KEPENTINGAN INDONESIA DALAM MENGANTISIPASI ANCAMAN CYBER SERTA KERENTANANNYA TERHADAP PENCEGAHAN STRATEGIS SERANGAN KONVENSIONAL

Efatha Filomeno Borromeu Duarte[1)]
[1)] Fakultas Ilmu Sosial dan Ilmu Politik Universitas Udayana
Email:Efathaborromeu@unud.ac.id [1],

ABSTRACT

Sebagian besar fokus dalam akademik dan komunitas praktisi di Indonesia terfokus dalam upaya pencegahan serangan siber. Telah dilakukan dalam-pencegahan domain, dan bahkan studi pencegahan lintas domain telah sebagian besar berkaitan dengan pekerjaan instrumen kekuatan noncyber untuk mencegah serangan siber. Bagaimanakah Kepentingan Indonesia Dalam Mengantisipasi Ancaman Cyber Serta Kerentanannya Terhadap Pencegahan Strategis Serangan Konvensional. Penelitian ini menggunakan data sekunder. Data sekunder dapat dijelaskan sebagai data yang diperoleh memlalui hasil wawanara yang sudah diolah baik melalui media, jurnal dan sebagainya. Hasil penelitian 1). Strategi Aktor Dalam Penguatan Pencegahan Perang Siber. 2). Risiko Cyber Hingga Konvensional. 3). Rekomendasi Kebijakan. 4). Spionase.

Keywords*: Siber, Ancaman, Kerentanan*

1. PENDAHULUAN

Cendekiawan dan praktisi di bidang Strategi Pertahanan saat ini sangat fokus pada konflik strategis untuk mengantisipasi serta menghadapi serangan siber dan tenti ini merupakan keharusan bagi Indonesia: pertama, untuk mempertahankan dan memperkuat arus pencegahan serangan siber yang signifikan dengan dapat memberikan konsekuensi; dan yang kedua, untuk membalikkan gelombang perilaku tindakan jahat kriminal yang mungkin tidak Tereskalasi sampai ke tingkat serangan dengan bersenjata, tetapi tentu ini dapat namun memiliki implikasi strategis yang terakumulatif dan merupakan suatu suksesi yang tergabung dalam bagian dari kampanye musuh.

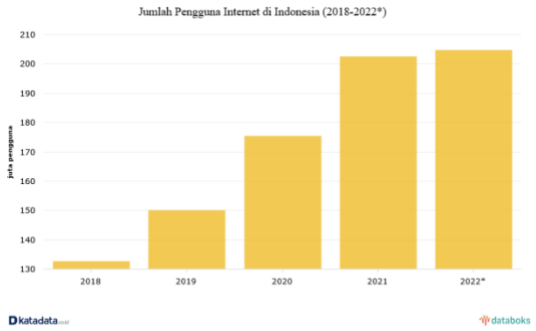
Saat ini dengan perubahan lingkungan strategis yang cepat, ancaman dalam dunia siber makin menjadi sorotan dantentu dengan beberapa kemuktahiran metode serangan serta kurang adaptifnya arah kebijakan pemerintah berubah bisa lebih baik atau lebih buruk secara terus menerus.

Hal inilah yang memaksa peranan yang maksimal dari Badan Siber dan Sandi Negara (BSSN) Kementerian Informasi dan Komunikasi sebagai *leading sector* dalam bidang informasi dan teknologi haruslah sudah responsif, adaptif juga aplikatif dengan menyesuaikan diri pada situasi perubahan masa kini.

Tetapi gerakan respon Indonesia ini sangat penting disoroti karena bagaimanapun tentulah hal ini merupakan ikwal mashlatan negara Indonesia, latar belakangnya ialah bahwa masih kurangnya perhatian yang terucucur dalam kajian-kajian serta penelitian mengenai keamanan hubungan lintas domain, mengenai pertahanan dan ancaman perang siber untuk segera mendektaksi taktik musuh yang bergerak di bawah tanah dengan tingkat siklus perang tinggi.

Pada kenyataanya disadari atau tidak yang menjadi pertanyaan besar ialah mengapa musuh dalam dunia siber lebih memilih untuk melawan Indonesia di level bawah seperti dunia siber, dan berusaha untuk menghindari konfrontasi agresi militer secara langsung. Pahami bersama bahwa dalam kondisi yang relatif sama pula, musuh-musuh baik state actor maupun non state aktor juga dapat melakukan investasi besar-besaran dalam teknologi serta inovasi mereka untuk secara langsung dapat mengejar ketertinggalan itu sekaligus untuk menambah kemampuan untuk melindungi diri mereka sendiri dari ancaman luar.

