah informasi-informasi rahasia seperti surat-surat dinas, aset pertahanan dan lain-lain. Ini telah membuka rahasia negara kepada umum. Sikap ini perlu diperbaiki dan perlunya ada peraturan dan kebijakan dari pemerintah supaya surat-surat serta informasi rahasia dan bernilai strategis tidak sewenang-wenangnya diletakkan di internet. Berkaitan ancaman peperangan siber, maka telah ada kebijakan yang menetapkan komputer yang digunakan untuk perihal operasi dan rahasia tidak boleh disambungkan ke internet. Sambungan ke internet adalah rawan bagi serangan siber dan informasi bisa disadap oleh pihak lain. Insiden penyadapan dan pemonitoran bukan sesuatu yang asing jika kita mengikuti perkembangan dunia. Insiden pembongkaran aktivitas penyadapan dari agensi AS yaitu National Security Agency (NSA) telah mengejutkan dunia. David Snowden telah membongkar aktivitas ini kepada dunia. Pelbagai rahasia negara lain telah berjaya dicuri dan aktivitas negara lain telah berjaya dimonitor oleh NSA. Oleh itu semua negara harus siap dalam nenghadapi ancaman penyadapan dan serangan siber negara lain. Pishing dan spyware adalah ancaman kepada pengguna media siber karena musuh-musuh sentiasa mencari ruang dan peluang untuk menaman tools ini agar segala informasi dapat diambil oleh pihak musuh yang berniat menyadap kita. Pegawai pemerintah perlu senantiasa waspada agar tidak menjadi korban tool ini. Sekiranya akun ini sudah dicemari spyware, maka segala urusan dinas akan dapat diawasi musuh/lawan.

Di samping itu, serangan siber atas sistem pemerintahan dan ekonomi juga boleh meruntuhkan negara, seperti apa yang berlaku di Estonia dan Georgia. Serangan sistem pemerintahan oleh Rusia

telah merusakkan ekonomi dan politik negara tersebut. Penggunaan media siber yang tidak dikawal mampu memusnahkan keamanan, kesejahteraan dan ekonomi negara. Sekiranya ini berlaku, negara akan kehilangan investor dan ekonomi negara akan merosot. Kemerosotan ekonomi akan memusnahkan asas negara dan negara akan menjadi huru hara. Data bank yang dirusakkan bukan hanya bisa memusnahkan negara itu sendiri, malah rakyat juga akan menjadi gawat karena segala uang dan harta bisa hilang dalam masa yang singkat. Serangan siber kepada sistem negara bukan sahaja membinasakan negara. Namun rakyat juga bisa mendapat dampak serangan ini. Penggangguan kepada sistem transportasi bisa membawa kecelakaan kepada penumpang. Sebagai contoh, jika sistem navigasi pesawat diganngu, maka risiko kecelakaan dan korban sukar untuk dielakkan dan bisa membawa kepada konflik keamanan.

Dengan hampir semua lingkungan kehidupan bersandarkan kepada teknologi informasi, kerawanan keamanan siber akan memberi bencana yang besar kepada negara. Baik dari segi ekonomi, politik, keamanan, dan lain-lain. Maka sangatlah penting untuk diketahui bagaimana peran penggunaan media siber dalam rangka keamanan negara.

Kejadian dan outcome dari penggunaan media siber yang telah mengganggu keamanan negara dan perlu untuk diteliti mengapa hal tersebut terjadi. Pemerintah yang seharusnya sudah mempunyai kebijakan dalam mencegah berlakunya kerusakan yang timbul akibat sikap pengguna media siber yang tidak bertanggung jawab.

Berdasarkan uraian rumusan masalah di atas, maka pertanyaan penelitian yang diajukan adalah sebagai berikut

a) Mengapa media siber mampu mengancam keamanan nasional ?
b) Bagaimana mengatasi ancaman siber terhadap keamanan nasional ?

Teori Digunakan

Teori yang digunakan dalam penelitian ini adalah sebagai berikut.

a) Teori Keamanan Nasional
b) Teori Perang Asimetris.
c) Teori Komunikasi.

Teori Keamanan Nasioanal adalah secara umum dan teori perang asimetris dan teori komunikasi akan digunakan dalam pembahasan yang lebih mendalam

Teori Keamanan Nasional menurut Alan Collins (2003) adalah *"National security is the requirement to maintain the*

survival of the nation-state through the use of economic, military and political power and the exercise of diplomacy." Keamanan nasional adalah sebuah kebutuhan untuk menjaga ketahanan suatu bangsa melalui daya ekonomi, militer serta kekuatan politik dan kepiawaian berdiplomasi. Karena sifat yang kompetitif diantara bangsa-bangsa, keamanan nasional dengan negara yang mempunyai nilai sumber daya yang signifikan didasarkan kepada tindakan-tondakan teknis dan proses operasional. Hal ini berkisar dari perlindungan informasi yang berkaitan dengan rahasia Negara untuk persenjataan bagi militer hingga strategi bernegosiasi dengan negara bangsa lain. Oleh itu harus dilakukan beberapa langkah bagi memastikan keamanan negara terus dipelihara.

Perang asimetris yaitu peperangan menggunakan sistem dan tujuan (susunan bertempur) yang inkonvensional, mempunyai banyak nama diantaranya istilah yang populer adalah peperangan asimetris (asymmetrical warfare). Jenis perang yang termasuk asimetris adalah insurjensi, terrorisme dan Perang Internal Baru (Seskoad, 2010). Carl von Clausewitz menemukan teori center of gravity yang mengatakan bahawa siapa yang mengusai ketinggian akan menang perang. Ketinggian pada hari ini bisa di definisikan sebagai teknologi dan informasi. Beliau dalam bukunya "On War" menegaskan bahwa "uncertainty is fundamental to warfare". Segala ketidakpastian tersebut diakibatkan oleh lemahnya fungsi intelijen untuk mendeteksi tentang tujuan musuh; waktu, lokasi atau bahkan rencana serangan; keberadaan senjata baru yang digunakan; dan perkembangan bentuk baru perang. Sun Tzu memberikan titik berat pada intelijen, pengelabuhan, dan pendekatan tidak langsung kepada musuh sebagai cara yang paling efektif untuk memenangkan pertempuran. Penggunaan kemampuan intelijen, pengelabuhan, dan mendekati musuh secara diam-diam dan tidak langsung merupakan titik berat pembahasan taktis Sun Tzu dalam tataran operasional pertempuran (Seskoad, 2015).

Penggunaan media siber dan media sosial sebagai alat yang efektif untuk organisasi dan mobilisasi dapat dijelaskan oleh beberapa teori komunikasi yang mapan. Agenda Setting Theory adalah teori yang menyatakan bahwa media massa merupakan pusat penentuan kebenaran dengan kemampuan media

massa untuk mentransfer dua elemen yaitu kesadaran dan informasi ke dalam agenda publik dengan mengarahkan kesadaran publik serta perhatiannya kepada isu-isu yang dianggap penting oleh media massa. Teori agenda setting pertama kali dikemukakan oleh Walter Lippman (1965) pada konsep "The World Outside and The Picture in Our Head" yang sebelumnya telah menjadi bahan pertimbangan oleh Bernard Cohen (1963) dalam konsep "The mass media may not be successful in telling us what to think, but they are stunningly successful in telling us what to think about". Penelitian empiris ini dilakukan Maxwell E. McCombs dan Donald L. Shaw ketika mereka meneliti pemilihan presiden tahun 1972. Mereka mengatakan, walaupun para ilmuwan yang meneliti perilaku manusia belum menemukan kekuatan media seperti yang disinyalir oleh pandangan masyarakat yang konvensional, belakangan ini mereka menemukan cukup bukti bahwa para penyunting dan penyiar memainkan peranan yang penting dalam membentuk realitas sosial kita. Itu terjadi ketika mereka melaksanakan tugas keseharian mereka dalam menonjolkan berita. Khalayak bukan saja belajar tentang isu-isu masyarakat dan hal-hal lain melalui media, mereka juga belajar sejauh mana pentingnya suatu isu atau topik dari penegasan yang diberikan oleh media massa.