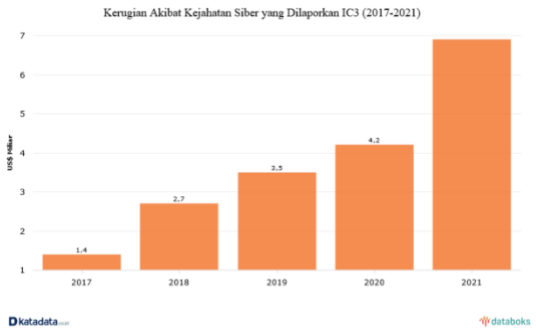
Dengan jelasnya data, bahwa Indonesia adalah salah satu pemain dengan populasi pengguna internet banyak di dunia ini tentunya tak terelakan. DIlansir dari *We Are Social*, (https://wearesocial.com/us/,2022)
pada masa kini saja terdapat 204,7 juta pengguna aktif internet di Tanah bumi Pertiwi per Januari tahun 2022. tren peningkatan angka bertambah lurus naik naik berkisar pada 1,03%.



Gambar 1.1 Pengguna Internet (https://wearesocial.com/us/)

Dengan melihat data di atas maka jelas saja bahwa Indonesia secara teknologi harus sudah membentuk kemampuan siber yang canggih dengan adaptasi dari riset-riset unggulan militernya.

Disisi lain tanpa kita sadari bahwa faktanya bahwa saat ini banyak terjadi peningkatan kejahatan siber atau *cyber crime.* Banyak pengguna maka banyak juga para kriminal dan yang dilansir ialah angka kerugian yang ditimbulkan menyeramkan bahkan terus meningkat tajam kurun waktu hanya lima tahun terakhir. Tercatat bahwa pada tahun 2017 saja, data menunjukan kerugian akibat kejahatan siber yang terlaporkan ke *Internet Crime Complaint Center* (IC3) mencapai US$1,4 miliar. Nilai kerugian atas tindakan kriminal tersebut saja US$6,9 miliar pada 2021.



Gambar 1.2 (Kata Data.com)

Keadaanya bahwa telah terjadi peningkatan nilai kerugian akibat

kejahatan dunia siber dan ini tercatat lengkap dengan jumlah sebekitar 51,7% per tahunnya. Dalam kurun rentang waktu lima tahun terakhir, seperti yang dilansir oleh IC3 melapokan mendapat pengaduan sebanyak 552 ribu dari seluruh belahan dunia.

Meskipun saat ini terdapat aturan keamanan atas data-data pribadi diatur dalam legislasi dan regulasi, yang tertuang dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE 2008) dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE 2016) Pasal 26 Ayat 1 bahwa kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan. Peraturan Menteri Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Tetapi tampaknya perlu diteliti lagi bagaimanakah kita melihat Kepentingan Indonesia Dalam Mengantisipasi Ancaman Cyber Serta Kerentanannya Terhadap Pencegahan Strategis Serangan Konvensional?

2. KAJIAN PUSTAKA

2.1 CYBER SPACE

Dalam dunia maya atau yang terkadang disebut *Cyberspace* isitilah ini dapat didefinisikan sebagai sebuah ruang di mana informasi beredar dari satu media ke media lain dan di mana ia diproses, diduplikasi, dan disimpan.

Dapat dinalari juga merupakan suatu ruang di mana alat berkomunikasi, di mana teknologi informasi terkoneksi secara masif di mana-mana. Jadi tentunya pada dasarnya, dunia maya terdiri dari komunikasi sistem, komputer, jaringan, satelit, dan infrastruktur komunikasi yang semuanya menggunakan informasi dalam format digitalnya. Ini termasuk suara, suara, teks, dan data gambar yang dapat dikontrol dari jarak jauh melalui jaringan, yang meliputi: teknologi dan alat komunikasi seperti berikut ini:

- Wifi
- Laser
- Modem
- Satelit
- Jaringan lokal
- Handphone
- Serat optik
- Komputer
- Perangkat penyimpanan
- Peralatan tetap atau bergerak

2.2 KEAMANAN SIBER

Dunia maya, seperti medan pertempuran virtual, telah menjadi tempat untuk konfrontasi. tion: perampasan data pribadi, spionase ilmiah, ekonomi dan aset komersial perusahaan yang menjadi korban pesaing atau kekuasaan asing, gangguan layanan yang diperlukan untuk berfungsinya ekonomi dan kehidupan sehari-hari, kompromi informasi yang terkait dengan kedaulatan kita. (Delon, F. 2008.)