Metode penelitian

Data primer dalam penelitian ini diperoleh dari pejabat-pejabat terkait kemanan siber dan agensi siber. Untuk data sekunder diperoleh dari studi pustaka dan dokumen yang berkaitan dengan keamanan siber. Penentuan personal yang menjadi narasumber data dilakukan dengan model *Purposive sampling,* yaitu dipilih dengan pertimbangan tertentu sesuai dengan tujuan penelitian. Yang menjadi objek penelitian dalam penelitian ini yaitu adalah keamanan nasional hasil dari penggunaan media siber.

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif analisis. Penelitian kualitatif adalah penelitian yang datanya dinyatakan dalam bentuk verbal dan dianalisis tanpa menggunakan teknik statistik. Fokus penelitian dalam metode kualitatif dan yang diteliti untuk melihat sejauh mana sikap dan kebijakan yang direncanakan mampu menjejaskan keamanan nasional. Penelitian difokuskan pada faktor-faktor kerawanan keamanan, sikap dan kebijakan.

Hasil dan Pembahasan

Hasil Penelitian diperoleh sebagai berikut:

a. Ancaman Siber Kepada Negara

Media siber menjadi kerawanan kepada negara karena serangan siber mudah dilakukan oleh mereka yang berilmu dan tidak semesti state actor. Serangan siber dilakukan secara asymmetric dan tidak memerlukan teknologi yang tinggi. Negara yang bergantung kepada internet dan rangkaian yang tinggi lebih tinggi adalah lebih rawan kepada serangan siber. Kebergantungan kepada peralatan dan sistem yang dibangunkan oleh negara luar menyebabkan kerawanan bertambah tinggi. Dari segi teknis, semua peralatan mempunyai kerawanannya sendiri. Sikap pegawai dan karyawan juga bisa membuka peluang kepada lawan melakukan serangan siber dengan jaya. Pemerintah juga harus memastikan rangkaian komunikasi meraka aman dan tidak mudah diserang oleh musuh.

Teori Keaman Nasional menurut Alan Collins (2003) adalah "*National security is the requirement tomaintain the survival of the nation-state through the useof economic, military and political power and the exercise of diplomacy*." Keamanan nasional adalah sebuah kebutuhan untuk menjaga ketahanan suatubangsa melalui daya ekonomi, militer serta kekuatan politik dan kepiawaianberdiplomasi. Karena sifat yang kompetitif diantara bangsa-bangsa, keamanan nasionaldengan negara yang mempunyai nilai sumber daya yang signifikan didasarkan kepada tindakan-tondakan teknis dan proses operasional. Hal ini berkisar dari perlindunganinformasi yang berkaitan dengan rahasia Negara untuk persenjataan bagi militer hingga strategi bernegosiasi dengan negara bangsa lain.

Ancaman adalah siber satu ancaman nyata (*real*) kepada sesebuah Negara. Ini didukung oleh data-data yang menunjukkan peningkatan serangan siber setiap tahun. Seiring dengan perkembangan teknologi, Senjata Siber (*cyber weapon*) menjadi bertambah canggih dan senang digunakan. Senjata Siber lebih murah, dan kadangkala boleh dibangunkan oleh sesaorang yang mahir dalam pengaturcaraan. Tidak banyak kos dan peralatan yang diperlukan tetapi modalnya hanya kemahiran dalam menulis kode-kode komputer dan dunia bisa tergoncang. Senjata siber

boleh digunakan oleh pihak-pihak berkepentingan bukan hanya *state actor*, malahan digunakan oleh penggnanas, penjenayah dll.

Ancaman siber tidak dapat memberi kemusnahan secara fizikal tetapi kemusnahannya adalah dalam bentuk maya dan mempunyai impak yang tinggi kepada sesebuah Negara. Kasus di Estonia dan Gerogia adalah contohnya nyata bagaimana serangan yang tidak memusnahkan fizikal tetapi bisa memberi dampak yang tinggi kepada negara tersebut. Stunext worm adalah contoh seranga siber yang tidak memusnahkan fizikal tetapi dapat memberi kesan kepada operasi nuklir Iran. Serangan siber boleh dilakukan sama ada secara *direct* atau menggunakan proxy melalui negara-negara lain yang susah untuk dikesan. Ini karena beberapa negara digunakan sebagai proxy dalam laluan serangan menyulitkan negara sasaran mengesan sumber serangan. Selain itu, penggodam atau penyerang bisa dari *state, non state*, kriminal, ekstrimis dan juga para amatur. Ancaman siber boleh melumpuhkan ekonomi, pentadbiran, sosial dll sesebuah negara. Serangan jenis *ransom ware* akan menyebabkan kerugian uang. Selain itu seranga kepada infrstruktur, transportasi dan administarsi akan memberi dampak ekonomi kepada negara yang diserang.

Berdasar semua uraian di atas, maka ditemukan bahwa media siber mampu memberi ancaman keamanan kepada negara sesuai dengan teori dan konsep keamanan negara yang digunakan dalam penulisan ini. Bermacam langkah perlu dilakukan bagi menangani permasalahan yang timbul dari media siber. Bermula dari pemerintah hingga ke pengguna yaitu rakyat dan karyawan perlu dididik ilmu keamanan siber agar dampak negatif tidak mudaratkan negara. Selain Pendidikan, perlu juga dibuat kebijakan, peraturan dan SOP sebagai panduan kepda karyawan dan rakyat agar semua dapat menggunakan media siber tanpa menjejaskan keamanan negara. Dengan spektrum ancaman yang besar dan luas, maka perlu dibuat satu komando bagi mengkoordinasi operasi semua instansi berkaitan siber seperti polisi, angkatan tentera, kementerian komunikasi dan lain-lain lagi. Jika semua instansi ini diintegarsi dan berkoordinasi, maka ancaman siber nasional dapat ditangani dengan tuntas dan efektif.

b.Faktor-faktor Kerawanan kepada Ancaman Siber

Teori Hukum Moore adalah salah satu hukum yang terkenal dalam industri mikroprosesor yang menjelaskan tingkat pertumbuhan kecepatan mikroprosesor. Dia mengatakan bahwa pertumbuhan kecepatan perhitungan mikroprosesor mengikuti rumusan eksponensial[2]. Oleh itu peralatan komputer berkembang dengan cepat karena mikroprosesor berkembang dengan eksponensial. Pihak yang terkait perlu senantiasa memastikan peralatan sistem pertahanan siber adalah senantiasa berada dalam teknologi terbaru.

Faktor Politik juga memain peranan dalam kerawanan siber. Kebijakan pemerintah dan sentimen kenegaraan dan politik bisa memicu serangan siber. Penyebaran virus komputer dapat merusak jaringan komputer yang digunakan oleh pemerintah, perbankan, pelaku usaha maupun perorangan yang dapat berdampak terhadap kekacauan dalam sistem jaringan. Dapat dipastikan apabila sistem jaringan komputer perbankan tidak berfungsi dalam satu hari saja dapat menimbulkan kekacauan pembayaran maupun transaksi keuangan bagi nasabah. Kondisi ini memerlukan kebijakan politik pemerintah untuk menanggulangi *cyber crime* yang berkembang.

Perilaku atau budaya masyarakat yang senang membagi-bagi data serta informasi (USB dan lisan) juga bisa mendedahkan diri kepada kerawanan siber. Segala kata sandi dan alamat internet perkakasan perlu disimpan rapi agar tidak diketahui pihak lain. Budaya ini perlu diperbetulkan agar tidak menjadi ancaman kepada negara sekiranya staf pemerintah tidak mengamalkan budaya kerja yang betul. Perilaku perkongsian lokasi dan gambar-gambar rahasia juga adalah penyebabnya berlaku kerawanan siber kepada negara. Rahasia-rahasia ini diketahui karena kesilapan staf sendiri dan bukannya dengan usaha pihak lain.

Daripada analisis di atas, ditemukan bahwa adalah sukar untuk memelihara keamanan siber karena terdapat spektrum ancaman yang luas. Bermula dari *human factors* hingga kepada faktor peralatan. Oleh itu diperlukan untuk pihak-pihak yang terkait untuk sentiasa mengikuti

[2] www.umsl.edu pada July 2017.

perkembangan peralatan siber. SDM harus sentiasa dilatih dan perlu dibuat perintah tetap atau SOP supaya mereka tidak cuai dalam melaksanakan penugasan. Pihak pemerintah juga harus sentiasa memperbaharui kebijakan agar kebijakan yang relevan digunakan. Kerawanan siber boleh ditangani dengan memberi pendidikan keamanan siber kepada karyawan dan rakayt. Biaya dan dana dari pemerintah perlu disediakan bagi mengimbangi perubahan dan perkembangan siber yang senantiasa berkembang. Peralatan harus sentiasa mampu menangkis serangan siber dan SDM juga harus bisa menjaga keamanan siber negara.

c. Tipe Ancaman Media Siber bagi Negara.

Terdapat banyak macam ancaman siber kepada negara seperti yang telah dibahas di sub judul di atas. Berdasarkan teori keamanan nasional oleh Allan Collins (2013), maka sub judul ini akan membahas dua tipe utama yang menjadi kerawanan utama kepada amanan nasional yaitu cyber spoinase dan propaganda siber.

Antara yang tipe ancaman yang paling ditakuti adalah cyber spoinase. Spionase cyber merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang computerized. [3]

Propaganda di media siber juga bisa mengancam kestabilan negara. Negara-negara seperti AS, China dan Rusia melakukan propaganda siber dalam mendapatkan pengaruh politik mereka. Pihak militer Rusia telah mengakui adanya upaya dalam skala yang cukup besar untuk melakukan perang siber. Seperti dilansir dari BBC.com, Menteri Pertahanan Rusia, Sergei Shoigu mengatakan adanya pasukan IT yang terlibat dalam intelijen untuk melakukan propaganda yang efektif. Selama berlangsungnya perang dingin, pihak Timur dan Barat mencurahkan segala bentuk upaya untuk sebuah propaganda. Proganda dibuat untuk mempengaruhi opini publik secara global serta untuk menjual ideologi – ideologi mereka.

[3] www.ebook.repo.mercubuana-yogya.ac.id pada July 2017.

Menurut Keir Gile, seorang pakar dibidang Militer Rusia, telah memperingati adanya Perang Siber yang telah disebar, sementara pihak barat terfokus pada Prajurit maya dan peretas. Tujuannya adalah untuk mengontrol informasi dengan segala cara. Rusia telah melakukan segala bentuk uji coba terhadap NATO. Mantan Panglima militer Rusia Jenderal Yuri Baluyevksy mengatakan bawah kemenangan dalam sebuah perang siber menjadi lebih penting ketimbang perang konvesional, karena tidak ada pertumpahan, tetapi dampaknya sangat luas, sehingga mampu melumpuhan struktur kekuatan musuh. [4]

Maka dapat ditemukan bahwa ancaman siber bisa datang dari *state actor* yang bisa jadi sipil dan militer juga menarget instansi pemerintah seperti ketanteraan, perusahaan dan elemen sipil. Ancaman siber juga bisa datang dari *non state actor* yang menyerang pemerintah tanpa koordinasi dan terkoordinasi. Justeru tipe ancaman siber kepada negara memang banyak dan spektrumnya begitu luas dan sukar untuk diprediksi. Pertahanan siber perlu mantap dan sentiasa mengikuti perkembangan teknologi. Perlunya semua instansi berkoordinasi agar spektrum ancaman yang luas ini dapat ditangani.

d. Potensi Serangan Siber oleh *State Actor*

Kebergantungan negara-negara kepada internet dan rangkaian membuka ruang untuk serangan. Dengan segala sistem telah mula menggunakan komputer dan dikoneksi melalui rangkaian komputer, ini membuka peluang dan ruang bagi begara lain melakukan serangan. Kegagalan mengamankan CNII akan memberi dampak yang teruk seperti yang berlaku di Estonia dan Georgia. Koordinasi segala agensi dan aparat peringkat nasional perlu dilakukan bagi mempertahankan aset-aset kritikal negara. Serangan seumpamanya boleh melanda mana-mana negara.

Teori Perang Clausewitz menyatakan bahwa perang merupakan kelanjutan dari kebijakan dalam bentuk lain sehingga perang memiliki makna yang sangat luas baik perang dalam bentuk fisik (atau menggunakan kekuatan *hard power*) maupun non fisik (*soft power*). Serangan siber bisa dilakukan melalui soft power tanpa

[4] www.mastel.id pada July 2017.

melakukan pertempuran. Bermacam cara bisa dilakukan bagi melakukan soft power seperti propaganda media social, penyadapan dan menggangu sistem pertahanan dan administrasi.

Teori Perang Clausewitz mengenai *Center of Gravity* mengatakan siapa yang mengusai ketinggian akan menang perang. Ketinggian pada hari ini membawa maksud teknologi. Kekuatan siber bisa memberi daya ganda kepada siapa yang menguasainya. Segala kekuatan musuh bisa dikuasai dan diserang melalui media siber. Ini telah berlaku di konflik di Estonia dan Georgia.

Serangan cyber, untuk mendukung operasi militer konvensional memiliki banyak potensi menjadi pengganda kekuatan pada medan pertempuran yang kompleks saat ini. Pada tahun 2008, skenario itu berlaku dalam konflik Russo-Georgia dengan operasi konvensional Rusia didukung dan kesuksesannya disempurnakan oleh serangan cyber yang terkoordinasi dengan hati-hati, melalui sebuah kekuatan pengganti, itu membuat Republik Georgia tidak mampu mempertahankan dirinya baik di dunia cyber mau pun domain fisik.

Konflik Russo-Georgia mungkin bukan insiden pertama kombinasi serangan di wilayah fisik dan dunia maya, namun ini adalah contoh bagus untuk melakukan serangan cyber melalui kekuatan proxy, ciri khas perang tidak konvensional, dukungan dari Strategik yang lebih besar dan tujuan operasional dari kekuatan konvensional. Serangan oleh milisi maya sangat penting untuk mengacaukan pemerintah Republik Georgia, yang menolaknya mengakses infrastruktur komunikasi kritisnya, dan membiarkan lawan mengendalikan persepsi konflik yang mengarah ke dan selama konflik aktual di lapangan. Orang-orang Rusia dapat memanfaatkan kekuatan inkinetik mereka yang signifikan dan mendapat keuntungan dari tindakan milisi cyber untuk mengalahkan orang-orang Georgia yang pasti. Pelajaran untuk mengambil dari kasus ini, dan untuk penelitian selanjutnya, mencakup manfaat dari kedua situasi atribusi yang suram dan kerja serentak senjata dan senjata kinetik. [5]

Maka dapat disimpulkan bahwa negara-negara *super power* sedang

[5]Monteray,2014

melakukan aktivitas siber baik aktif mau pun pasif. Konflik di Georgia adalah satu pengajaran bagaimana serangan siber digabungkan dengan serangan fisik bisa memberi kemenangan kepada pihak Rusia. Serangan siber di Estonia pula adalah satu kasus di mana hanya serangan siber tanpa serangan fisik bisa melumpuhkan sebuah negara. Maka sebuah negara itu harus mempunyai kesediaan agar serangan siber bisa dikalahkan. Perlunya badan bertindak siber ditubuhkan oleh semua negara bagi mengantisipasi serangan siber yang bakal mendatang.

e. **Penyadapan Oleh Negara Lain.**

Teori Perang Clausewitz menyatakan bahwa perang merupakan kelanjutan dari kebijakan dalam bentuk lain sehingga perang memiliki makna yang sangat luas baik perang dalam bentuk fisik (atau menggunakan kekuatan *hard power*) maupun non fisik (*soft power*). Teori Perang Clausewitz mengenai *Center of Gravity* mengatakan siapa yang mengusai ketinggian akan menang perang. Ketinggian pada hari ini membawa maksud teknologi. Kekuatan siber bisa memberi daya ganda kepada siapa yang menguasainya. Penyadapan siber memberi memberi kelebihan dari segi informasi untuk melakukan diplomasi politik, informasi ekonomi dan lain-lain.