Keamanan Siber diibaratkan sebuah lapangan permainan hukum di mana otoritas lokal dan pemerintah bertujuan untuk menciptakan sebuah payung hukum mereka untuk mengatur, mengatur, dan melindungi aset berwujud dan aset tidak berwujud dari kejahatan dunia maya, kegiatan

spionase, dan serangan menempatkan hubungan yang sama dalam suatu domain besar.

3. METODELOGI PENELITIAN

Dalam penelitian ini peneliti menggunakan pendekatan kualitatif deskriptif analitis.. Jenis data yang digunakan berasal media pemberitaan dan data sekunder berasal dari literatur-literatur yang mendukung data. Kemudian pada teknikpengumpulan data terdiri dari dokumentasi studi kepustakaan, kemudian teknik analisa datanya dianalisadari setiap peristiwa dan juga teori yang ada.

3.1 JENIS DAN SUMBER DATA

Dalam penelitian ini menggunakan data sekunder. Data sekunder dapat dijelaskan sebagai data yang diperoleh memlalui hasil wawanara yang sudah diolah baik melalui media, jurnal dan sebagainya. Hal ini di perkuat oleh Husein Umar (2013:42) data sekunder adalah: “Data sekunder merupakan data primer yang telah diolah lebih lanjut dan disajikan baik oleh pihak pengumpul data primer atau oleh pihak lain misalnya dalam bentuk tabel-tabel atau diagram- diagram”. Sedangkan menurut Nur Indrianto dan Bambang Supomo (2013:143) data sekunder adalah: Data sekunder merupakan sumber data penelitian yang diperoleh peneliti secara tidak langsung melalui media perantara (diperoleh dan dicatat oleh pihak lain)”.

3.2 TEKNIK PENGUMPULAN DATA

Teknik pengumpulan data merupakan suatu teknik ataupun berbagai cara yang digunakan peneliti guna mendapatkan data penelitiannya. Teknik yang digunakan dalam penelitian ini adalah melalui studi pustaka (library research). Studi pustaka adalah teknik pengumpulan data yang dilakukan dengan mengumpulkan dan membaca literatur yang relevan seperti buku, informasi berita, dan laporan jurnal ilmiah, yang khususnya berkaitan dengan Kepentingan Indonesia Dalam Indonesia Japan Economics Partnership Agreement Terkait Perikanan Indonesia.

4. HASIL DAN PEMBAHASAN

4.1 STRATEGI AKTOR DALAM PENGUATAN PENCEGAHAN PERANG SIBER

Hal pertama yang dapat kita perhatikan ialah bagaiama peran Presiden apakah akan mau berturut-turut memberikan suatu rekomendasi berupa instrumen kebijakan untuk mengadministrasi dan mengakomodasi sektor pertahanan siber agar jauh lebih detail dalam implementasinya.

Dalam sisi strategisnya terkadang kata pencegahan adalah sangat bersifat koersif yang memiliki usaha untuk mencegah aktor mengambil tindakan yang tidak dapat diterima. (Freedman, 2004). Mari kita coba telaah lebih lanjut bahwa konsep pencegahaan dapat berupa suatu tindakan agresif yang dapat berupa kampanye tentang supremasi kekuatan militer Indonesia sehingga kita dapat memberikan suatu pukulan mundur dari niat mereka untuk memerangi Indonesia dalam sisi siber.

Dalam tataran aksinya berdasarkan dalam logika dasar: yaitu, untuk mencegah musuh sebelum berkehendak dalam mengambil tindakan yang tidak diinginkan melalui sebuah Ancaman-ancaman yang ada tentu ini sangat bermanfaat.Indonesia bisa menjadi sangat represif dalam

melihat percaturan keamanan global untuk fokus dalam politik geo-politik dan geo-strategi. Semua terpusat dalam suatu kemanfaatan dari kerja nyata pemimpin negara untuk mau lebih agresif dengan kredibilitasnya.