State Hackers semakin menargetkan institusi pemerintah, fasilitas industri dan bisnis dengan teknik canggih yang mengganggu operasi, menyadap informasi rahasia dan juga dapat mengakibatkan kebocoran informasi dan kerugian pendapatan. Saat ini, baik organisasi publik maupun swasta tidak mengamankan data, informasi dan sistem siber dengan efektif. Banyak kasus di mana negara-negara aggressor mencurahkan sumber daya yang tampaknya tak terbatas untuk mencapai tujuan mereka, termasuk bakat waktu, uang, dan hacker. Negara yang diserang pula, tantangannya adalah dengan menyebarkan sumber daya yang terbatas dengan sangat efisien. [6]

Rusia dan China adalah dua negara yang menngunakan intelijen untuk ekonomi dan bisnes. Keduanya menyebarkan alat-alat malware yang canggih dan alat-alat yang lebih sederhana dan praktis untuk mencapai tujuan mereka. Dalam banyak kasus,

[6] www.tech.newstatesman.com pada July 2017

elemen umum dari serangan tersebut adalah eksploitasi elemen manusia dalam sebuah organisasi. Vektor serangan ini, mengeksploitasi komponen manusia di dalam infrastruktur target, juga meningkat dalam kompleksitas. Jadi bukan hanya bagian dari serangan yang canggih, tapi juga pengembangan eksploitasi titik lemah lainnya dalam perusahaan. Selain itu, kelompok kriminal mengadopsi alat dan teknik yang sama yang membuat kesenjangan antara penempatan oleh negara bangsa dan penyebaran oleh kelompok kriminal, dalam hal waktu dan kualitas, menyusut. [7]

Rusia selain mereka tetap berkomitmen untuk mengacak informasi bisnis yang akan membantu persaingan mereka di dunia, prioritas utama mereka adalah mengumpulkan informasi militer dan diplomatik. Untuk tujuan ini, mereka telah menempatkan talenta dan sumber daya yang signifikan untuk menargetkan jaringan pemerintah A.S. untuk mengumpulkan informasi diplomatik yang memberi mereka keuntungan dalam negosiasi atau keputusan strategis karena informasi ini memungkinkan mereka untuk memprediksi posisi strategis dan keputusan A.S.

Sebagai perbandingan, tujuan utama kemampuan pengumpulan cyber China adalah memungkinkan Badan Usaha Milik Negara (BUMN) bersaing dan mendominasi pada tingkat ekonomi global. Selama dasawarsa terakhir, para profesional cybersecurity telah mencatat adanya peningkatan jumlah intrusi jaringan yang mengakibatkan penggusuran informasi bisnis, termasuk komunikasi IP dan eksekutif. Itu adalah ciri khas kelompok hacking China, khususnya Grup 61398, yang dikenal mencuri rahasia dagang dari perusahaan seperti Westinghouse dan US Steel.

Upaya Grup 61398 untuk menargetkan teknologi dan informasi bisnis yang memajukan sektor industri strategis China merupakan lambang dari inisiatif hacking China. Analis Cybersecurity secara langsung mengkorelasikan industri kunci China berusaha untuk tumbuh dengan sektor yang mereka targetkan dengan serangan cyber. Justeru perlu untuk melindungi informasi di jaringan yang

[7] *Ibid.*

mungkin bernilai bagi musuh ekonomi yang canggih seperti China. [8]

Tindakan dari Snowden, mantan kontraktor NSA yang membongkar dan membocorkan ke media kegiatan mata-mata NSA dan Australia Signal Directorate (ASD), kini makin berkembang, menyentuh, dan membuat resah demikian banyak negara di dunia. NSA dalam kaitan komunitas 5-Eyes (AS, Inggris, Australia, Kanada, dan Selandia Baru) melakukan tindak spionase, memonitor sistem komunikasi negara-negara dan bangsa lain, termasuk 35 kepala negara. Khusus ASD di bawah kendali Amerika Serikat (AS) melakukan tindak spionase di kawasan Asia. Direktur NSA Jenderal Keith Alexander akhirnya mengakui bahwa NSA melakukan penyadapan. Selain itu, Alexander menegaskan bahwa tugas penyadapan tersebut diperintahkan oleh diplomat dan parlemen AS sendiri.[9] Maka dapat ditemukan bahwa negara-negara *super power* memang melakukan kegiatan penyadapan baik untuk tujuan intelijen, memerangi teroris, kekuatan diplamatik dan perdagangan. China dan Rusia telah berjaya dalam ekonominya dengan menjalankan penyadapan bagi tujuan ekonomi. Kelompak 5 Eye telah menjadikan upaya memonitor teroris kepada upaya memonitor negara lain bagi tujuan strategis. Oleh itu perlunya instansi-instansi negara bergabung bagi melindungi negara dari kegiatan penyadapan oleh negara lain. Perlu dilakukan koordinasi tehadap semua instansi yang terkait dalam menangani penyadapan terhadap negara. Pemerintah juga sebaiknya melakukan *road show* ke seluruh kementerian dan badan pemegang rahasia negara, untuk meningkatkan kesadaran sekuriti dalam menghadapi teknologi penyadapan yang sangat canggih itu.

f. **Media Sosial Mengubah Pemerintahan.**

Media siber bisa digunakan sebagai medium bagi menyalurkan idea dan propaganda dalam mengubah pemerintahan. Negara-negara mundur amat rawan jika media siber digunakan sebagai penyebaran propaganda.

Teori *Agenda Setting* yang diperkenalkan oleh McCombs dan DL Shaw (1972) mengatakan bahwa jika media memberi tekanan pada suatu

[8] *Ibid.*

[9] www.tni-au.mil.id pada Agustus 2017.

peristiwa, maka media itu akan mempengaruhi khalayak untuk menganggapnya penting. Jadi apa yang dianggap penting media, maka penting juga bagi masyarakat. Dalam hal ini media siber diasumsikan memiliki efek yang sangat kuat, karena masyarakat bisa mengakses informasi tanpa kontrol pemerintah. Dengan negara-negara mengenakan kontrol media radio dan televisi, media siber tidak bisa dikontrol karena ia masih baru dan bersifat internasional dan luar batas negara.

Teori ketergantungan terhadap media mula-mula diutarakan oleh Sandra Ball-Rokeach dan Melvin Defleur. Teori ini memprediksikan bahwa khalayak tergantung kepada informasi yang berasal dari media massa dalam rangka memenuhi kebutuhan khalayak bersangkutan serta mencapai tujuan tertentu dari proses konsumsi media massa. Namun perlu digarisbawahi bahwa khalayak tidak memiliki ketergantungan yang sama terhadap semua media. Contohnya orang muda dan berpendidikan lebih cenderung menngunakan media siber dalam mendapat informasi.

Situasi yang berlaku saat Arab Spring amat terakait denga kedua-dua teori ini. Kebangkitan Arab muncul lewat 2010 untuk membantah kekuasaan pemerintah authoritarian yang bermula dari Libya, Tunisia, Bahrain, Syria dan seterusnya merebak ke negara Timur Tengah dan Afrika Utara dan salah satu darinya adalah Mesir. Kebangkitan ini menular dengan pantas kerana adanya media sosial untuk menyebarkan dan mencambah setiap isu sensitif kegawatan negara Mesir. Ia juga telah menjambat beribu-ribu rakyat Mesir untuk bersatu dan keluar berdemonstrasi di jalanan untuk menyokong penyingkiran rejim pemerintahan Mubarak. Media sosial telah memberi impak terhadap pengetahuan, sikap dan tingkah laku khalayak merentasi global.[10]

Teori *Agenda Setting* telah berjaya dilaksanakan di dalam Arab Spring. Ini dapat dibuktikan dengan konfesi Presiden Turkey Academy of Military Sciences, Gen Makhmut Gareyev (2013) mengatakan bahwa teknologi informasi yang bersifat subversif yang telah dibangun oleh negara barat sejak 2011 adalah punca

[10] Ahmad, 2017

kejatuhan pemerintahan di Mesir, Tunisia dan Libya setelah 2 tahun dibangun. Situasi sebelum kerusuhan juga di simulasi dengan sengaja mencetuskan provokasi untuk melihat tindakan pihak pemerintah dalam dua tahun itu. Akhirnya media siber digunakan bagi memanggil rakyat berdemonstarsi hingga dapat menjatuhkan pemerintah. Berita yang dimasukkan setiap hari selama dua tahun itu telah berjaya membentuk opini publik untuk menjelekkan pemerintah. Akhirnya masyarakat tidak mempercayai pemerintah dan pemerintahan di negara-negara tersebut telah berjaya ditukarkan.

Pada temuan penulis, rakyat pada hari ini memang tidak bisa dijauhkan dari media sosial seperti facebook, tweter, whatapp dan lain-lain. Hampir setiap jam pengguna media sosial akan mendapat masukan baru yang belum tentu kebenarannya kandungannya. Oleh itu perlunya undang-undang bagi mengontrol supaya informasi yang berbaur fitnah tidak sewenang-wengangnya berlegar di internet. Rakyat juga perlu dididik agar dapat menapis informasi supaya mereka bisa menilai kebenaran sesuatu informasi. Pemerintah juga perlu mewujudkan badan penangkis propaganda agar rakyat tidak terpengaruh dengan propaganda musuh negara.

g. **Cyber Terorisme**

Teroris mengunakan media siber dalam menjalan operasi mereka. Justeru perlu untuk pihak pemerintah memonitor aktivitas ini agar terorisme tidak berkembang. Media social dan siber digunakan karena bisa diakses oleh banyak orang dan teroris bisa berkomunikasi sesama mereka dalam aktivitas ini. Penggunaan siber memberikan *outreach* yang luas dalam mengembangkan agenda ekstrimis. Penggunaan media sosial amat berkesan kerana jaringan tanpa batasan dan luas senang digunakan untuk menyebarkan ideology teror. Penyebaran ideologi ekstrimis/teroris melalui media sosial telahpun berhasil. Bukti-bukti yang dikeluarkan menunjukkan kempanye perkaderan yang dijalankan oleh ISIS telah berjaya menarik ribuan pengikut untuk turut sama berjuang. Ini menunjukkan media sosial adalah medium yang berkesan untuk penyebaran ideologi ektrimis/teroris.

Penulisan ini menguraikan dua teori media dalam membahas isu cyber

terrorism yaitu Teori *Agenda Setting* dan Teori Kebergantungan Media. Teori *Agenda Setting* yang diperkenalkan oleh McCombs dan DL Shaw (1972) mengatakan bahwa jika media memberi tekanan pada suatu peristiwa, maka media itu akan mempengaruhi khalayak untuk menganggapnya penting. Maka dengan isu yang membangkitkan semangat dan ideologi yang sering dimainkan berulang-ulang bisa mempengaruhi pemikiran dan semangat melakukan aksi terror. Teori ketergantungan terhadap media mula-mula diutarakan oleh Sandra Ball-Rokeach dan Melvin Defleur. Teori ini memprediksikan bahwa khalayak tergantung kepada informasi yang berasal dari media massa dalam rangka memenuhi kebutuhan khalayak bersangkutan serta mencapai tujuan tertentu dari proses konsumsi media massa. Namun perlu digarisbawahi bahwa khalayak tidak memiliki ketergantungan yang sama terhadap semua media. Dalam kasus ini, mereka yang cenderung kepada ideologi perjuangan kelompok teror akan cenderung mencari informasi berkaitan teroris. Maka media siber adalah tempat yang baik bagi meluaskan ideologi teroris karena ia bisa diakses keseluruh dunia.

Para teroris dapat memanipulasi media siber bagi mendapat komunikasi yang aman. Beberapa alternatif lain yang mereka gunakan bisa seperti Telegram yang sudah sejak awal ditujukan untuk komunikasi mobile yang aman. Penggunaan aplikasi dengan enkripsi seperti Telegram juga sebenarnya masih terbuka dengan kelemahan, tapi untuk menerobosnya dibutuhkan upaya yang cukup rumit bagi kebanyakan orang biasa. Tidak semua mampu perusahaan telekomunikasi bisa menangkap komunikasi rahasia seperti ini. Tools yang menyediakan komunikasi yang aman via internet malah sudah tersedia banyak bahkan diantaranya gratis.

Teroris juga bisa memprogram dan membuat aplikasi sendiri. Sebagian kelompok teroris lebih percaya dengan aplikasi buatan sendiri dalam berkomunikasi dan membuat kontak dengan anggotanya. Berbagai kelompok teroris juga memiliki tim teknis yang membuat aplikasi bagi kelompoknya. Tidak hanya berbasis dekstop, kini beberapa aplikasi mobile juga sudah dibuat dengan semakin

populernya platform android yang digunakan hampir di seluruh dunia.

Maka dengan pembahasan di atas, ditemukan bahwa media siber memberi banyak kelebihan kepada teroris dalam melakukan operasi meraka. Selain dari penyebaran ideologi, media siber bisa menjadi medan komunikasi aman untuk teroris, media penggerak operasi, sumber pengumpulan dana dan juga sebagai *data mining*. Oleh itu instansi pemerintah dan pasukan keamanan harus siap dan mempunyai pasukan yang bisa menanggulangi aktivitas teroris yang menggunakan media siber dalam operasi mereka. Semua pasukan keamanan harus terintegrasi dan bisa melakukan operasi secara bersama. Segala data dan sistem harus terkoneksi dan bisa dikongsi bersama instansi keamanan.

h. Langkah Mengatasi Serangan Siber

Untuk mengkonseptualisasikan keamanan siber dan mengembangkan kebijakan perlindungan, kita perlu membagi dunia siber mengikut kategori dimana kerentanannya paling mungkin terjadi. Salah satu kemungkinan adalah menganalisis dunia siber di berbagai tingkat, setiap tingkat menunjukkan konsekuensi yang berbeda dari gangguan infrastruktur maya. Konsekuensi dari insiden cyber dan mekanisme respons yang tepat sangat berbeda di tingkat global, regional dan negara-negara dari pada tingkat struktur masyarakat, sektor ekonomi atau individu. Tapi semua tingkat ini terhubung erat di dunia maya, dan setiap sistem respons yang efektif perlu ditangani secara bersamaan. [11]

Maka Penulis menemukan bahwa penanganan ancaman siber kepada negara bisa dilakukan dengan diintegrasikan semua elemen dan instansi yang terkait dengan keamanan siber. SOP dan bidang tugas juga harus dijelaskan supaya tidak berlaku pertindihan tugas. Perlu juga dilakukan kampanye kesadaran keamanan siber supaya pengguna mengetahui cara yang aman dan benar menggunakan media siber.