4.1.2 RISIKO CYBER HINGGA KONVENSIONAL

Mari kita fokuskan sedikit pada suatu keandaian yaitu bagaimana jika nantinya dari perang siber dapat mempengaruhi pencegahan perang Nuklir? Tentu hal ini sangat bisa terjadi secara nyata. Saat ini pada perkembanganya terdapat banyak sekali kerentanan dunia maya yang merasuk dalam seluruh sektor konvensional dan berimplikasi pada nuklir. Buktinya saja saat ini tiap negara di dunia terus mengejar pertahanan dan memfokuskan pada kajian riset yang berhubungan dengan modernisasi yang mengandalkan pada pemuktahiran infrastruktur digital yang rentan. (DOD, January 2013)

Dalam sebuah studi ternyata kerentanan ini hadir di tiga kategori, yang memiliki kekhawatiran yang berbeda-beda:
1). Kerentanan teknis dalam program senjata sudah di bawah
pengembangan serta sistem lapangan,
2). Kerentanan sistemik ini pada tingkat di seluruh platform jaringan ("sistem kerentanan tem-of-sistem), pasokan rantai dan akuisisi dari buah-buah proses, dan
3). Kerentanan nonteknis berasal dari operasi pengumpulan informasi. Konektivitas, otomatisasi, estetika, kesadaran dalam situasional, dan presisi adalah ini semua adalah komponen inti dari militer yang harus telah difasilitasi oleh stake holder terkait, namun, lembaga juga hadir untuk mau banyak memberikan analisis kerentanan dan akses poin untuk diperbaiki agar dapat menciptakan data bsae untuk intrusi dan serangan dunia maya.

4.1.3 REKOMENDASI KEBIJAKAN

Barang tentu ini saling ketergantungan bagaimana politik hukum Indonesia harus juga memperhatikan semua aspek baik dari dunia siber, konvensional, dan potensi perang tingkat energi nuklir. Rekomendasinya jelas bahwa para pembuat kebijakan Indonesia harus memprioritaskan upaya untuk mengurangi kemampuan siber dunia yang dapat berakhir pada agresi yang bersifat konvensional dan energi nuklir. Indonesia harus bermain dan mengukur kemampuan dunia dan juga turut memastikan mereka tangguh terhadap tindakan musuh di dunia maya atau tidak.

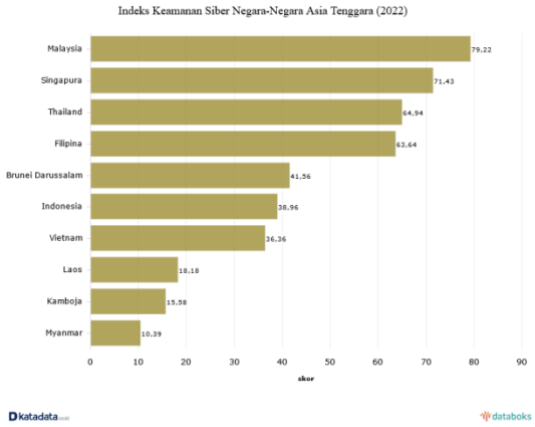
Menglah kita menganut paham bebas aktif tetapi dalam dunia yang kitan terdistorsi risiko ini haruslah diambil untuk hal ini memang bukanlah sebuah kemampuan Indonesia dan mungkin dimiliki negara seperti AS tetapi ini mungkin tidak begitu buruk dan mungkin saat kritis.

4.1.4 SPIONASE

Lain dari pada yang lain strategi spionase ini sangat penting yang mendukung kekuatan dunia maya. Adopsi rencana ini dilakukan terhadap sistem negara Indonesia dan ini tentu akan memungkinkan musuh untuk meniru strategi kita tapi kita dapat membuat sesuatu mekanisme

pertahanan Indonesia tanpa investasi yang gila biayanyadan ini akan sangat sebanding atas nama riset penelitian.

Indonesia akan memahami postur pencegahannya sendiri hasil dari riset dari negara lain secara kredibel dan efektif.
selama krisis dan konflik.