1) Penanganan ancaman Siber Tingkat Global dan Regional

Gangguan infrastruktur informasi di tingkat global dan regional akan memberi implikasi yang besar dan serius apabila diserang. Meskipun

[11]Tiirmaa (2011). Cyber Security Threats and responses : at Global, Nation-State. http://www.ceri-scienes-po.org pada 4 Juni 2017

gangguan global dan regional hampir tidak menjadi sasaran aktor internasional yang bertanggung jawab, secara teoritis hal tersebut dapat terjadi sebagai secara tidak disengajakan dalam menggunakan serangan cyber sebagai bagian dari konflik yang dikombinasikan dengan bentuk serangan fisik. Misalnya, jika dua kekuatan regional berusaha melemahkan satu sama lain, salah satunya (negara X) dapat meluncurkan serangan cyber operasi bersamaan dengan serangan fisik terhadap infrastruktur informasi (kabel optik, router dll) dengan bertujuan untuk mengganggu kegiatan ekonomi di negara lain (negara Y) untuk tujuan politik. Tetapi karena sistem keuangan regional dapat bergantung pada layanan keuangan yang diberikan oleh negara Y, ini akan menyebabkan gangguan yang serius untuk pusat keuangan di dekatnya, sehingga menyebabkan penurunan PDB yang serius di negara lain di wilayah ini. Data yang tidak bisa melewati kabel akan melalui satelit dan koneksi lainnya justeru akan membebani kapasitas sektor ICT, yang kemudian dapat menyebabkan efek domino yang berbeda di wilayah lain. Di tingkat global dan regional, mekanisme tanggap insiden internasional dan jaringan kerja sama formal perlu dibentuk oleh pemerintah, organisasi internasional dan komunitas pemangku kepentingan perusahaan sektor TIK untuk menjamin kemampuan pengelolaan kejadian dalam kasus adanya gangguan global.[12]

Maka penulis menemukan bahwa perlu diadakan kerjasama sesama negara bagi menangani masalah siber diperingkat regional dan dunia. Ini boleh dilaksanakan dalam PBB atau Interpol bagi bekerjasama dalam kerjasama keamanan siber. Ini karena jika negara itu diserang secara siber, maka negara lain dan regional juga bisa terkena dampak ekonomi. Selain daripada itu, aktivitas kriminal dan teroris dunia bisa ditangani dengan kesatuan dan integrase operasi negara-negara di dunia.

[12] *Ibid.*

2) **Penanganan ancaman Siber Nasional Tingkat Negara**

Kategori kerentanan kedua menyangkut tingkat negara bangsa. Salah satu konflik yang paling ditakuti di dunia siber adalah serangan siber yang menghancurkan terhadap infrastruktur penting sebuah negara dilakukan dengan bersama serangan fisik. Namun, serangan siber selama konflik militer tidak akan menjadi masalah bagi analis karena dalam kasus perang yang meluas, akan memungkinkan untuk menerapkan kerangka undang-undang internasional yang mencakup konflik bersenjata, dan mengatur aspek kemanusiaan dari sebuah konflik. Hukum Konflik Bersenjata dan Hukum Humaniter Internasional menetapkan persyaratan untuk menghindari korban di kalangan penduduk sipil, menahan diri dari tanggapan yang tidak proporsional, untuk mempertimbangkan efek sekunder dan tertier dll.[13]

Skenario yang sangat mungkin terjadi dalam konflik modern masa depan adalah penggunaan organisasi kriminal mengunakan media siber sebagai proxy negara lain. Kriminal mungkin kehilangan jejak dan mereka bersembunyi di balik fakta bahwa peraturan nasional dalam mengkriminalkan kejahatan cyber sangat sama antara negara dengan negara yang lain. Petugas penegak hukum terbebani dan tidak ada cukup perhatian yang diberikan pada masalah kejahatan siber internasional.

Negara-negara juga harus menghadapi kemungkinan serangan teroris yang menggunakan metode cyber atau menggunakan gabungan kekuatan serangan fisik dan cyber untuk mencapai tujuan sebuah operasi. Meskipun koordinasi anti-teror di antara negara-negara telah diperkuat setelah 9/11 dan sebagian besar negara di dunia bekerja sama di bidang ini, kemungkinan adanya ancaman dan respons akan mendapatkan pengetahuan yang diperlukan dan menggunakan metode cyber dalam operasi mereka. Perlu diketahui bahwa sejauh ini para teroris belum melakukan serangan nyata terhadap infrastruktur internet. Ini karena

[13] *Ibid.*

mereka membutuhkan internet sebagai alat rekrutmen dan tidak ingin merugikan media utama yang memfasilitasi komunikasi mereka.[14]

Maka Penulis menemukan bahwa penanganan ancaman siber kepada negara bisa dilakukan dengan diintegrasikan semua elemen dan instansi yang terkait dengan keamanan siber. SOP dan bidang tugas juga harus dijelaskan supaya tidak berlaku pertindihan tugas.

3) **Penanganan ancaman Siber Nasional Tingkat Masyarakat**

Kategori kerentanan ketiga terkait dengan dampak sosial dari aktivitas berbahaya di internet. Ini mencakup rekayasa sosial yang mengurangi kepercayaan di antara orang-orang, dan juga metode maya yang digunakan untuk mengagitasi, meneror, menyebarkan, atau menganggap tokoh masyarakat atau kelompok tertentu di masyarakat.

Teknologi informasi dan komunikasi yang berkembang pesat telah meningkatkan komunikasi massa dan media-medianya ke tempat yang menonjol di masyarakat modern. Di era di mana media bergerak ke Internet dan komunikasi sosial beralih ke Chat room elektronik, kerusakan teknologi apapun akan mempengaruhi sejumlah besar orang. Pencurian identitas melalui jejaring sosial menempati peringkat sebagai ancaman cyber paling umum dalam beberapa tahun terakhir, dan banyak orang masih belum mengetahui bagaimana cara menghindari serangan semacam ini terhadap identitas mereka.

Maka penulis menemukan bahwa yang paling penting dalam menangani ancaman peringkat masyarakat adalah dengan mengadakan kampanye kesaran keamanan siber agar semua pihak tau bagaimana menjaga keamanan siber untuk diri sendiri, masyarakat dan negara.

4) **Individu**

Kategori terakhir adalah meningkatnya kegiatan berbahaya di dunia maya oleh individu pengguna komputer. Dalam kebanyakan skenario insiden siber, individu akan terpengaruh oleh gangguan siber dan akan menderita

[14] Ibid.

dari hilangnya layanan yang support kehidupan sehari-hari mereka. Dengan malapetaka siber buatan manusia atau teknologi, sebagian besar konsekuensinya bisa sangat tidak terduga, memiliki efek sekunder dan tersier. Bahkan pendekatan yang paling canggihpun tidak bisa menentukan secara pasti semua saling ketergantungan antara infrastruktur informasi penting yang mendukung fungsi normal masyarakat.

Individu yang cuai juga merupakan ancaman di dunia maya jika komputer mereka yang tidak dilindungi akan digunakan sebagai bagian dari tentara komputer yang tidak terkoordinasi. Kerentanan serius tambahan pada tingkat individu yang patut mendapat perhatian adalah kelalaian pegawai. *Human negligence* dan kurangnya kemahiran adalah juga punca serangan luaran dan dalaman.[15]

Maka penulis dapat menemukan bahwa unsur manusiawi juga adalah rawan kepada keamanan siber. Maka perlu diadakan kampanye bagi menyadarkan rakyat dan karyawan agar menggunakan internet dengan aman dan mematuhi SOP yang telah dikeluarkan.

Kesimpulan dan Saran

Berdasarkan pokok hasil penelitian dan analisis pada bab-bab sebelumnya dapat disimpulkan bahwa media siber mempunyai kerawanan yang bisa dimanipulasi bagi mengancam keamanan negara. Maka pihak pemerintah perlu mengambil langkah-langkah yang sewajarnya untuk mengelakkan siber menjadi medan mengancam keamanan nasional.

a. Media Siber Mampu Mengancam Keamanan Nasional.

1) Ancaman Siber Kepada Negara

Secara keseluruhan, ancaman siber kepada negara adalah nyata (real) dan bisa dilakukan oleh *state* dan *non state actor*. Senjata Siber (cyber weapon) menjadi bertambah sofistikated dan senang digunakan. Senjata Siber lebih murah dan boleh dibangunkan oleh seorang yang mahir dalam pengaturcaraan. Serangan dilakukan sama ada secara *direct* atau menggunakan proxy melalui negara-negara lain yang sulit untuk dikesan. Ancaman siber boleh melumpuhkan ekonomi, administrasi, sosial dan lain-lain bagi sebuah negara. Negara yang

[15] Ibid.

tinggi bergantungnya kepada internet dan rangkaian komputer adalah lebih rawan kepada serangan siber.

2) **Faktor-faktor Kerawanan kepada Ancaman Siber**

   Adalah sukar untuk memelihara keamanan siber karena terdapat spektrum ancaman yang luas. Bermula dari *human factors* hingga kepada faktor peralatan. Kebijakan perlu senantiasa dikaji bagi memastikan kebijakan dan hokum yang digunakan masih relevan.

3) **Tipe Ancaman Media Siber kepada Negara**

   Maka dapat ditemukan bahwa ancaman siber bisa datang dari *state actor* yang bisa jadi sipil dan militer juga menarget instansi pemerintah seperti ketanteraan, perusahaan dan elemen sipil. Ancaman siber juga bisa datang dari *non state actor* yang menyerang pemerintah tanpa koordinasi dan terkoordinasi. Justeru tipe ancaman siber kepada negara memang banyak dan spektrumnya begitu luas dan sukar untuk diprediksi. Pertahanan siber perlu mantap dan sentiasa mengikuti perkembangan teknologi. Perlunya semua instansi berkoordinasi agar spektrum ancaman yang luas ini dapat ditangani.

4) **Potensi Serangan Siber oleh *State Actor***

   Kebergantungan negara-negara kepada internet dan rangkaian membuka ruang untuk serangan. Kegagalan mengamankan CNII akan memberi dampak yang teruk seperti yang berlaku di Estonia dan Georgia. Negara-negara *super power* sedang melakukan aktivitas siber baik aktif mau pun pasif. Maka sebuah negara itu harus mempunyai kesediaan agar serangan siber bisa dikalahkan.

5) **Penyadapan Oleh Negara Lain**

   Maka dapat ditemukan bahwa negara-negara *super power* memang melakukan kegiatan penyadapan baik untuk tujuan intelijen, memerangi teroris, kekuatan diplamatik dan perdagangan. China dan Rusia telah berjaya dalam ekonominya dengan menjalankan penyadapan bagi tujuan ekonomi. Kelompak *5 Eye* telah menjadikan upaya memonitor teroris kepada upaya memonitor negara lain bagi tujuan strategis. Oleh itu perlunya instansi-instansi negara bergabung bagi melindungi negara dari kegiatan penyadapan oleh negara lain. Perlu dilakukan koordinasi tehadap semua instansi yang terkait dalam menangani penyadapan terhadap negara.

6) **Media Sosial Mengubah Pemerintahan**

Rakyat pada hari ini memang tidak bisa dijauhkan dari media sosial seperti facebook, tweter, whatapp dan lain-lain. Hampir setiap jam pengguna media sosial akan mendapat masukan baru yang belum tentu kebenarannya kandungannya. Oleh itu perlunya undang-undang bagi mengontrol supaya informasi yang berbaur fitnah tidak sewenang-wengangnya berlegar di internet. Rakyat juga perlu dididik agar dapat menapis informasi supaya mereka bisa menilai kebenaran sesuatu informasi. Pemerintah juga perlu mewujudkan badan penangkis propaganda agar rakyat tidak terpngaruh dengan propaganda musuh negara.

7) **Cyber Terrorism**

Maka dapat ditemukan bahwa teroris mengunakan media siber dalam menjalan operasi mereka. Justeru perlu untuk pihak pemerintah memonitor aktivitas ini agar terorisme tidak berkembang. Media sosial dan siber digunakan karena bisa diakses oleh banyak orang dan teroris bisa berkomunikasi sesama mereka dalam aktivitas ini. Penggunaan siber memberikan *outreach* yang luas dalam mengembangkan agenda ekstrimis. Penggunaan media sosial amat berkesan kerana jaringan tanpa batasan dan luas senang digunakan untuk menyebarkan ideology teror. Penyebaran ideologi ekstrimis/teroris melalui media sosial telahpun berhasil. Ditemukan bahwa media siber memberi banyak kelebihan kepada teroris dalam melakukan operasi meraka.

b. Langkah Mengatasi Serangan Siber

Maka ditemukan bahwa terdapat beberapa macam yang bisa dilakukan dalam menghindar dan menangani serangan siber. Antara cara adalah

1) Pertahan siber yang diperkuat.
2) Penyelarasan dan kerjasama serta komunikasi secara berkesan di antara semua agensi berkaitan di dalam perkongsian maklumat dan bertindakbalas dengan pantas.
3) Kepahaman semua agensi mengenai tahap ancaman perlu dicapai dengan perkongsian maklumat seperti katalog kelemahan, analisis impak dan sebagainya. Tahap ancaman perlu dikenalpasti secara terperinci supaya semua pihak mempunyai kepahaman yang sama.

Saran

Berdasarkan analisis dan kesimpulan di atas, disarankan kepada pihak pemerintah dan yang berkait dengan langkah tindak lanjut sebagai berikut:

a. Memaksimalkan kemahiran lokal dalam pembangunan infrastruktur teknologi informasi nasional.
b. Menjalinkan kerjasama internasional dan regional dalam bidang siber agar ancaman siber dalam kriminal, teroris dan lain-lain dapat ditangani melangkaui batas negara.

Daftar Pustaka

Buku

Creswell, J. W. (2014). Research design: Pendekatan kualitatif, kuantitatif, dan mixed. Yogyakarta: Pustaka Pelajar.

Castell. (1996). *The Rise of Network Society*. West Sussex: Wiley-Blackwell.

Depdikbud. (1994). *Kamus Besar Bahasa Indonesia.* Jakarta : Balai Pustaka.

Indrawan, Rully & R. Poppy Yaniawati. 2014. *Metode penelitian, Kuantitatif, Kualitatif, dan campuran untuk manajemen, pembangunan, dan pendidikan*. Bandung : Refika Aditama.

Miriam B. (2009). Dasar-dasar Ilmu Politik. Jakarta : PT.Gramedia Pustaka.

Sekolah Staf dan Komando TNI AD. (2010). *Kajian Triwulan IV*. Bandung.

Sekolah Staf dan Komando TNI AD. (2016). *Pedoman Penyusunan Karya Tulis Militer Ilmiah*. Bandung.

Sugiyono. (2014). *Memahami penelitian kualitatif*. 2014. Bandung : Alfabeta.

United States Joint Command (2006). Informations Operations.

United States Joint Command (2003). Phycological Operations.