Gambar 1.3
(Kata Data.com)

Menurut National Cyber Security Index (NCSI) yang dikutip Senin (07/03), keamanan siber Indonesia menempati urutan ke-6 di Asia Tenggara. Indonesia saat ini berada di peringkat 83 dari 160 negara di dunia. NCSI mendasarkan penilaian ini pada beberapa metrik, termasuk: B. Aturan hukum nasional tentang keamanan siber, ada tidaknya lembaga pemerintah di bidang keamanan siber, kerja sama pemerintah di bidang keamanan siber, dan bukti publik seperti situs web resmi pemerintah dan program terkait lainnya.

Menggunakan indikator ini, NCSI menilai skor keamanan siber Indonesia di 38,96 dari 100. Angka ini jauh di bawah nilai negara tetangga.

Malaysia memiliki keamanan siber terbaik di Asia Tenggara dengan skor 79,22. Keamanan siber negara tetangga itu menempati urutan ke-18 di dunia. Menurut data National Cyber Security Index (NCSI) yang dikutip Senin (3/7), keamanan siber Indonesia menempati urutan keenam di Asia Tenggara. Indonesia saat ini berada di peringkat 83 dari 160 negara di dunia.

5. KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Karena kemajuan teknologi siber di seluruh dunia, Indonesia tampaknya menjadi salah satu pemain kunci dalam manajemen lalu lintas informasi siber di masa depan. Saat ini, Indonesia berada di posisi pertama di antara negara-negara yang bisa menjadi sasaran para hacker. Dengan hadirnya fungsi siber sebagai arena politik internasional, Indonesia mendukung pertahanan dan keamanan siber nasional untuk mencegah ancaman siber global, baik sipil maupun militer yang telah menjadi

6. DAFTAR PUSTAKA

Daftar Pustaka:

Buku:

Brascomb, Anne W. 1986. Toward A Law of Global Communication Network. USA: Longman.

Longworth, Elizabeth. 2000. “The Possibilities for legal framework for cyberspace-Including New Zealand Perspective”. Dalam Theresa Fuentes et.al (editor). The International Dimesions of Cyberspace Law: Law of Cyberspace Series. Vol.1. Aldershot: Ashgate Publishing Limited.

Pusat Teknologi Informasi dan Komunikasi Badan Pengkajian dan Penerapan Teknologi (BPPT). 2007. Kajian Konvergensi Teknologi Informasi dan Komunikasi. Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT.

Lawrence Freedman, Deterrence (Cambridge, UK: Polity, 2004), 26. 11

Jurnal:

Arianto, Adi Rio. 2017. “Cyber Security: Geometripolitika dan Dimensi pembangunan Keamanan Dunia Era Horizontal Abad 21”. Jurnal Power In International Relations. Universitas Potensi Utama. Vol. 1. No.2. Februari.

Ardiyanti, Handrini. 2014. “Cyber-Security dan Tantangan Pengembangannya di Indonesia”. Jurnal Politica. Vol. 5. No. 1. Juni.

Indrawan, Raden Mas Jerry dan Efriza 2017. “Bela Negara Sebagai Metode Pencegahan Ancaman Radikalisme di Indonesia”. Jurnal Pertahanan dan Bela Negara. Universitas Pertahanan Indonesia. Vol. 7.No. 3. Desember.

Menthe, D. 1998. “Jurisdiction in Cyberspace: A Theory of International Space”.

Michigan Telecommunications and Technology Law Review. 23 April.

Sanusi, M. Arsyad. 2005. Hukum Teknologi dan Informasi. Bandung: Tim Kemas Buku.

Vivian, John. 2008.Teori Komunikasi Massa. Jakarta: Kencana.

Thompson, Ronald & William Cats Barril. 2003. Information Technology and Management. New York: Mc Graw Hill.

Makalah:

Arianto, Adi Rio. 2016. “Keamanan Siber Menuju Perang Geometri Antarbangsa: Geometripolitika dan Arsitektur Keamanan Dunia Era Horizontal Abad 21″.

Prosiding Konvensi Nasional Asosiasi Ilmu Hubungan Internasional Indonesia VII (VENNAS AIHII VII).

Akamai. 2013. “The State of The Internet Report”. Dokumen Americas Highlights. Second Quarter.

Peraturan Menteri Pasal 9 Peraturan Menteri Komunikasi dan Informatika No. 29/PER/M. KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M. Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Website

Gautama, Hasyim, “Penerapan Cyber Security”, dalam http://kemhubri.dephub.go.id/pusdatin/files/materi/penerapan_Cybersecurity.pdf, diakses pada 17 Oktober 2012