Jurnal

Amos Granit (March 2010). Cyberspace as a Military Domain – In What Sense? Institute for Intelligence Studies at IDF Military Intelligence.

Ball, Desmond, and Gary Waters. "Cyber Defence and Warfare." Security Challenges 9, no. 2 (2013): 91-98.

Ball, Desmond. "China's Cyber Warfare Capabilities." Security Challenges 7, no. 2 (Winter 2011): 81-103.

Baylon, Caroline, Roger Brunt, and David Livingstone. "Cyber Security at Civil Nuclear Facilities: Understanding the Risk." Chatham House. 2015.

Beidleman, Scott W. "Defining and Deterring Cyber War." Master's thesis, U.S. Army War College, June 2009.

Bejtlich, Richard. "Outside Perspectives on the Department of Defense Cyber Strategy." The Brookings Institution. September 29, 2015.

Bendiek, Annegret and Tobias Metzger. "Deterrence theory in the cyber-century: Lessons from a state-of-the-art literature review." Lecture Notes in Informatics (LNI), Gesellschaft fur Informatik, Bonn, 2015.

Benitz, Jorge, and Jason Healey. "Cyber Offense is King." The Atlantic Council. July 30, 2012.

Borum, Randy, and Ronald Sanders. "Cyber Intelligence: Preparing Today: for Tomorrow's Threats." Intelligence and National Security Alliance, 2015.

Collins, Alan (2003). Security and Southeast Asia: domestic,regional and global issues ,Singapore: ISEAS

Cilluffo, Frank J., and Joseph R. Clark. "Preparing for Netwars: Repurposing Cyber Command." The Journal of International Security Affairs (2012):111-118.

Cilluffo, Frank J., Sharon L. Cardash, and George C. Salmolraghl. "A Blueprint for Cyber Deterrence: Building Stability through Strength." Military and Strategic Affairs 4, no. 3 (December 2012): 3-23.

Clarke, Richard A. "Securing Cyberspace through International Norms: Recommendations for Policymakers and the Private Sector." Good Harbor Security Risk Management, LLC. 2012.

Clayton, Blake and Adam Segal. "Addressing Cyber Threats to Oil and Gas Suppliers." Council on Foreign Relations. 2013.

Colby, Elbridge. (June 24, 2013). "Cyberwar and the Nuclear Option." The National Interest.

Collins, Alan, (2003). Security and Southeast Asia: domestic,regional and global issues ,Singapore: ISEAS.

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. "On Cyber Warfare." Chatham House. 2010.

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. "Cyber Security and the UK's Critical National Infrastructure." Chatham House. 2011.

Cornish, Paul, Rex Hughes, and David Livingstone. "Cyberspace and the National Security of the United Kingdom." Chatham House. 2009.

Craig, Anthony and Brandon Valeriano. "Conceptualising Cyber Arms Races." Presented at the 8th International Conference on Cyber Conflict, Tallinn, Estonia, 2016.

CSIS Commission on Cybersecurity for the 44th President. "A Human Capital in Crisis: Technical Proficiency Matters." Center for Strategic and International Studies. November 2010.

CSIS Commission on Cybersecurity for the 44th President. "Securing Cyberspace for the 44th Presidency." Center for Strategic and International Studies. December 2008.

Eidman, Christopher R. Monterey (2014). Unconventional cyber warfare: cyber opportunities in unconventional warfare, California: Naval Postgraduate School.

Fauziah (2017). Kebergantungan Media Sosial Terhadap Isu Arab Spring Dalam Kalangan Khalayak di Malaysia, Jurnal Komunikasi Malaysian Journal of Communication Jilid 33(1)2017: 423-437, Universiti kebangsaan Malaysia.

Federal Ministry of the Interior. (February 2011) "The New Cyber Security Strategy for Germany,"Berlin.

Lynn, WJ. (February 15, 2011) "Remarks on Cyber at the RSA Conference" ,as delivered by, III, San Francisco, California.

Noor, Elina. (2011) "The Problem with Cyber Terrorism." In SEARCCT's Selection of Articles Vol. 2, 51-64.

Sebastian M. Convertino II, Lou Anne DeMattei, Tammy M. Knierim, (July 2007)). Flyingand Fighting in Cyberspace. Alabama: Air University Press.

The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028 (22 February 2010).

Weedon, Jen. (2015). "Beyond 'Cyber War'" Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine." In Cyber War in Perspective: Russian Aggression against Ukraine, ed.

Kenneth Geers, 67-78. Tallinn: NATO CCD COE Publication.

Wirtz, James J. (2015) "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy." In Cyber War in Perspective: Russian Aggression against Ukraine, ed. Kenneth Geers, 29-38. Tallinn: NATO CCD COE Publication.

Joint Publication 3 – 13 : Joint Operations, Feb 2006

Web

Bernama. (2017). "Ubah kempen cara lama. Pada 31 Januari 2017." http://www.utusan.com.my/berita/politik/ubah-kempen-cara-lama-ahmad-zahid-1.434300/bn-nasional-1.434305

El-Nawawy. Kamis. (2012) "Cyberactivists Paving the Way for the Arab Spring: Voices from Egypt, Tunisia and Libya." Pada 1 May 2017. http://www.cyberorient.net/article.do?articleId=7994

Indonesia dalam Situasi Perang Generasi Keempat (2016). http://www.beritasatu.com/nasional/351486-indonesia-dalam-situasi-perang-generasi-keempat.html

Jagatreview (2015). "Waspada! Tren Terbaru Serangan Spionase Cyber – EquationDrug" http://www.jagatreview.com/2015/03/pr-waspada-tren-terbaru-serangan-spionase-cyber-equationdrug/ diakses pada 25 Agusuts 2017.

Mudzakir Maruf (2016). Indonesia Ketar-ketir Lawan Cyberterrorism. https://semarak.news/2016/11/22/10781-indonesia-lawan-cyberterrorism.html

Leo Taddeo (2017). "Nation-state cyber attacks come out of the shadows" http://tech.newstatesman.com/guest-opinion/nation-state-cyber-attacks-come-shadows diakses pada 1 Juni 2017.

Marsda TNI (Pur) Prayitno Ramelan (2013). "Opini Pray Tentang Penyadapan NSA dan ASD di Harian Sindo." https://tni-au.mil.id/pustaka/opini-pray-tentang-penyadapan-nsa-dan-asd-di-harian-sindo pada 10 Agustus 2017.

Mohammad. (2014) Keamanan Nasional. Pada 30 May 2017 https://polmas.wordpress.com/2014/10/10/keamanan-nasional/.

Perang Generasi Ke 4 (Fourth Generation Warfare). Pada 14 Juni 2017. http://strategitaktik.blogspot.com/2013/08/perang-generasi-ke-4-fourth-generation.html.

Perang Generasi Ke 4 (Fourth Generation Warfare). Pada 14 Juni 2017. http://strategitaktik.blogspot.com/2013/08/perang-generasi-ke-4-fourth-generation.html.

Republika.co.id (2016) http://trendtek.republika.co.id/berita /trendtek/internet/17/05/23/oqd8kn313-negara-dengan-pertahanan-siber-yang-lemah-bakal-merugi pada 27 Agustus 2017

Ryan, Y. (2011). Anonymous and the Arab uprisings The cyber activists discuss their work and the broader global push for freedom of speech and freedom from oppression. Pada 5 Mei 2017 http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html

Robert Farley (2016). Just How Wide-Reaching Are China's Economic Espionage Efforts? http://thediplomat.com/2016/12/just-how-wide-reaching-are-chinas-economic-espionage-efforts/ diakses pada 25 Agustus 2017.

Tiirmaa (2011). Cyber Security Threats and responses: at Global, Nation-State. http://www.ceri-scienes-po.org pada 4 Juni 2017.